KNIHA KÓDŮ A ŠIFER

SIMON SINGH

Utajování od starého Egypta po kvantovou kryptografii

Vydala roku 2003 nakladatelství Dokořán a Argo

ISBN 80-86569-18-7 (Dokořán)
ISBN 80-7203-499-5 (Argo)

„Touha odhalovat tajemství je hluboce zakořeněna v lidské přirozenosti. Dokonce i ten nejméně zvědavý člověk zpozorní, dostanou-li se mu do rukou jinak nedostupné informace. Občas se sice někomu poštěstí získat zaměstnání, jehož náplní je řešení záhad, většinou jsme však nuceni uspokojovat svou dychtivost luštěním různých hádanek sestavených jen tak pro zábavu. Málokdo se dostane v luštění záhad dále než ke křížovkám a detektivním příběhům, řešení tajuplných kódů je seriózní činností jen pro několik vyvolených."

John Chadwick
The Decipherment of Linear B (Rozluštění lineárního písma B)

Obsah

O české kryptologii

Motto:
Šifrování je často jedinou možnosti, jak chránit cenná data.

Kryptologie není naukou o kryptách, jak si hodně lidí myslí, ale o šifrách, a její vliv na světovou historii je fascinující. A jaká je česká kryptologie? Máme také my nějaké tajné pracoviště nebo podzemní město, jako je tomu v Anglii v Menwith Hill, kde se luští a vyhodnocují zachycené komunikace? Tahle tichá pracoviště totiž ovlivňovala výsledky všech válek, na něž si vzpomenete. Také naše šifrogramy, proudící za druhé světové války mezi Londýnem a domácím odbojem, byly luštěny, jak ostatně po válce potvrdili sami *zajatí* Němci, kteří luštění prováděli. Začal jsem druhou světovou válkou, protože v předválečné české kryptologii se nedělo nic významného. Po válce se česká kryptologie stabilizovala a vyvíjela až do roku 1989 v závislosti na tehdejším SSSR. Přestože nejexponovanější vládní spoje byly zajištěny sovětskou technikou, byly vyvíjeny šifrátory také ryze české a úroveň kryptologie nebyla malá. Soustředila se však výhradně na zajištění potřeb ministerstev (zahraničí, vnitro, armáda) a státně-mocenského aparátu. Po sametové revoluci došlo k odlivu pracovníků příslušných služeb do komerční oblasti, kde vznikala poptávka po šifrovacích zařízeních, programech pro ochranu dat apod. Zařadili jsme se dokonce mezi vývozce šifrovacích zařízení a softwaru. Během uplynulých 13 let se také samostudiem vyškolilo několik desítek vysokoškoláků v oblasti počítačové bezpečnosti a částečně i aplikované kryptologie. Všude ve vyspělých zemích se však kryptologie

už řadu let vyučuje na vysokých školách a o bezpečnosti a kryptologii zde *vycházejí* stovky knih. Přesto i tam je po těchto specialistech velká poptávka. Prudký nárůst zaznamenala také teorie. Před dvaceti lety proběhla během roku jediná světové kryp-tografická konference, nyní se jich každoročně koná více než pět. Lidé, kteří rozumí metodám ochrany dat, jsou a budou potřební v mnoha bankách, na ministerstvech a v jiných státních institucích, u mobilních operátorů, v průmyslu informačních a komunikačních technologií apod. Dnes tu ale tito lidé chybí - a chybí i příslušnáčeská terminologie. I když jsem se snažil po celých deset uplynulých let kryptologii popularizovat - zejména každý měsíc v časopise *Chip*, *ale* i na různých bezpečnostních konferencích - výsledek je nevalný. Každý druhý technik místo šifrovat řekne „kryptovat" a místo au-tentizace „autentikace". Chce to zkrátka ještě čas. Získal jsem však mladého kolegu Tomáše Rosu, jednoho z mála porevolučních vysokoškoláků, který si může říkat kryptolog. V takto vzniklém tandemu jsme při práci na jednom projektu pro Národní bezpečnostní úřad také objevili závažnou chybu v programu PGP. Tím jsme dostali „českou kryptologii" i na stránky *The New York Times* (PGP používají miliony Američanů a jsou na něj hrdí, viz 8. kapitola této knihy). Podařilo se nám přispět i k rozvoji teorie a popsat možné útoky na algoritmus RSA tam, kde by to nikdo nečekal. Po dvaceti letech konání světových kryptografických konferencí tak v Kalifornii letos zazněl i náš příspěvek. Český kryptologický výzkum stále tvoří roztroušené a izolované ostrůvky, na tom jsme nic nezměnili, ale Češi jsou chytrý národ, takže za několik let může situace vypadat mnohem nadějněji.

Co v knize nenajdete

A teď ještě pár slov o tom, jaké významné události se odehrály až po napsání knihy, takže v ní již nemohly být zaneseny. V roce 1998 byl za čtvrt milionu dolarů sestrojen DES-Cracker - stroj, který je během devíti dnů schopen vyzkoušet všech 2^{56} (tj. 72 057 594 037 927 936) možných klíčů šifry DES. Dále se na internetu spojilo 300 000 dobrovolníků a po čtyřech letech práce jejich počítače vyluštily 64bi-tový klíč k šifře RC5. Nejpodstatnější událostí bylo však přijetí nového amerického šifrovacího standardu AES v roce 2002. Byl vybrán po čtyřech letech veřejné soutěže a i jeho nejkratší klíč má cca 3.10^{38} možných hodnot, je tedy tak velký, že vyzkoušení všech možností dostupnými hmotnými pozemskými zdroji je vyloučené. Ledaže by došlo ke zcela převratnému pokroku, například na poli tzv. kvantových počítačů, o nichž se v knize také dočtete. Jako obrana proti kvantovým počítačům už byly také zkonstruovány nové kvantové šifrátory. Jinými slovy, neustálý souboj kryptografů a kryptoanaly-tiků se nezastavil. Už už se *zdálo*, že kryptografové vyhráli, neboť AES bude dost silná, ale luštitelé přišli s novým objevem, který dostal divné jméno - postranní kanály. Kryptoanalytici ukázali desítky možností, jak čerpat informace nejen z vlastních šifrogramů, ale i ze způsobu jejich vzniku, ze způsobu, jak šifrátory pracují nebo komunikují se svým okolím. Dokáží užitečnou informaci získat z těch nejnicotnějších detailů, například z chybových hlášení typu „dešifrování této zprávy nedopadlo dobře", z časového trvání operací nebo z elektromagnetického vyzařování šifrátoru. Tyto fantastické objevy nových možností kryptoanalýzy vyvolají protiakci kryptogra-fů. Mnoho

zařízení nebo počítačových programů se dostane do nového ohrožení, mnozí výrobci nebudou na tato nová nebezpečí reagovat a mnoho lidí bude stále dělat tytéž chyby jako před sto lety. A tajné služby? Ty se po pádu železné opony přeorientovaly více na ekonomickou špionáž. K tomu přistupuje nový protivník - mezinárodní terorismus. Proto zápas mezi kryptografy a kryptoanalytiky vůbec nekončí, naopak je stále dramatičtější. Ani velký bratr nespí, neboť - jak se říká v NSA: „V Boha věříme, vše ostatní monitorujeme."

RNDr. Vlastimil Klíma, prosinec 2002

Úvod

Králové, královny a generálové po tisíce let spoléhali na účinné komunikační systémy, jež jim umožňovaly vládnout jejich zemím a velet armádám. Zároveň si vždy byli vědomi, jaké následky by mělo, kdyby jejich zprávy padly do nepovolaných rukou: vyzrazení cenných tajemství cizincům, odhalení klíčových informací nepříteli. Bylo to právě riziko vyzrazení, co vedlo k rozvoji kódů a šifer, tedy technik určených k ukrytí smyslu zprávy před všemi kromě zamýšleného příjemce.

Ve snaze dosáhnout utajení provozují jednotlivé státy svá šifrová pracoviště zodpovědná za bezpečnost komunikací, kde se vyvíjejí a uvádějí do praxe nejlepší možné šifry. Cizí luštitelé šifer se naopak snaží tyto šifry rozluštit a získat ukrytá tajemství. Luštitelé šifer jsou lingvističtí alchymisté, jakési mystické společenství, které se snaží vyluštit z nesrozumitelných symbolů jejich skrytý význam. Historie kódů a šifer je příběhem boje mezi tvůrci a luštiteli šifer, boje probíhajícího po staletí, intelektuální bitvy, jež měla a má hluboký dopad na světové dějiny.

Při psaní této knihy jsem sledoval dva hlavní cíle. Prvním z nich je zmapovat vývoj kódů. Slovo vývoj je případné, protože rozvoj šifrovacích technik lze chápat jako evoluční zápas. Kód je vždy v ohrožení. Jakmile luštitelé vyvinou nový způsob, jak odhalit slabinu kódu, ztratí tím kód svůj význam. Buď zmizí, nebo se přetvoří v nový, účinnější kód. I ten pak prosperuje pouze do té doby, než se podaří odhalit jeho slabiny - a tak dále. Jde o analogii situace, v níž se nachází například bakteriální kmen nakažlivé nemoci. Bakterie žijí, prosperují a přežívají do té doby, než lékaři najdou antibiotika, jež jsou namířena proti slabému místu daných bakterií a dovedou je zabít. Bakterie jsou tak nuceny dál se vyvíjet a antibiotika „přelstít". Pokud se jim to povede, budou znovu přežívat a prosperovat. Jsou pod neustálým evolučním tlakem, jímž působí nasazení nových a nových léků.

Neustálý boj mezi tvůrci a luštiteli šifer vedl k celé řadě významných vědeckých objevů. Tvůrci šifer vždy usilovali o stále dokonalejší utajení komunikací, zatímco jejich luštitelé vyvíjeli ještě rafinovanější techniky útoku. V této snaze o uchování i odhalení tajemství musely obě strany zvládnout rozmanité obory a technologie od matematiky po lingvistiku, od teorie informace po kvantovou fyziku. Vynaložené úsilí bylo pro všechny zmíněné obory přínosem a jejich práce vedla často k urychlení technického pokroku. Nejvýraznějším příkladem je vznik moderních počítačů.

Kódy stojí v pozadí mnoha historických mezníků. Někdy rozhodovaly o výsledcích bitev, jindy zapříčinily smrt korunovaných hlav. Pro ilustraci klíčových okamžiků evolučního vývoje kódů vám předkládám příběhy o politických

intrikách, o životě a smrti. Historie kódů je natolik bohatá, že jsem byl nucen mnoho fascinujících příběhů vynechat - má práce rozhodně nevedla k vyčerpávajícímu výsledku. Pokud se chcete dovědět více a prostudovat problematiku detailněji, odkazuji vás na seznam doporučené literatury.

Vedle souhrnu vývoje kódů a jejich důsledků pro historii je druhým cílem knihy ukázat, že tato tematika je dnes důležitější než kdy dříve. V době, kdy se informace stávají stále cennější komoditou, kdy komunikační revoluce mění podobu společnosti, začíná hrát šifrování v každodenním životě stále důležitější roli. Naše telefonní hovory se dnes běžně spojují přes satelity, naše e-maily procházejí po cestě celou řadou počítačů. Takové komunikace lze snadno odposlouchávat, což ohrožuje naše soukromí. Podobná úvaha platí i pro obchodní záležitosti; stále větší podíl obchodu se realizuje prostřednictvím internetu, takže je nezbytné zajistit firmám a jejich zákazníkům bezpečnost. Jedinou metodou, jež může ochránit soukromí a zaručit úspěch elektronického obchodu, je šifrování. Umění tajné komunikace, známé též jako kryptografie, poskytne zámky a klíče informačního věku.

Zároveň je nutno říci, že rostoucí poptávka široké veřejnosti po kryptografii je v rozporu s požadavky vymahatelnosti práva a národní bezpečnosti. Policie a tajné služby po desetiletí užívaly odposlechů v boji proti teroristům a organizovanému zločinu, ale současný vývoj velmi silných kódů hrozí tím, že by takový postup mohl ztratit účinnost. S nadcházejícím 21. stoletím vyvíjejí zastánci občanských práv stále větší tlak na široké využití kryptografie v zájmu ochrany práv jednotlivce. Spolu s nimi zastávají stejné stanoviskozástupci podnikové sféry, kteří se dožadují silné kryptografie kvůli bezpečnosti transakcí v rychle se rozvíjejícím světě elektronického obchodu. Ti, kteří jsou odpovědní za právo a pořádek, naopak apelují na vlády, aby použití kryptografie omezily. Otázkou je, čeho si ceníme výše - soukromí, nebo efektivně pracující policie? Existuje nějaký kompromis?

I když má kryptografie v dnešní době velký význam i pro občanské aktivity, je třeba zdůraznit, že ani vojenská kryptografie neztrácí své opodstatnění. Říká se, že první světová válka byla válkou chemiků, neboť v ní byl poprvé použit chlór a hořčičný plyn; druhá světová válka je označována kvůli atomové bombě jako válka fyziků. Třetí světová válka by pak mohla být válkou matematiků, neboť právě oni mají pod kontrolou její nejdůležitější zbraně - informace. Matematici vyvinuli kódy, s jejichž pomocí se dnes chrání vojenské informace. Jistě není překvapením, že existují jiní matematici, kteří se snaží tyto kódy luštit.

Při popisu evoluce kódů a jejich významu pro historii lidstva jsem si dovolil malou odbočku. Kapitola 5 popisuje vyluštění některých starověkých písem včetně lineárního písma B a egyptských hieroglyfů. Z technického hlediska tu je patrný jeden rozdíl: kryptografie se zabývá komunikací, jež byla záměrně navržena tak, aby skryla tajemství před nepřítelem, zatímco písma starověkých civilizací takový účel neměla; prostě jsme jen postupem věků ztratili schopnost je číst. Avšak dovednosti potřebné k odhalení smyslu archeologických textů se velmi podobají těm, jež potřebují luštitelé šifer. Ještě dříve, než jsem si přečetl knihu Johna Chadwicka *The Decipherment of Linear B* (Rozluštění lineárního písma B), která

popisuje nalezení smyslu textu starověké středomořské civilizace, jsem byl fascinován skvělými intelektuálními výkony těch, kteří dokázali rozluštit písmo našich předků a umožnili nám tak dovědět se více o jejich civilizaci, víře a každodenním životě.

Puristům se musím omluvit za název knihy v anglickém vydání - *The Code Book.* Nejde v ní jen o kódy. Termín „kód" se vztahuje ke *zcela,* konkrétnímu typu tajné komunikace, jenž během staletí ztratil na významu. V rámci kódu se slovo či fráze nahrazuje jiným slovem, číslem či symbolem. Například tajní agenti mají svá krycí (kódová) jména chránící jejich identitu, tedy slova používaná namísto skutečných jmen. Podobně lze slovní spojení Útok za úsvitu nahradit kódovým slovem Jupiter a to zaslat veliteli na bitevní pole, aby

informace zůstala nepříteli skrytá. Pokud se štáb a velitel předem dohodli na kódu, pak význam slova Jupiter bude oběma stranám jasný, zatímco nepřítel, který je zachytí, nebude rozumět ničemu. Alternativou ke kódu je šifra - technika působící na nižší úrovni, která nahrazuje písmena namísto celých slov. Pokud například nahradíme každé písmeno tím, jež následuje po něm v abecedě (tedy namísto A píšeme B, namísto B píšeme C a tak dále), pak Útok za úsvitu přepíšeme jako Vupl ab vtwjuv. Šifry jsou ústředním pojmem kryptografie, takže by se tato kniha měla správně jmenovat *The Code and Cipher Book,* obětoval jsem však přesnost zvučnosti. [My v českém překladu nikoli - pozn. překl.]

Tam, kde bylo třeba, jsem uvedl definice různých technických pojmů používaných v kryptografii. Přestože se jimi obecně vzato řídím, místy jsem použil i termín, který možná není technicky přesný, je však u laické veřejnosti známější. Dovolil jsem si to učinit jen tehdy, je-li význam slova z kontextu zcela jasný. Na konci knihy najdete slovníček pojmů. Žargon kryptografie je ostatně zpravidla zcela průhledný: tak například *otevřený text je* zpráva před zašifrováním, *šifrový text* zpráva po zašifrování. Než ukončím tento úvod, musím se ještě zmínit o problému, jemuž čelí každý autor, jenž se dotkne oblasti kryptografie: věda o tajemství je převážně sama o sobě tajná. Mnozí z hrdinů této knihy nedosáhli během svého života veřejného uznání, neboť jejich práce stále ještě měla diplomatickou či vojenskou hodnotu. Během přípravných prací pro tuto knihu jsem měl možnost hovořit s experty britské Government Communications Headquarters (GCHQ), kteří mě seznámili s detaily právě odtajněného pozoruhodného výzkumu ze 70. let. Díky tomuto odtajnění se tři z největších světových kryptografů dočkali ocenění, jež jim právem *náleží.* Toto odhalení mi však připomnělo, že podobných případů, o nichž nevím nic ani já, ani jiní publicisté, je jistě více. Organizace jako GCHQ nebo americká NSA (National Securi-ty Agency) pokračují v utajeném výzkumu na poli kryptografie, takže jejich výsledky jsou tajné a jejich pracovníci anonymní.

Navzdory problémům souvisejícím s utajením jsem věnoval poslední kapitolu knihy spekulacím o budoucnosti kódů a šifer. Zároveň se v ní pokouším zjistit, zda dovedeme odhadnout, kdo v evoluční bitvě mezi tvůrci a luštiteli šifer zvítězí. Navrhnou tvůrci šifer někdy kód, jenž nelze nijak rozluštit, a dosáhnou tak svého cíle -absolutního utajení? Nebo to snad budou luštitelé šifer, kteří posta-ví stroj schopný dešifrovat cokoli? Jsem si vědom toho, že nejlepší mozky oboru pracují v

tajných laboratořích, kde mají k dispozici dostatek prostředků pro svůj výzkum; má tvrzení v poslední kapitole proto mohou být nepřesná. Uvádím například, že kvantové počítače - stroje schopné vyluštit jakoukoli dnešní šifru - jsou dosud ve velmi primitivním stadiu vývoje, je však klidně možné, že někdo již takový počítač sestrojil. Jediní lidé, kteří by mohli poukázat na mé omyly, jsou však ti, kteří to udělat nesmějí.

1

Šifra Marie Stuartovny

V sobotu 15. října 1586 ráno vstoupila královna Marie do zaplněné soudní síně na zámku Fotheringhay. Léta věznění a revmatické onemocnění si vybraly svou daň, přesto vyhlížela stále důstojně, upraveně a nade vší pochybnost královsky. Za doprovodu svého lékaře prošla kolem soudců, úředníků a přihlížejících. Přistoupila k trůnu, který stál uprostřed dlouhé úzké místnosti. Chvíli měla za to, že trůn je výrazem respektu k její osobě, ale zmýlila se. Trůn měl symbolizovat nepřítomnou královnu Alžbětu, Mariina nepřítele a žalobce. Marii zdvořile odvedli na protější stranu místnosti, na místo pro obžalovaného, kde jí připravili židli potaženou karmínovým sametem.

Marie Stuartovna byla obžalována z velezrady. Obvinili ji ze spiknutí, jež si kladlo za cíl zavraždit královnu Alžbětu a získat anglický trůn pro Marii. Sir Francis Walsingham, Alžbětin hlavní tajemník, již předtím uvěznil ostatní účastníky spiknutí, získal jejich doznání a nechal je popravit. Teď bylo jeho záměrem prokázat, že v čele spiknutí stála Marie a že zasluhuje hrdelní trest.

Walsingham věděl, že než bude moci nechat Marii Stuartovnu popravit, musí Alžbětu přesvědčit o její vině. I když Alžběta Marií opovrhovala, měla několik důvodů, proč být zdrženlivá, než ji pošle na smrt. Za prvé Marie byla skotskou královnou, a proto se mnozí tázali, zda anglický soud vůbec smí odsoudit k smrti cizí hlavu státu. Za druhé by Mariina poprava mohla představovat nepříjemný precedens - smí-li stát zabít jednu královnu, pak by se případní rebelové mohli odhodlat zabít i druhou panovnici, tedy samu Alžbětu. K Mariině popravě také nepřispívalo krevní pouto, Alžběta a Marie byly totiž sestřenice. Zkrátka a dobře, bylo jasné, že Alžběta popravu povolí jen tehdy, prokáže-li Walsingham nade vší pochybnost, že Marie patřila ke spiklencům usilujícím o její smrt.

Za spiknutím stála skupina mladých anglických katolických šlechticů, kteří měli v úmyslu odstranit Alžbětu, jež byla protestant-ské víry, a na její místo dosadit katoličku Marii. Soudu bylo zřejmé, že Marie byla pro spiklence klíčovou osobou, zpočátku však nebylo jasné, zda o spiknutí věděla a zda s ním souhlasila. (Věděla a souhlasila.) Walsinghamovým úkolem bylo prokázat hmatatelné spojení mezi Marií a spiklenci.

Onoho rána v první den procesu usedla Marie Stuartovna na lavici obžalovaných, oblečená do černého sametu vzbuzujícího soucit. Obvinění z velezrady neměli právo na obhájce a nesměli předvolat své vlastní svědky. Marii nepovolili ani tajemníka, který by jí pomohl v přípravě na proces. Přesto nebyla její situace beznadějná. Veškerá její korespondence se spiklenci byla šifrovaná,

namísto slov se skládala ze symbolů, které neměly očividný význam. Marie Stuartovna byla přesvědčena, že i kdyby Walsingham dopisy získal, nerozpoznal by, co znamenají. Jestliže zůstane obsah dopisů tajemstvím, nelze jich použít jako důkazu proti ní. To však záviselo na spolehlivosti šifry.

Naneštěstí pro Marii nebyl Walsingham jen tajemníkem, ale také šéfem anglické špionáže. Získal Mariiny dopisy určené spiklencům a věděl zcela přesně, kdo by je uměl rozluštit. Nejlepším odborníkem v zemi byl Thomas Phelippes, který se léta věnoval luštění šifer nepřátel královny Alžběty a poskytoval tak důkazy k jejich odsouzení. Pokud by dokázal přečíst dopisy, které si vyměňovala Marie se spiklenci, pak by smrt skotské královny byla neodvratná. Na druhou

stranu, kdyby šifra byla tak promyšlená, že by její tajemství uchránila, mohla by Marie vyváznout živá. Nebylo to poprvé, kdy síla šifry rozhodovala o životě a smrti.

Vývoj tajného písma

Některé z nejstarších zmínek o tajném písmu pocházejí od Herodota - „otce historie", jak ho nazval římský filozof a politik Cicero. Ve svých *Dějinách* shrnuje Herodotos konflikty mezi Řeky a Peršany v 5. století př. n. 1. Chápal je jako konfrontaci svobody a otroctví, jako boj mezi nezávislými řeckými státy a perskými utla-čovateli. Podle Herodota to bylo právě umění tajných zpráv, co za-chránilo Řecko před dobytím Xerxem - Králem králů, který byl despotickým vůdcem Peršanů.

Dlouhodobé nepřátelství mezi Řeky a Peršany dosáhlo kritického bodu krátce poté, co Xerxes začal stavět Persepolis, nové hlavní město svého království. Z celé říše a sousedních států sem proudily poplatky a dary. Významnou výjimkou byly Athény a Sparta. Xerxes chtěl takovou opovážlivost ztrestat a začal shromažďovat vojsko. Prohlásil, že „rozšíříme perskou říši tak, že její jedinou hranicí bude nebe a slunce nedohlédne země, jež by nepatřila nám". Po pět let sbíral největší vojenskou sílu v dosavadní historii. V roce 480 př. n. 1. byl připraven na překvapivý úder.

Přípravy perské armády však pozoroval Řek Demaratus, který byl ze své vlasti poslán do vyhnanství a žil v perském městě Susy. Přestože byl vyhnanec, cítil nadále loajalitu k Řecku, a tak se rozhodl poslat do Sparty varování před Xerxovými útočnými plány. Problém však byl, jak zprávu dopravit, aby ji nezachytily perské hlídky. Herodotos píše:

„Nebezpečí prozrazení bylo velké a Demaratus přišel jen na jeden způsob, jak zprávu zaslat. Seškrábal vosk ze dvou voskových psacích destiček, sepsal Xerxovy záměry přímo na jejich dřevo a pak zprávu znovu zakryl voskem. Tabulky byly na první pohled prázdné a nevzbudily zájem stráží. Když dorazily do cíle, nikdo nedokázal rozluštit jejich tajemství, až - jak jsem se dověděl - Kleomenova dcera Gorgo (manželka Le-onida) uhodla, oč jde, a řekla ostatním, že je třeba seškrabat vosk. Když tak učinili, našli zprávu, přečetli ji a sdělili ostatním Řekům."Kvůli varování se do té doby bezbranní Řekové *začali* ozbrojovat. Zisky státních stříbrných dolů, dosud rozdělované mezi občany, byly použity ke stavbě dvou set válečných lodí.

Xerxes ztratil moment překvapení. Když jeho loďstvo vplulo do zálivu u

Salaminy nedaleko Athén, byli Řekové připraveni. Xerxes se domníval, že chytil řecké loďstvo do pasti, avšak byli to naopak Řekové, kteří vlákali nepřítele do úzkého zálivu. Věděli, že jejich malé a méně početné lodě by na otevřeném moři proti perské flotile neobstály, ale v zálivu se uplatnila jejich větší manévrovací schopnost. Když se otočil vítr, zůstali Peršané uzavřeni v zálivu. Perská princezna Artemisia byla se svou lodí obklíčena ze tří stran, přesto se pokusila uniknout na volné moře, namísto toho však narazila do jedné z vlastních lodí. Vznikla panika, při které došlo k dalším srážkám, a Řekové rozpoutali krvavou řež. Během jediného dne tak byla pokořena ohromná perská vojenská síla.

Demaratova strategie tajné komunikace spočívala v prostém ukrytí zprávy. Herodotos popisuje i jinou událost, kdy ukrytí textu postačilo k bezpečnému zaslání zprávy. Vypráví příběh, v němž vystupuje Histiaios, který chtěl povzbudit Aristagora Milétského ke vzpouře proti perskému králi. Aby zaslal své poselství bezpečně, oholil Histiaios hlavu svého posla, napsal zprávu na kůži lebky a počkal, až poslovi znovu narostou vlasy. Jak je vidět, v tomto historickém období se menší zpoždění dalo tolerovat. Posel pak mohl cestovat bez potíží, nenesl přece nic závaďného. V cíli své cesty si znovu oholil hlavu a ukázal ji příjemci zprávy.

Komunikace utajená pomocí ukrytí zprávy se nazývá *steganografie*, podle řeckých slov *steganos* (schovaný) a *graphein* (psát). Během dvou tisíc let, jež nás dělí od Herodotových časů, se v různých částech světa rozvinuly různé formy steganografie. Staří Číňané například psali *zprávy* na jemné hedvábí, které pak zmačkali do malé kuličky a zalili voskem. Posel pak voskovou kuličku polkl. Italský vědec Giovanni Porta v 16. století popsal, jak ukrýt zprávu ve vejci vařeném natvrdo pomocí inkoustu vyrobeného z jedné unce kamence a pinty octa. Tím se pak napíše zpráva na skořápku. Roztok pronikne jejími póry a zanechá zprávu na vařeném bílku. Přečíst ji lze, až když vajíčko oloupeme. Do oblasti steganografie patří rovněž neviditelné inkousty. Již z 1. století našeho letopočtu pochází návod Plinia Staršího, jak použít mléko pryšce *(Titbymalus sp.* z čeledi *Euphorbiaceae)* jako neviditelný inkoust. Po zaschnutí je mléko zcela

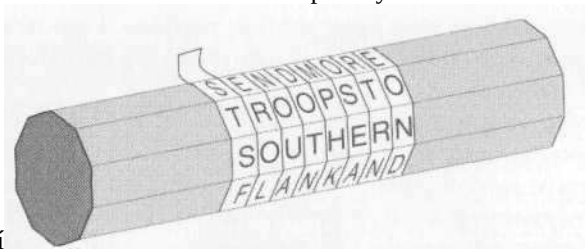
průhledné, když se však lehce zahřeje, zhnědne. I moderní špioni občas improvizovali s použitím vlastní moči, když jim došla zásoba tajného inkoustu.

Dlouhá tradice steganografie jasně ukazuje, že jde o techniku, jež sice poskytuje určitý stupeň utajení, má však zásadní vadu. Když už se zprávu jednou podaří objevit, je prozrazena naráz. Pouhé její zachycení znamená ztrátu veškerého utajení. Důkladná stráž může prohledávat všechny osoby cestující přes hranice, oškrabávat voskové tabulky, nahřívat čisté listy papíru, loupat vařená vejce, holit lidem hlavy a tak dále. Určité množství zpráv se tak vždy podaří zachytit.

Souběžně se steganografií se proto začala rozvíjet i *kryptografie, jejíž název* pochází z řeckého slova *kryptos* (skrytý). Cílem kryptografie není utajit samu existenci zprávy, ale její význam, a to pomocí šifrování. Aby nešlo zprávu přečíst, pozmění se podle pravidel předem dohodnutých mezi odesilatelem a příjemcem. Pokud taková zpráva padne do rukou nepříteli, je nečitelná. Nezná-li nepřítel použitá šifrovací pravidla, pak se mu podaří zjistit obsah zprávy jen s velkým úsilím, anebo vůbec ne.

Přestože jsou kryptografie a steganografie nezávislé techniky, je možné je pro větší bezpečnost zprávy kombinovat. Příkladem takové techniky jsou mikrotečky, používané především během druhé světové války. Němečtí agenti v Latinské Americe dovedli fotografickou cestou zmenšit celou stránku textu do tečky o průměru menším než milimetr a tu pak umístit jako normální tečku za větou do nevinného dopisu. FBI poprvé zachytila mikroteč-ku roku 1941, když dostala tip, ať hledá na papíře jemný odlesk, způsobený použitým filmovým materiálem. Američané od té doby mohli číst obsah zachycených mikroteček, ovšem s výjimkou případů, kdy němečtí agenti zprávu před zmenšením ještě zašifrovali. V případech, kdy Němci takto kombinovali kryptografii se steganografií, mohli Američané jejich komunikaci monitorovat a občas přerušovat, nezískali však žádné informace o německých špionážních aktivitách. Kryptografie je účinnější než steganografie, protože pomocí ní lze zabránit tomu, aby informace padla do rukou nepřítele.

Kryptografii můžeme rozdělit na dvě větve - *transpozici* a *substituci.* Při transpozici se písmena zprávy uspořádají jiným způsobem než původním, jde tedy vlastně o přesmyčku. Takový postup není

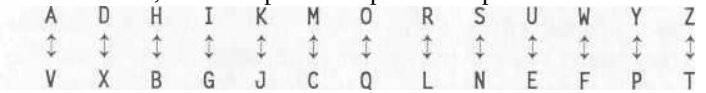


Obrázek 2: Když se pruh kůže odvine z odesilatelovy tyče, obsahuje zdánlivě náhodně uspořádaná písmena: S, T, S, F,... Zpráva se znovu objeví jen tehdy, navineme-li pruh na jinou tyč o stejném průměru.

sloupnost nic neříkajících písmen. Zpráva tak byla zašifrována. Posel vezme pruh kůže, a aby dodal ještě steganografické zdokonalení, může jej použít třeba jako opasek - s písmeny ukrytými na rubu. Příjemce pak pruh kůže ovine kolem tyče se stejným průměrem, jaký použil odesilatel. V roce 404 př. n. 1. dorazil ke králi Sparty Lysandrovi raněný a zkrvavený posel, který jako jediný z pěti přežil těžkou cestu z Persie. Podal Lysandrovi svůj opasek. Ten jej ovinul kolem tyče správného průměru a dověděl se, že se na něho perský Farnabazus chystá zaútočit. Díky této utajené komunikaci se Lysan-dros včas připravil na útok a nakonec jej odrazil.

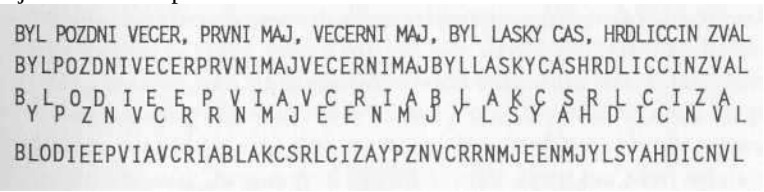
Alternativou k transpozici je substituce. Jeden z prvních popisů substituční šifry se objevuje v *Kámasútře,* kterou napsal ve 4. století n. 1. bráhman Vátsjájana. Vyšel však přitom z rukopisů o 800 let starších. *Kámasútra* doporučuje ženám studovat šedesát čtyři umění, mezi nimi vaření, oblékání, masáž a přípravu parfémů. Na seznamu jsou však i dovednosti, jež bychom v této souvislosti očekávali méně - žonglování, šachy, vazba knih a tesařství. Doporučeným uměním číslo 45 na Vátsjájanově seznamu je *mlecchita-vikalpa,* umění tajného písma, jež

se doporučuje ženám, aby mohly ukrýt informace o svých *vztazích*. Jednou z doporučených technik je náhodně spárovat písmena abecedy a poté nahradit každé písmeno původní zprávy jeho partnerem. Kdybychom tento princip aplikovali na latinskou abecedu, můžeme písmena spárovat například takto:



příliš bezpečný u velmi krátkých zpráv, například takových, jež sestávají z jednoho slova, protože dostupných kombinací písmen je příliš málo. Tři písmena lze například uspořádat jen šesti různými způsoby: bok, bko, kbo, obk, okb, kob. S rostoucím počtem písmen však počet variací prudce roste, takže nalézt původní text bez znalosti použitého pravidla je nemožné. Vezměte si kupříkladu tuhle krátkou větu. Po odstranění mezer, interpunkce a diakritiky (jak je v češtině zvykem) má celkem 35 písmen, jež lze uspořádat téměř 39 000 000 000 000 000 000 000 000 000 000 odlišnými způsoby. Kdyby člověk prověřil jednu kombinaci za vteřinu a na dešifrování by pracovalo dnem i nocí celé lidstvo, trvalo by ověření všech možností téměř 14 OOOkrát déle, než jaké je podle současných znalostí celkové stáří vesmíru.

Náhodné uspořádání písmen zdánlivě *nabízí* velmi vysoký stupeň bezpečnosti, protože z hlediska nepřítele je obtížné rozluštit i velmi krátkou větu. Je tu však problém. Transpozicí vznikne velmi obtížný anagram, jehož luštění není snadné nejen pro nepřítele, ale i pro příjemce zprávy. Aby byl tento způsob šifrování efektivní, je třeba se držet nějakého poměrně jednoduchého systému, na němž se předem dohodl příjemce a odesilatel a jenž zůstal před nepřítelem utajen. Školáci si někdy posílají zprávy kódované „podle plotu", což znamená, že se zpráva rozdělí do dvou řádků a ty se pravidelně střídají písmeno po písmenu. Spodní řádek se pak připojí za horní. Například:



Příjemce může zprávu rekonstruovat tím, že celý proces provede v opačném pořadí. Existuje mnoho dalších forem transpozičních šifer, k nimž patří například třířádkový „plot". Jinou možností je prohodit pořadí každé dvojice písmen: první a druhé písmeno si vymění místo, třetí a čtvrté rovněž a tak dále.

Další formou transpozice je historicky první vojenské šifrovací zařízení, tzv. *scytale* ze Sparty. Jde o dřevěnou tyč, kolem níž se ovine proužek kůže nebo pergamenu, jak je vidět na obrázku 2. Odesilatel napíše zprávu podél tyče, pak proužek odmotá - a dostane po-Namísto schuzka o pulnoci pak odesilatel napíše NMBETJV Q YER-SQMG. Jde o tzv. substituční šifru, při níž se každé písmeno otevřeného textu nahradí jiným písmenem. U transpozice si písmena zachovají svou identitu, ale změní pozici, u substituce je tomu přesně naopak.

První dokumentovaný záznam použití substituční šifry pro vojenské účely se objevuje v *Zápiscích o válce galské* od Julia Caesara. Cae-sar popisuje, jak poslal zprávu Ciceronovi, který byl obklíčen a hrozilo mu, že bude muset kapitulovat. Substituce nahradila římská písmena řeckými, nečitelnými pro nepřítele. Caesar popisuje dramatický účinek doručení zprávy:

„Posel dostal rozkaz, ať vhodí kopí s připevněnou zprávou přes hradby tábora, pokud by se nemohl dostat dovnitř. Tak se i stalo. Gal, vystrašený možným nebezpečím, mrštil kopí. Nešťastnou náhodou se stalo, že se kopí zabodlo do věže. Teprve třetího dne si ho povšiml jeden z vojáků, který kopí sejmul a zanesl Ciceronovi. Ten si přečetl zprávu a poté ji oznámil svým vojákům, což všem přineslo velikou radost."

Caesar používal tajné písmo tak často, že Valerius Probus dokonce sepsal celkový přehled jeho šifer. Toto dílo se bohužel nezachovalo. Díky Suetoniovu dílu *Životopisy dvanácti císařů* (De vita Caesarum) z 2. století n. 1. však máme detailní popis jednoho z typů šifer, jež Julius Caesar používal. Každé písmeno zprávy nahrazoval písmenem nacházejícím se v abecedě o tři pozice dále. Kryptografové často používají termín *otevřená abeceda* pro abecedu původního textu a *šifrová abeceda* pro znaky, jimiž je tvořen šifrovaný text. Když umístíme otevřenou abecedu nad šifrovou, jak je to vidět na obrázku 3, je zřejmé, že se od sebe liší posunutím o tři pozice, proto se této formě substituce říká *Caesarova posunová šifra* nebo jen Caesarova šifra. Každou kryptografickou substituci, v níž se písmeno nahrazuje jiným písmenem či symbolem, nazýváme šifra.

Suetonius se zmiňuje pouze o posunu o tři písmena, je však jasné, že lze použít posun o jakýkoli počet znaků od 1 do 25 a vytvořit tak 25 odlišných šifer. Kromě toho se nemusíme omezovat jen na posun abecedy. Její znaky můžeme seřadit libovolným způsobem, čímž se počet možných šifer významně zvýší. Existuje více než 400 000 000 000 000 000 000 000 000 takových uspořádání a tedy stejný počet možných šifer.

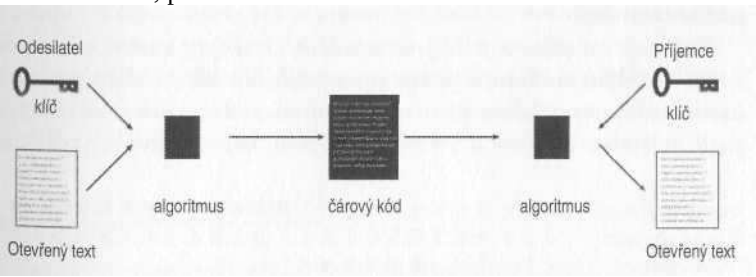
Otevřená abeceda	abcdefghijklmnopqrstuvwxyz
šifrová abeceda	DEFGHIJKLMNOPQRSTUVWXYZABC
Otevřený text	Veni, Vidi, Vici
šifrovýtext	YHQL. YLGL. YLFL

Obrázek 3: Aplikace Caesarovy šifry na krátkou zprávu. Caesarova šifra využívá šifrovou abecedu, jež se vytvoří z otevřené abecedy posunem o určitý počet míst -v tomto případě o tři. V kryptografii existuje konvence zapisovat znaky otevřené abecedy malými a znaky šifrové abecedy velkými písmeny. Podobné se původní zpráva - otevřený text - píše malými písmeny, zatímco zašifrovaná zpráva - šifrový text - velkými.

Každou šifru můžeme popsat pomocí obecné šifrovací metody, jíž říkáme *algoritmus*, a pomocí *klíče*, který specifikuje detaily použitého šifrování. V případě, o němž nyní mluvíme, spočívá algoritmus v náhradě každého z písmen otevřené abecedy písmenem šifrové abecedy, přičemž šifrová abeceda smí obecně sestávat z jakýchkoli variací abecedy otevřené. Klíč definuje přesné uspořádání šifrové abecedy. Vztah mezi algoritmem a klíčem je patrný z obrázku 4.

Padne-li nepříteli do rukou šifrový text, může se stát, že dokáže odhadnout, jaký algoritmus byl použit, avšak nebude znát klíč. Nepřítel se může například domnívat, že každé písmeno otevřeného textu bylo nahrazeno jiným písmenem

šifrové abecedy, ale nebude vědět, o jakou šifrovou abecedu jde. Je-li klíč spolehlivě střežen, pak



Obrázek 4: Když chce odesilatel zašifrovat zprávu, použije šifrovací algoritmus. Algoritmus je obecný popis šifrovacího systému a musí být konkrétně specifikován pomocí klíče. Výsledkem aplikace klíče a algoritmu na otevřený text je zašifrovaná zpráva - šifrový text. Pokud jej zachytí nepřítel, nedokáže zprávu dešifrovat. Příjemce, který zná jak algoritmus, tak klíč, však může šifrový text převést zpět na otevřený a zprávu si přečíst.nepřítel nemůže zachycenou zprávu dešifrovat. Význam klíče -ve srovnání s algoritmem - je základním principem kryptografie. V roce 1883 jej velmi výstižně shrnul nizozemský lingvista Auguste Kerckhoffs von Nieuwenhof ve své knize *La cryptographie militaire* (Vojenská kryptografie): „Kerckhoffsův princip: bezpečnost šifrovacího systému nesmí záviset na utajení algoritmu, pouze na utajení klíče."

Kromě utajení klíče je důležité, aby šifrovací systém disponoval širokým rozsahem potenciálních klíčů. Pokud například odesilatel použije Caesarovu šifru, jde o poměrně slabé šifrování, protože potenciálních klíčů je pouze 25. Z hlediska nepřítele je v takovém případě zapotřebí prozkoumat jen 25 možností. Pokud však odesilatel použije obecnější substituční algoritmus, který umožňuje přeskupit otevřenou abecedu do šifrové libovolným způsobem, je na výběr rázem 400 000 000 000 000 000 000 000 000 možných klíčů. Jeden z nich znázorňuje obrázek 5. Nepřítel pak stojí před nepředstavitelným úkolem vyzkoušet všechny myslitelné klíče. Kdyby dokázal prověřit jeden za vteřinu, trvalo by mu prověření všech možností miliardkrát déle, než je dnes odhadovaná doba existence vesmíru.

Krása tohoto typu šifer spočívá v tom, že se snadno používají a přitom poskytují vysoký stupeň bezpečnosti. Odesilatel může snadno definovat klíč, který je tvořen pouze jiným pořadím znaků abecedy, zatímco nepřítel v podstatě nemůže šifru vyluštit tzv. hrubou silou. Jednoduchost klíče je podstatná, protože odesilatel a příjemce jej musejí sdílet, a čím je klíč jednodušší, tím nižší je riziko nedorozumění.

Existuje i možnost ještě jednoduššího klíče, pokud se odesilatel smíří s malým snížením počtu potenciálních klíčů. Namísto zcela náhodného uspořádání písmen šifrové abecedy zvolí v takovém případě odesilatel *klíčové slovo* nebo *klíčovou frázi*- Máme-li například

Otevřená abeceda abcdefghi j kl mnopq rstuvwxyz
Šifrová abeceda JLPAWIQBCTRZYDSKEGFXHUONVM
Otevřený text e t t u, brute?
Šifrovýtext WX XH, LGHXW?

Obrázek 5: Příklad obecného substitučního algoritmu, v němž se každé písmeno otevřeného textu nahradí jiným písmenem podle klíče. Klíčem je šifrová abeceda -obecně jakékoli přeuspořádání otevřené abecedy.

užít klíčovou frázi JULIUS CAESAR, začneme odstraněním mezer mezi slovy a opakujících se písmen. Dostaneme JULISCAER. Tuto posloupnost znaků pak použijeme jako začátek šifrové abecedy. Zbytek šifrové abecedy je tvořen zbylými abecedními znaky v normálním pořadí. Bude tedy vypadat takto:

Otevřená abeceda abcdefghi jklmnopqrstuvwxyz šifrová abeceda JULISCAERTVWXYZBDFGHKMNOPQ

Výhodou je, že se klíčové slovo či fráze dá snadno zapamatovat a je jimi dán i celý zbytek abecedy. To je důležitá vlastnost - pokud musí odesilatel uchovávat šifrovou abecedu na papíře, je tu vždy riziko, že se jej zmocní nepřítel a utajenou komunikaci přečte. Dá-li se klíč zapamatovat, je nebezpečí menší. Počet šifrových abeced generovaných pomocí klíčových slov a frází je samozřejmě menší než počet abeced vytvářených bez všech omezení, jejich množství je však pořád značné - a postačující k tomu, aby útok hrubou silou neměl naději.

Díky této jednoduchosti a síle dominovala substituční šifra tajné komunikaci po celé první tisíciletí našeho letopočtu. Systém byl natolik bezpečný, že neexistovala motivace k jeho dalšímu zdokonalování. Před potenciálními luštiteli šifer naopak stála výzva. Existuje nějaký způsob, jak zachycenou šifrovanou zprávu rozluštit? Mnoho starověkých vědců bylo přesvědčeno, že substituční šifra je kvůli obrovskému množství možných klíčů nerozluštitel-ná, a po staletí se to potvrzovalo jako nezvratná pravda. Luštitelé šifer však nakonec našli zkratku, jak se bez testování všech klíčů obejít. Našli způsob, jak namísto miliard let vystačit s několika minutami. Tento průlom, ke kterému došlo na Východě, vyžadoval unikátní kombinaci lingvistiky, statistiky a náboženského zanícení.

Arabští kryptoanalytici

Ve věku kolem čtyřiceti let začal Muhammad pravidelně navštěvovat osamělou jeskyni na hoře Hirá poblíž Mekky. Bylo to jeho soukromé útočiště, místo pro motlitbu, meditaci a rozjímání. Během jednoho hlubokého přemítání, které se datuje někdy kolem roku 610, ho navštívil archanděl Gabriel, jenž se mu představil jako poselBožího. Tím začala řada zjevení, jež pokračovala až do Muhammadovy smrti o dvacet let později. Zjevení byla písemně zaznamenávána ještě za Prorokova života, avšak jen jako útržky. Teprve Abú Bakr, první chalífa islámu, je uspořádal do souvislého textu. V jeho práci pokračoval druhý chalífa Umar se svou dcerou Hafsou a definitivně ji dokončil třetí chalífa Uthmán. Každé zjevení se stalo jednou ze 114 kapitol *Koránu.*

Vládnoucí chalífa nesl odpovědnost za pokračování práce Prorokovy, za obhajobu jeho učení a šíření slova Božího. Od roku 632, kdy se chalífou stal Abú Bakr, do smrti čtvrtého chalífy Alího v roce 661 se islám rozšířil do poloviny tehdy známého světa. Po dalším století postupné konsolidace se roku 750 ujal moci abbásovský cha-lífát. Tím začal zlatý věk islámské civilizace. Věda a umění se rozvíjely stejnou měrou. Islámští řemeslníci nám zanechali nádherné obrazy, zdobné plastiky a nejskvělejší výšivky, jaké kdy kdo stvořil, zatímco odkaz islámských vědců je patrný už jen z množství arabských slov, jež patří do lexikonu moderní vědy - jako například *algebra, alkohol* či *zenit.*

Bohatství arabské kultury vzniklo především díky tomu, že islámská společnost byla bohatá a mírumilovná. Abbásovští cha-lífové se o dobývání nových území starali méně než jejich předchůdci. Namísto toho soustředili svou pozornost na vytvoření organizované společnosti, v níž vládla hojnost. Nízké daně umožnily obchodníkům prosperovat, řemesla vzkvétala. Přísné zákony zas omezily korupci a

chránily občany před násilím. Protože fungování státu záviselo na účinné správě, potřebovali jeho úředníci bezpečný komunikační systém; ten získali pomocí šifer. Je doloženo, že šiframi se chránily nejen citlivé státní záležitosti, ale například i daňové záznamy. To dokazuje, že šifrovací techniky byly zcela běžné a značně rozšířené. Další důkazy lze získat z dobových úředních předpisů, jako například z knihy *Adab al-Kuttdb* (Příručka úředníkova), která pochází z 10. století a obsahuje pasáže věnované šifrám.

Arabští úředníci zpravidla používali šifrovou abecedu, jež vznikla prostým přeuspořádáním otevřené abecedy, jak jsem se o tom zmínil již dříve. Někdy také používali šifrovou abecedu s jinými symboly. Například a z otevřené abecedy mohlo být nahrazeno znakem # v šifrové abecedě, namísto b se psalo znaménko + a tak dále. Taková substituční šifra, v níž je šifrová abeceda tvořena písmeny,

symboly nebo jejich směsí, se nazývá *monoalfabetickd substituční šifra*. Všechny substituční šifry, o nichž jsme zatím mluvili, spadají do této kategorie.

Kdyby Arabové dokázali na poli kryptografie jen to, že byli schopni vytvářet monoalfabetické substituční šifry, stěží by si zasloužili významnější zmínku v dějinách kryptografie. Avšak skutečnost je jiná: kromě znalosti použití šifer věděli arabští učenci také, jak je luštit. V podstatě tak vynalezli *kryptoanalýzu*, tedy nauku, jak dešifrovat zprávu bez znalosti klíče. Zatímco kryptograf hledá nové metody utajení zpráv, kryptoanalytik útočí na slabá místa takových metod ve snaze utajené zprávy přečíst. Arabským kryptoanalytikům se podařilo objevit metodu, jak zlomit monoal-fabetickou substituční šifru, jež byla zcela bezpečná po několik století.

Kryptoanalýza mohla vzniknout až ve chvíli, kdy společnost dosáhla dostatečně vysoké úrovně v několika disciplínách, k nimž patří matematika, statistika a lingvistika. Islámská civilizace byla ideální kolébkou kryptoanalýzy, neboť islám vyžaduje dosažení spravedlnosti ve všech oblastech lidské aktivity, k tomu jsou nezbytné znalosti, tzv. il*m*. K úlohám každého muslima patří rozvíjet své znalosti ve všech oblastech. Ekonomický úspěch abbásovského chalífátu vedl k tomu, že učenci měli dostatek času, prostředků a dalších zdrojů, aby tuto svou povinnost mohli plnit. Snažili se převzít znalosti předchozích civilizací. Překládali egyptské, babylonské, indické, čínské, perské, syrské, arménské, hebrejské a latinské texty do arabštiny. Chalífa al-Mamún založil roku 815 v Bagdádu tzv. Bait al-Hikmá (Dům moudrosti) - knihovnu a překladatelské centrum.

Islámská civilizace byla schopna nejen znalosti shromažďovat, ale rovněž je dále šířit - díky tomu, že od Číňanů převzala technologii výroby papíru. Tak vnikla nová profese *warraqín* neboli „ten, kdo pracuje s papírem" - jakási kopírka v lidské podobě, opisovač rukopisů, který zásoboval rychle se rozvíjející trh s publikacemi. Ve vrcholném období produkovala arabská civilizace desítky tisíc knih ročně; v jediném předměstí Bagdádu se nacházelo přes sto knihkupectví. Vedle klasických textů jako příběhy *Tisíc a jedna noc* se v takových knihkupectvích našla díla *zabývající* se každou myslitelnou oblastí poznání, čímž se udržovala v chodu tehdy nejvzdělanější a nejvíce sečtělá společnost světa.Vynález kryptoanalýzy souvisel nejen s rozvojem světských nauk, ale rovněž s růstem náboženské vzdělanosti. V Basře, Kúře a Bagdádu se nacházely hlavní teologické školy, kde se zkoumala Mu-

hammadova zjevení shrnutá v *Koránu*. K předmětům zájmu teologů patřilo seřadit je do chronologické posloupnosti, čehož docílili například průzkumem četnosti slov v textech jednotlivých zjevení. Vycházeli z předpokladu, že některá slova se vyvinula poměrně nedávno, takže pokud určité zjevení taková slova obsahuje, je potom mladší než ostatní. Teologové rovněž studovali h*adíth* - souhrn Prorokových proslovů. Snažili se dokázat, že všechny jeho části lze skutečně právem připsat Muhammadovi. Proto studovali etymologii jednotlivých slov a strukturu vět, aby ověřili, zda texty mají stejnou lingvistickou strukturu jako ty, u nichž je Prorokovo autorství pokládáno za nezvratné.

Je důležité, že teologové se přitom nezastavili na úrovni jednotlivých slov. Zkoumali i jednotlivá písmena a povšimli si jejich rozdílné relativní četnosti. Písmena a al jsou v arabštině nejběžnější, částečně proto, že tvoří určitý člen al-, zatímco písmeno j se objevuje desetkrát méně. Toto na první pohled bezúčelné pozorování vedlo k prvnímu velkému průlomu v kryptoanalýze.

Není známo, kdo jako první pochopil, že četnosti jednotlivých písmen lze využít k luštění šifer. První známý popis této techniky však pochází od učence z 9. století, jehož plné jméno znělo Abú Ju-súf Jaqúb ibn Isháq ibn as-Sabbáh ibn 'omrán ibn Ismail al-Kindí, známý jako „filozof Arabů". Je autorem 290 knih o lékařství, astronomii, matematice, jazykovědě a hudbě. Jeho největší pojednání, znovuobjevené teprve roku 1987 v Sulajmanově osmanském archivu v Istanbulu, se nazývá *Rukopis o dešifrování kryptograftckých zpráv*, jehož titulní stranu vidíte na obrázku 6. Přestože rukopis obsahuje podrobnou analýzu statistiky, arabské fonetiky a syntaxe, popsal al-Kindí celý svůj revoluční systém ve dvou stručných odstavcích:

‚Jedním ze způsobů, kterak rozluštit šifrovanou zprávu, známe-lí její jazyk, je nalézt odlišný otevřený text v tomtéž jazyce, dlouhý alespoň na arch papíru či podobně, a spočítat výskyty jednotlivých písmen v něm. Nejčastější písmeno nazveme pak „prvním", druhé nejčastější „druhým", další „třetím" a tak dále, dokud je nepojmenujeme všechna.Pak pohlédneme na šifrovaný text, jenž chceme rozluštit, a rovněž sečteme výskyty symbolů. Najdeme nejčastější symbol a zaměníme jej písmenem označeným jako „první" ze vzorku otevřeného textu. Druhý nejčastější symbol pak nahradíme písmenem „druhým", následující „třetím" a tak dále, dokud všechny symboly nezaměníme za písmena."

Vysvětlení snáze pochopíme na běžné anglické abecedě. Nejprve musíme prostudovat delší úsek běžného anglického textu, možná několik různých textů, abychom zjistili frekvenci výskytu každé hlásky. V angličtině se nejčastěji vyskytuje hláska e, následuje t, pak a - a tak dále (viz tabulka 1). V dalším kroku prozkoumáme šifrový text a stanovíme četnost výskytu jeho hlásek. Pokud se v něm jako nejčastější symbol vyskytuje například J, pak je velmi pravděpodobné, že toto písmeno nahrazuje hlásku e. Pokud je druhým nejčastějším symbolem v šifrovém textu P, pak jde pravděpodobně o náhradu za t - a tak dále. Technika popsaná al-Kindím, známá dnes jako *frekvenční analýza*, ukazuje, že není třeba zkoušet každý klíč z miliard možných. Namísto toho lze zjistit obsah zašifrovaného textu jednoduchou analýzou četnosti znaků v šifrovém textu.

Na druhou stranu nelze tuto techniku používat zcela mechanicky, protože seznam frekvencí hlásek v tabulce 1 představuje průměr

Znak	Četnost	Znak	Četnost
a	8,2	n	6,7
b	1,5	o	7,5
c	2,8	P	1,9
d	4,3	q	0,1
e	12,7	r	6,0
f	2,2	s	6,3
g	2,0	t	9,1
h	6,1	u	2,8
1	7,0	v	1,0
j	0,2	w	2,4
k	0,8	x	0,2
1	4,0	y	2,0
m	2,4	z	0,1

Tabulka 1: Tato tabulka relativních četností je založena na úsecích anglického textu z novin a beletrie. Výchozí vzorek obsahoval celkem 100 365 znaků anglické abecedy. Tabulku sestavili H. Beker a F. Piper, původně byla publikována v knize *Cipber Systems: The Protection of Communication* (Šifrovací systémy: ochrana komunikace).

a neodpovídá zcela přesně poměrům v každém možném textu. Tak například, krátká zpráva o vlivu atmosférických poměrů na chování pruhovaných čtyrnožců v Africe nebude přímočarou frekvenční analýzou snadno řešitelná: „From Zanzibar to Zambia and Zaire, ozone zones make zebras run zaný zigzags." („Od Zanzibaru až po Zambii a Zaire běhají zebry bláznivě cikcak kvůli ozónovým zónám.") Obecně se dá říci, že u kratších textů je pravděpodobnější, že se jejich frekvence hlásek liší od standardní. Pokud jde o méně než sto písmen, bývá dešifrování velmi obtížné. Delší texty zpravidla odpovídají standardnímu rozložení frekvencí, i když výjimky také existují. Francouzský spisovatel Georges Perec napsal roku 1969 dvousetstránkovou novelu *La disparition* (Zmizení), která nepoužívá slova obsahujících hlásku e. Anglický spisovatel a kritik Gilbert Adair dokázal přeložit Perecův text do angličtiny se zachováním původního principu - obešel se bez hlásky e. Adairův překlad nazvaný *A Void* (Prázdnota) je překvapivě čtivý (viz příloha A). Kdyby byla celá tato kniha zašifrována monoalfabetickou substituční šifrou, pak by naivní pokus o dešifrování ztroskotal na úplné nepřítomnosti jinak nejčastější hlásky anglické abecedy.

Když jsme nyní popsali první nástroj kryptoanalýzy, budu pokračovat příkladem jeho využití. V textu jsem vás nechtěl zatěžovat příliš mnoha příklady, u frekvenční analýzy však učiním výjimku - částečně proto, že technika je snazší, než vypadá, a částečně proto, že jde o nejzákladnější nástroj kryptoanalytika. Následující příklad navíc poskytuje obrázek o způsobu kryptoanalytikovy práce. Přestože je frekvenční *Analýza* postavena především na logické úvaze, příklad nám ukáže, že kryptoanalytik se neobejde také bez intuice, pružnosti, odhadu a jisté lstivosti.

Luštění šifry

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL. QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS. KXUYPD: „DJOXL EYPD. ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?" OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLKPředstavte si, že se nám podařilo zachytit tuto šifrovanou zprávu. Naším úkolem je rozluštit ji. Víme, že text je v angličtině a že byl zašifrován monoalfabetickou substituční šifrou, o klíči však nemáme ani ponětí. Zkoušet všechny možné klíče je nepraktické, takže je třeba nasadit frekvenční analýzu. Dále se krok za krokem podíváme na luštění šifry, pokud se vám však zdá, že víte, jak na to, můžete příklad přeskočit a pokusit se o vyluštění sami.

Bezprostřední reakcí každého kryptoanalytika, který dostane do ruky podobný šifrový text, je zjistit četnost jednotlivých písmen, což vede k výsledkům zapsaným v tabulce 2. Není žádným překvapením, že četnost jednotlivých znaků je rozdílná. Otázka zní: Dokážeme identifikovat podle těchto četností jejich význam? Šifrový text je poměrně krátký, takže frekvenční analýzu nelze uplatnit mechanicky. Bylo by naivní předpokládat, že nejčastější znak šifrového textu 0 odpovídá nejčastější hlásce anglické abecedy e nebo že osmý nejčastější znak šifrového textu Y reprezentuje h, osmé nejčastější písmeno anglické abecedy. Otrockým použitím frekvenční analýzy by vznikl nesmysl. První slovo šifry, jímž je PCQ, bychom například vyluštili jako a o v.

Můžeme však začít tím, že soustředíme svou pozornost jen na tři znaky, jež se v šifrovém textu vyskytují více než třicetkrát. Jde o pís-

Znak	Frekvence	
	Počet výskytů	V procentech
A	3	0,9
B	25	7,4
C	27	8,0
D	14	4,1
E	5	1,5
F	2	0,6
G	1	0,3
H	0	0,0
I	11	3,3
J	18	5,3
K	26	7,7
L	25	7,4
M	11	3,3

Znak	Frekvence	
	Počet výskytů	V procentech
N	3	0,9
0	38	11,2
P	31	9,2
Q	2	0,6

R	6	1,8
S	7	2,1
T	0	0,0
U	6	1,8
V	18	5,3
W	1	0,3
X	34	10,1
Y	19	5,6
Z	5	1,5

Tabulka 2; Frekvenční analýza zašifrované zprávy.

mena 0, X a P. S poměrně značnou jistotou můžeme předpokládat, že nejběžnější *znaky* šifrového textu odpovídají nejběžnějším znakům anglické abecedy, i když ne nutné v odpovídajícím pořadí. Jinými slovy, nemůžeme si být jisti, že 0 = e, X = t a P = a, ale můžeme předběžně odhadnout, že

0 = e,t nebo a, X = e, t nebo a, P = e, t nebo a.

Chceme-li pokračovat s rozumnou mírou jistoty a zjistit identitu tří nejčastěji se vyskytujících písmen 0, X a P, potřebujeme jemnější formu frekvenční *analýzy*. Namísto pouhého sčítání četností výskytu se podíváme, jak často se jednotlivá písmena vyskytují v sousedství jiných. Například: sousedí písmeno 0 s mnoha různými písmeny, nebo je jeho výskyt vázán na několik konkrétních písmen? Odpověď na tuto otázku nám napoví, zda 0 reprezentuje samohlásku či souhlásku. Pokud jde o samohlásku, bude se pravděpodobně vyskytovat vedle většiny ostatních písmen, je-li to souhláska, bude se většině ostatních písmen vyhýbat. Například písmeno e se může v angličtině vyskytnout prakticky vedle každé jiné hlásky, zatímco písmeno t se sotva najde v kombinaci s b, d, g, j, k, m, q či v.

Níže uvedená tabulka si všímá tří nejčastěji se vyskytujících písmen 0, X a P a shrnuje, jak často je nalezneme před jiným písmenem či po něm. Například 0 se vyskytuje před A jednou, po něm nikdy, takže první políčko tabulky má hodnotu 1. Písmeno 0 nalezneme v sousedství většiny jiných hlásek, zcela se vyhnulo jen sedmi, takže v prvním řádku tabulky je sedm nul. Písmeno X je rovněž „společenské", druží se s většinou jiných písmen a vyhnulo se jen osmi z nich. Písmeno P je daleko méně přátelské. Páruje se pouze s několika málo jinými písmeny, patnácti se zcela vyhnulo. Zdá se, že 0 a X reprezentují samohlásky, zatímco P souhlásku.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ    0    1    9    0    3    1110
146012280410030112 X 0 7 0 11110 2 4 6 3 0 3 19 0 2 40332001
P 10 5 6 0 0 0 0 0 112 2 0 8 0 0 0 0 0 0110 9 9 0
```

Nyní je třeba zjistit, které samohlásky se skrývají pod 0 a X. Pravděpodobně jde o hlásky e a a, nejběžnější anglické samohlásky, ale platí, že 0 = e a X = a, nebo je tomu naopak? K zajímavým vlastnostem šifrového textu patří to, že 00 v něm nalezneme dvakrát, zatím-co XX ani jednou. V angličtině se kombinace ee vyskytuje mnohem častěji než a a, takže je pravděpodobné, že 0 = e a X=a.

V tuto chvíli jsme již spolehlivě identifikovali dvě z písmen šifrového textu. Náš závěr, že X = a, je dále podpořen skutečností, že X se objevuje v šifrovém textu samostatně; slovo a (neurčitý člen) je jedním z pouhých dvou anglických slov tvořených jediným písmenem. Jediné další písmeno, jež se v šifrovém textu vyskytuje samostatně, je Y, takže se zdá být velmi pravděpodobné, že reprezentuje jediné další jednopísmenné anglické slovo

I (osobní zájmeno „já"). Soustředění na jednopísmenná slova patří ke standardním kryptoanalytickým trikům, viz jejich seznam v příloze B. Dá se však použít jen tehdy, pokud šifrový text obsahuje mezery mezi slovy. Kryptograf je často odstraní, aby nepříteli ztížil analýzu.

Následující trik lze však použít bez ohledu na to, zda mezery mezi slovy máme či nikoli. Spočívá v odhalení písmene h, pokud jsme předtím již identifikovali písmeno e. Pro angličtinu je typický výskyt h před e (jako ve slovech the, then, they apod.), velmi vzácně se však h vyskytuje po e. Následující tabulka ukazuje, jak často se písmeno 0, o němž se domníváme, že reprezentuje e, vyskytuje před jinými znaky v šifrovém textu a jak často po nich. Z tabulky můžeme tedy odvodit, že písmeno B reprezentuje pravděpodobně h, protože před 0 se vyskytuje devětkrát, zatímco po něm ani jednou. Žádné jiné písmeno nemá vůči 0 tak asymetrický vztah.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ          po          0
10010100104000250000020100          před        8
09021010042012230410010012
```

Každé písmeno anglické abecedy má svou individualitu, danou jak jeho frekvencí, tak vztahem k jiným písmenům. Tato individualita umožňuje nalézt jeho skutečnou identitu, i když je skryta pomocí monoalfabetické substituční šifry.

Nyní jsme již spolehlivě určili čtyři písmena 0 = e, X = a, Y = i a B = h a můžeme začít nahrazovat šifrový text jeho ekvivalenty. Nadále se budu držet konvence, podle níž se znaky šifrového textu zapisují velkými a znaky otevřeného textu malými písmeny. To nám pomůže rozlišit mezi písmeny, jež teprve máme vyluštit, a těmi, jejichž identitu již známe.

PCQ VMJiPD LhiK L1Se KhahJaWaV haV ZCJPe E1PD KhahJiUaJ LhJee KCPK. CP Lhe LhCMKaPV aPV IiJKL PiDhL, QheP Khe haV ePVeV Lhe LaRe CI Sa'aJMI, Khe JCKe aPV EiKKev Lhe DJCMPV ZelCJe hiS, KaUiPD: „DJeaL E1PD, ICJ a LhCMKaPV aPV CPe PiDhLK i haNe ZeeP JeACMPLiPD LC UCM Lhe IaZReK CI FaKL aDeK aPV Lhe ReDePVK CI aPAiePL EiPDK. SaU i SaEe KC ZCRV aK LC AJaNe a IaNCMJ CI UCMJ SaGeKLU?"

eFiRCDMe, LaReK IJCS Lhe LhCMKaPV aPV CPe PiDhLK

Tímto jednoduchým krokem můžeme identifikovat několik dalších písmen, protože nyní již lze hádat slova. Nejběžnější anglická třípísmenná slova jsou the a and. V šifrovém textu je můžeme poměrně snadno určit - Lhe se vyskytuje šestkrát, a PV pětkrát. Takže L reprezentuje pravděpodobně t, P zastupuje n a V stojí namísto d. Teď tedy můžeme v nahrazování znaků šifrového textu pokračovat:

nCQ dMJinD thiK tiSe KhahJaWad had ZCJne EinD KhahJiUaJ thJee KCnK. Cn the thCMKand and IiJKt niDht. Qhen Khe had ended the taRe CI Sa'aJMI. Khe JCKe and EiKKed the DJCMnd ZelCJe hiS. KaUinD: „DJeat EinD. ICJ a thCMKand and Cne niDhtK i haNe Zeen JeACMntinD tC UCM the IaZReK CI FaKt aDeK and the ReDendK CI anAient EinDK. SaU i SaEe KC ZCRd aK tC AJaNe a IaNCMJ CI UCMJ SaGeKtU?"

eFiRCDMe, taReK IJCS the thCMKand and Cne niDhtK

Jakmile známe s jistotou několik písmen, postupuje kryptoana-lýza velmi rychle. Tak například slovo na konci druhé věty zní Cn. Každé anglické slovo obsahuje samohlásku, takže C musí být samohláska. Zbývá identifikovat jen dvě samohlásky u a o; u se nehodí*, takže C musí reprezentovat o. V šifrovém textu nalezneme také slovo Khe, což znamená, že K představuje buď t, nebo s. Již však víme, že L= t, takže je jasné, že K= s. Tato písmena vložíme do šifrového textu a objeví se slovní spojení thoMsand and one niDhts. Lze předpokládat, že jde o výraz thousand and one nights (tisíc a jedna noc), takže je pravděpodobné, že poslední řádek říká, že jde o úryvek

* Slovo „un" totiž v angličtině neexistuje, slovo „on" je předložka „na". Slovo „the" Je určitý člen, slovo „she" osobní zájmeno „ona", jiná třípísmenná slova končící na »he" neexistují.

z příběhů *Tisíc a jedna noc.* Z toho plyne, že M = u, I = f, J = r, D = g,

R = 1 aS=m.

Stejným způsobem bychom mohli pokračovat a uhodnout i zbytek slov, namísto toho se však podíváme, co již víme o šifrové a otevřené abecedě. Tyto dvě abecedy tvoří klíč a byly použity, když kryptograf šifroval zprávu. Stanovením významu jednotlivých písmen šifrového textu jsme vlastně určovali, jak vypadá šifrová abeceda. Souhrn našich dosavadních zjištění je obsažen v následujícím schématu: Otevřená abeceda abcdefghijklmnopqrstuvwxy z

Šifrováabeceda X--VOIDBY--RSPC--JKLM--------- Když se na schéma podíváme, můžeme naši kryptoanalýzu dokončit. Sekvence VOIDBY v šifrové abecedě naznačuje, že kryptograf použil jako základ klíče frázi. S trochou přemýšlení lze odhadnout, že fráze by mohla znít A VOID BYGEORGES PEREC, což se po odstranění mezer mezi slovy a opakujících se písmen zkrátí na AVOIDBYGERSPC. Pak už následují písmena v normálním abecedním pořadí, ovšem s výjimkou těch, která se vyskytují v klíčové frázi. Kryptograf použil méně obvyklý postup a neumístil klíčovou frázi na samý začátek šifrové abecedy, ale až od čtvrtého písmene. Učinil tak patrně proto, že klíčová fráze začíná písmenem A, takže by se museloo kódovat A = a. Jakmile jsme takto stanovili celou šifrovou abecedu, můžeme dokončit luštění textu. Kryptoanalýza je hotova: Otevřená abeceda abcdefghijklmnopqrstuvwxyz Šifrová abeceda XZAVOIDBYGERSPCFHJKLMNQTUW Now during this time Shahrazaď had borne King Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: „Great King, for a thousand and one nights I háve been recounting to you the fables of past ages and the legends of ancient kings. May I make so boid as to crave a favor of your majesty?" EpHogue, *Tales from the Thousand and One Nights*

Renesance na Západě

Mezi lety 800 a 1200 n. 1. prožívali Arabové období horečného rozvoje vzdělanosti a dosahovali významných intelektuálních úspěchů. V téže době uvízla

Evropa v temnotě. V době, kdy al-Kindí popisoval vynález kryptoanalýzy, Evropané se dosud potýkali se *základy* samotné kryptografie. Jedinými evropskými institucemi, kde se pracovalo na tajných písmech, byly kláštery, jejichž mniši studovali *Bibli* ve snaze odkrýt v jejím textu utajené významy - což je fascinace, která přetrvala i do moderní doby (viz příloha C).

Středověké mnichy přitahovala skutečnost, že Starý zákon obsahuje záměrné a očividné ukázky kryptografie. Dají se v něm například nalézt úseky textu šifrované tradiční hebrejskou substituční šifrou *atbaš.* Ta spočívá v tom, že se vezme písmeno, spočítá se, jak je vzdáleno od začátku abecedy, a nahradí se písmenem, které se nachází v téže vzdálenosti od konce abecedy. V angličtině by to znamenalo, že písmeno a se nahradí za Z, písmeno b za Y a tak dále. Sám název šifry *atbaš* napovídá, jak systém funguje, protože se skládá (ATBŠ) z prvního písmene hebrejské abecedy *(alef),* po němž následuje poslední *(tav),* poté druhé písmeno *(bet)* a nakonec předposlední *(šin).* Příklad šifry atbaš najdeme v knize Jeremjáš 25, 26 a 51, 41, kde namísto slova „Babel" (Babylon, v hebrejském zápisu BBL) najdeme „Šéšak". Písmeno *bet,* první písmeno slova Babel, je nahrazeno písmenem š*in,* tedy druhé písmeno v abecedě předposledním písmenem. Druhou souhláskou slova Babel je rovněž *bet,* takže se opět nahradí písmenem *šin.* Třetí souhláska slova Babel *lamed* je v hebrejské abecedě dvanáctá, nahradí se tedy hláskou dvanáctou od konce, což je *kaf.*

Atbaš a jiné biblické šifry měly patrně za úkol pouze navodit atmosféru tajemství, nikoli zakrýt význam. Stačily však na to, aby zažehly jiskru zájmu o seriózní kryptografii. Evropští mniši začali znovu objevovat staré substituční šifry, a tím se postarali o návrat kryptografie do západní civilizace. První evropskou knihu o kryptografii napsal ve 13. století anglický františkán a polyhistor Roger Bacon. Jeho *De secretis artis et naturae operibus etde nullitate magae* (List o tajných dovednostech a neexistenci magie) obsahuje popis sedmi metod, jak uchovat tajemství zpráv, a varuje: „Blázen je ten, kdo se-píše tajemství způsobem jiným než takovým, jenž jej chrání od nepovolaných."Ve 14. století se už kryptografie používala běžně. Zejména alchymisté a vědci s její pomocí udržovali v tajnosti své objevy. Geoffrey Chaucer, kterého známe spíše z literatury, byl rovněž astronomem a kryptografem - a dokonce autorem jedné z nejslavnějších starých evropských šifer. Ve svém díle *A Treatise on tbe Astrolabe* (Pojednání o astrolábu) uvedl několik dodatečných poznámek označených jako *The Equatorie ofthe Planetis* (O oběhu planet), v nichž je několik šifrovaných odstavců. Chaucerova šifra nahrazovala otevřený text symboly, například místo b psal 5. Šifrový text s podivnými symboly namísto písmen vypadá na první pohled komplikovaněji, ale je plně ekvivalentní tradiční náhradě písmen písmeny. Proces dešifrování a úroveň bezpečnosti se nijak nemění.

V 15. století byla již evropská kryptografie bouřlivě se rozvíjejícím oborem. Oživení věd, umění a vzdělanosti během renesance poskytlo nezbytné kapacity, zatímco rozvoj politických machinací vyvolal poptávku po utajení komunikace. Ideální prostředí pro kryptografii bylo především v Itálii. Ta byla jednak srdcem renesance, jednak mozaikou nezávislých městských států bojujících navzájem o

vliv a moc. Kvetla diplomacie, státy si vyměňovaly vyslance, kteří dostávali od svého vladaře dopisy s pokyny, jakou zahraniční politiku provozovat. Opačným směrem zas vyslanci posílali veškeré informace, jež se jim podařilo získat. Díky tomu vznikla značná poptávka po utajení komunikace v obou směrech. Každý stát si postupně zřídil šifrovou kancelář, každý vyslanec měl svého šifranta.

V téže době, kdy se kryptografie stala standardním diplomatickým nástrojem, se na Západě začala rozvíjet kryptoanalýza. Diplomaté se sotva stihli seznámit s uměním utajení zpráv a už tu byli protihráči usilující o prolomení této bezpečnosti. Je poměrně pravděpodobné, že kryptoanalýza byla v Evropě objevena nezávisle, současně však existuje možnost, že byla přenesena z arabského světa. Islámské objevy v matematice a vědách vůbec měly značný vliv na znovuzrození vědy v Evropě, kryptoanalýza tedy mohla být mezi importovanými naukami.

Bezpochyby prvním velkým evropským kryptoanalytikem byl Giovanni Soro, od roku 1506 tajemník pro šifry v Benátské republice. Sorův věhlas se šířil po celé Itálii, proto zasílaly spřátelené státy zachycené depeše do Benátek k rozluštění. Dokonce i Vatikán, tehdy zřejmě druhé nejdůležitější centrum kryptoanalýzy, zasílal Sorovi zdánlivě nerozluštitelné zprávy, jež padly jeho lidem do rukou. Papež Klement II. poslal Sorovi roku 1526 dvě šifrované zprávy; obě dostal zpět rozluštěny. Když jednu z papežových zpráv zachytili ve Florencii, papež poslal její kopii Sorovi v naději, že bude ujištěn o její nerozluštitelnosti. Soro skutečně potvrdil, že papežovu šifru rozluštit nedokáže, takže by se to nemělo podařit ani Florenťanům. Možná však šlo jen o taktický manévr, jehož cílem bylo vzbudit ve vatikánských kryptografech falešný pocit bezpečí - Soro patrně nestál o to, aby poukazoval na slabá místa papežských šifer, protože by tím přiměl Vatikán, aby vyměnil dosavadní systém za dokonalejší, který by už ani on sám nedokázal rozluštit.

Schopné kryptoanalytiky začaly zaměstnávat i jiné panovnické dvory v Evropě. Jedním z uznávaných byl Philibert Babou, kryptoa-nalytik francouzského krále Františka I. Babou si vydobyl reputaci svou nezdolnou výkonností, na rozluštění šifry totiž dovedl pracovat bez přestávky dnem i nocí. Král tak získal řadu příležitostí rozvíjet svůj dlouhodobý románek s analytikovou manželkou. Koncem 16. století dokázali Francouzi svou dovednost v kryptoanalýze především díky Francoisi Vietovi. Ten s obzvláštním potěšením luštil španělské šifry. Španělští kryptografové byli v porovnání se svými soupeři z jiných zemí Evropy poměrně naivní a nemohli uvěřit tomu, že jejich šifry jsou pro Francouze zcela průhledné. Španělský král Filip II. zašel dokonce tak daleko, že se obrátil na Vatikán a argumentoval, že Viete je určitě spolčen s ďáblem a měl by být povolán před kardinálský soud. Papež, který dobře věděl, že i jeho vlastní kryptoanalytici již léta čtou španělské šifry, žádost odmítl. Novinka se brzy rozšířila a španělští kryptografové se stali předmětem posměchu celé Evropy.

Španělské zahanbení bylo příznačné pro etapu charakterizovanou otevřeným bojem mezi kryptoanalytiky a kryptografy. Kryptografové tou dobou ještě stále spoléhali na monoalfabetickou substituční šifru, zatímco kryptoanalytici začínali k jejímu luštění užívat frekvenční analýzu. Ti, kdo sílu frekvenční analýzy dosud

neobjevili, věřili dál monoalfabetické substituci, aniž by si byli vědomi, jak snadno mohou Soro, Babou či Viete číst jejich šifry.

Země, jež si byly slabin monoalfabetické substituční šifry vědomy, se tehdy již snažily vyvinout lepší šifrování, jež by ochránilo jejich vlastní tajné komunikace před nepřítelem. Jedním z nejjednodušších zdokonalení monoalfabetické substituční šifry bylo zavede-ní tzv. *klamačů* či *nul,* tedy symbolů nebo písmen, jež nereprezentují písmena původního textu (jsou to vlastně bezvýznamné vsuvky). Například můžeme nahradit každé písmeno číslem od jedné do 99, takže - pokud vezmeme v úvahu, že anglická abeceda má 26 písmen - 73 čísel neodpovídá žádnému písmenu. Pokud je náhodně rozmístíme po šifrovém textu, a to s rozmanitou četností, ztížíme tím analýzu. Nuly (klamače) nebudou představovat pro příjemce zprávy žádný problém - ten je prostě bude ignorovat. Zmatou však nepřátelského kryptoanalytika, protože mu zkomplikují práci s frekvenční analýzou. Podobný účinek má záměrně špatný pravopis před zašifrováním zprávy, ponivač spúzobý zmnjenu f reqenze jednotHvíh hlázeg a kryptoanalytikovi se bude pracovat obtížněji, zatímco příjemce zprávu standardním způsobem dešifruje a pak už si nějak s pokrouceným, ale stále ještě čitelným pravopisem

poradí.

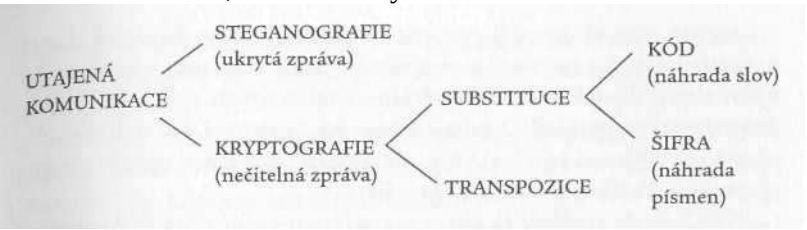
Jiný pokus, jak zdokonalit monoalfabetickou substituční šifru, spočíval v zavedení kódových slov. Pojem *kód* má v běžném jazyce velmi široký význam a často se používá obecně pro jakoukoli metodu utajené komunikace. Ve skutečnosti je však význam tohoto slova velmi specifický, jak jsem uvedl v úvodu, a týká se jen určitého způsobu substituce. Prozatím jsme hovořili o substitučních šifrách, kde se jedno písmeno nahrazuje jiným. Je však rovněž možné nahradit symboly na mnohem vyšší úrovni, například celá slova reprezentovat jinými slovy či symboly. Například:

zabít	= D	generál	= Σ	okamžitě	= 08
vydírat	= P	král	= Ω	dnes	= 73
zajmout	= J	ministr	= Ψ	večer	= 28
chránit	= Z	princ	= Θ	zítra	= 43

Otevřený text: Zabijte večer krále.
Šifrovaná zpráva: D-28-Ω.

Velmi zjednodušeně vzato je *kód* definován jako substituce na úrovni slov či frází, zatímco *šifra* je substitucí na úrovni písmen. Termín *zašifrovat* pak znamená zpracovat zprávu pomocí šifry, zatímco *zakódovat* značí použít kód. Podobně je tomu se slovy *dešifrovat* a *dekódovat.* Přehled těchto definicí přináší obrázek 7. Obecně se jich budu v textu knihy držet, ale pokud je význam zcela jasný, nebudu se bránit použití výrazů jako

„luštění kódu" ani tam, kde technicky



Obrázek 7: Nauka o utajené komunikaci a její hlavní podobory.

vzato jde o „luštění šifry" - druhý výraz je přesnější, první se však používá častěji.

Na první pohled se zdá, že kódy jsou bezpečnější než šifry, protože slova podléhají pravidlům frekvenční analýzy mnohem méně než písmena. Pro rozluštění monoalfabetické substituční šifry musíme identifikovat správný význam pouhých 26 znaků, kdežto při luštění kódu je třeba dobrat se významu stovek či tisíců slov. Když se však na kódy podíváme blíže, zjistíme, že v porovnání se šiframi trpí dvěma praktickými nedostatky. Jednak u šifry stačí, aby se odesilatel a příjemce dohodli na klíči, který definuje význam 26 znaků, a už si mohou vyměňovat libovolné zprávy. Má-li se dosáhnout stejné pružnosti u kódu, je třeba nejprve podstoupit obtížný proces definování kódového slova pro každé z tisíců slov, jež se mohou vyskytnout v otevřeném textu. Kódová kniha má pak stovky stránek a vypadá jako slovník. Sestavit ji je obtížné a nosit ji s sebou nepohodlné.

Za druhé, padne-li kódová kniha do rukou nepříteli, má to zdrcující důsledky. Veškerá utajená komunikace je mu rázem plně srozumitelná. Odesilatel a příjemce musí sestavit zcela novou kódovou knihu a tento objemný svazek je pak třeba doručit všem, kdo jsou zahrnuti v komunikační síti, například všem vyslancům dané země. Naproti tomu, odhalí-li nepřítel klíč substituční šifry, je poměrně snadné sestavit nový klíč, distribuovat jej a naučit se mu zpaměti.

Již v 16. století si byli kryptografové vědomi této nedokonalosti kódů, a proto raději spoléhali na šifry, případně na *nomenklátory.* Nomenklátor je kódovací systém, který vychází z šifrové abecedy, jež slouží k zašifrování většiny textu, je však doplněn o seznam kódových slov. Navzdory tomu není o mnoho bezpečnější než obyčejná šifra, protože většinu textu lze rozluštit frekvenční analýzou a *zbylá.* kódová slova pak uhodnout z kontextu.Stejně jako si dovedli poradit s nomenklátory, dokázali dobří kryptoanalytici pracovat i s pozměněným pravopisem a nulami. Jinými slovy, dovedli rozluštit většinu zachycených zpráv. Díky této dovednosti se podařilo rozluštit mnohá tajemství, jež ovlivňovala různá rozhodnutí jejich

vládců. Kryptoanalýza tak v nejednom vypjatém okamžiku ovlivnila dějiny Evropy.

Nikde jinde se důsledky kryptoanalýzy neprojevily tak dramaticky jako v případě Marie Stuartovny. Výsledek jejího procesu závisel plně na souboji mezi jejími kryptografy a kryptoanalytiky Alžběty I. Marie byla jednou z nejdůležitějších osobností 16. století - skotská a francouzská královna, která si dělala nárok na anglický trůn -a přesto o jejím osudu nakonec rozhodl kousek papíru se zprávou, přesněji řečeno to, zda se ji podaří rozluštit, či nikoli.

Babingtonovo spiknutí

24. listopadu 1542 porazila anglická vojska krále Jindřicha VIII. skotskou armádu v bitvě u Solway Moss. Jindřich se tak ocitl doslova před branami Skotska. Poražený skotský král Jakub V. se duševně i tělesně zhroutil a stáhl se na svůj hrad Falkland. Na nohy ho nepostavila ani zpráva o narození dcery Marie, k němuž došlo dva týdny po bitvě. Vypadalo to, jako by spíše jen čekal na tuto zvěst, aby mohl zemřít v míru, s vědomím, že učinil povinnosti zadost. Týden po Mariině narození Jakub V. zemřel ve věku pouhých třiceti let. Novorozená princezna se stala skotskou královnou Marií.

Marie se narodila předčasně, a proto zpočátku panovaly obavy, že dítě nepřežije. Na anglickém dvoře se říkalo, že Marie již zemřela, ale bylo to jen tamní zbožné přání - Angličané vítali každou zprávu, která by pomohla destabilizovat Skotsko. Marie rychle sílila a rostla. Ve věku devíti měsíců - 9. září 1543 - byla v kapli zámku Stirling korunována v přítomnosti tří nejvyšších šlechticů království, kteří ji symbolicky předali korunu, žezlo a meč.

Protože byla Marie ještě velmi malá, mohlo si Skotsko odech-nout od anglických nájezdů. Nepokládalo by se totiž za rytířské, kdyby Jindřich VIII. napadl zemi, jejíž král právě zemřel a jíž panovalo dítě. Namísto toho dal anglický král přednost tomu, aby si Marii předcházel v naději, že se podaří zařídit její sňatek s jeho synem Eduardem, čímž by se oba národy sjednotily pod vládou Tudorovců. Své intriky zahájil tím, že propustil skotské šlechtice zajaté u Solway Moss - ovšem pod podmínkou, že se zasadí o sjednocení s AngliíSkotský dvůr však Jindřichovu nabídku zamítl a dal přednost sňatku Marie s francouzským dauphinem (korunním princem) Františkem. Skotsko se tak rozhodlo pro spojenectví s jiným katolickým národem, což potěšilo Mariinu matku Marii Guiskou, jejíž vlastní manželství s Jakubem V. mělo sloužit především k upevnění vztahů mezi Skotskem a Francií. Jak Marie, tak František byli teprve děti, bylo však stanoveno, že se vezmou, František se stane francouzským králem, Marie

královnou, a tím se Skotsko sjednotí s Francií. Než se tak ale stane, měla Francie bránit Skotsko proti anglickým hrozbám.

Slib ochrany působil uklidňujícím dojmem, zejména tehdy, když Jindřich VIII. přešel od diplomacie k výhružkám ve snaze přesvědčit Skoty, že jeho vlastní syn je pro Marii Stuartovnu vhodnějším manželem. Jeho vojska se dopouštěla pirátství, ničila úrodu na polích, pálila vesnice a napadala města podél hranic. Tyto „drsné námluvy", jak se jim říká, pokračovaly i po Jindřichově smrti, k níž došlo roku 1547. Pod vedením jeho syna, krále Eduarda VI. (potenciálního ženicha) útoky vyvrcholily v bitvě u Pinkie Cleugh, do níž se již zapojila skotská armáda. Kvůli této situaci bylo rozhodnuto, že Marii bude bezpečněji ve Francii, mimo dosah anglické hrozby, kde se bude moci připravit na sňatek s Františkem. 7. srpna 1548 ve věku šesti let odplula do bretaňského přístavu Roscoff.

Mariina první léta na francouzském dvoře byla nejidyličtější v jejím životě. Byla obklopena přepychem, nehrozilo jí nebezpečí a postupně v ní sílila láska k budoucímu manželovi, následníkovi trůnu. Vzali se, když jim bylo šestnáct, a o rok později se stali francouzským královským párem. Všechno se již zdálo být připraveno k jejímu triumfálnímu návratu do Skotska, když tu manžel, jehož zdraví bylo vždy chatrné, těžce onemocněl. Ušní infekce, která ho trápila od dětství, se zhoršila tak, že zánět zasáhl mozek. Roku 1560, rok po korunovaci, František II. zemřel a Marie ovdověla.

Od tohoto okamžiku se Mariin život proměnil ve sled tragédií. Roku 1561 se vrátila do Skotska, kde mezitím nastaly velké změny. Během své dlouhé nepřítomnosti si Marie zachovala a posílila katolickou víru, zatímco se její poddaní *začali* obracet k protestantismu. Marie tolerovala přání většiny, zpočátku vládla poměrně úspěšně,ale roku 1565 se provdala za svého bratrance Jindřicha Stuarta, hraběte z Darnley, a tak se ocitla na sestupné dráze. Darnley byl zlý, brutální muž, jehož bezohledná touha po moci připravila Marii o loajalitu skotské šlechty. Hned následujícího roku dostala Marie děsivý důkaz manželovy barbarské povahy, když před jejíma očima zavraždil Mariina tajemníka Davida Riccia. Všem začalo být jasné, že v zájmu Skotska je třeba se Darnleyho zbavit. Historici se dosud neshodli, zda to byla Marie, nebo skotská šlechta, kdo se rozhodl pro spiknutí. Jisté je, že v noci z 8. na 9. února 1567 vzplál Darnleyho dům, a on sám byl při pokusu o útěk zardoušen. Jedinou kladnou stránkou tohoto Mariina manželství byl syn a dědic -Jakub.

Ani další Mariino manželství nebylo šťastnější. Jejím manželem se stal Jakub Hepburn, čtvrtý hrabě z Bothwellu. V létě 1567 ztratili protestantští skotští páni definitivně iluze o své katolické královně, Bothwella vyhnali ze země a Marii uvěznili, když ji předtím donutili, aby abdikovala ve prospěch svého čtrnáctiměsíčního syna Jakuba VI. Mariin nevlastní bratr hrabě Moray se stal

regentem. Následujícího roku však Marie z vězení uprchlá, posbírala armádu šesti tisíc věrných a naposledy se pokusila získat korunu. Její vojáci se střetli s regentovou armádou u malé vesnice Langside poblíž Glasgowa. Marie pozorovala průběh bitvy z nedalekého návrší. Její vojáci byli silnější počtem, postrádali však disciplínu a Marie musela sledovat, jak jsou jejich řady rozbíjeny. Když už byla porážka nevyhnutelná, Marie utekla. Nejraději by se vydala na východní pobřeží a odtud lodí do Francie, to by však znamenalo projít územím, jež ovládal její nevlastní bratr. Namísto toho proto zamířila na jih do Anglie, kde doufala v ochranu své sestřenice královny Alžběty I.

Marie se strašlivě přepočítala. Alžběta jí nenabídla nic než jen další vězení. Oficiálním zdůvodněním byla účast na vraždě Darnleyho, skutečná příčina však spočívala v Alžbětiných obavách - angličtí katolíci totiž považovali Marii za pravou anglickou královnu. Nárok na anglický trůn mohla Marie skutečně odvozovat od své babičky Marie Tudorovny, starší sestry Jindřicha VIII., Alžběta jako poslední Jindřichův žijící potomek však byla legitimnější následnicí. Podle katolíků však věci stály jinak: Alžběta jako dcera Anny Boleynové byla nelegitimní, protože Annu si vzal Jindřich VIII. po rozvodu s Kateřinou Aragonskou navzdory nesouhlasu papeže. Angličtí katolíci nikdy neuznali Jindřichův rozvod jako právoplatný, proto nepokládali za legitimní ani jeho sňatek s Annou Boleynovou a samozřejmě nepokládali jejich dceru Alžbětu za královnu. Místo toho ji považovali za nemanželské dítě a uchvatitelku.

Marie byla postupně vězněna na několika zámcích a usedlostech. Přestože ji Alžběta pokládala za jednu z nejnebezpečnějších csob v Anglii, mnoho Angličanů si vážilo Mariina vytříbeného chování, nepopiratelné inteligence a zjevné krásy. Alžbětin kancléř William Cecil se zmínil o Mariině „prohnanosti, s níž lichotila mužům". Cecilův pobočník Nicholas White to viděl podobně: „Oplývala svůdnou krásou, mluvila s příjemným skotským přízvukem a svou laskavostí zastírala pronikavý rozum." S přibývajícími lety však její krása uvadala, zdraví chátralo a naděje se zmenšovala. Její žalářník sir Amyas Paulet patřil k puritánům, vůči jejímu osobnímu kouzlu byl zcela imunní a zacházel s ní stále drsněji. Roku 1586, po 18 letech věznění, již přišla Marie o všechna svá privilegia. K pobytu jí určili Chartley Hall ve Staffordshire a zakázali jí jezdit do lázní v Buxtonu, kde jí koupele pomáhaly bojovat s častými nemocemi. Při své poslední návštěvě Buxtonu napsala diamantem na okenní tabulku: „Buxtone, jejž proslavily jeho horké prameny, sotva tě mé oko zří více - sbohem". Je zřejmé, že tušila brzkou ztrátu i toho kousku svobody, jenž jí ještě zbýval. K Mariinu rostoucímu zármutku přispěly i aktivity jejího devatenáctiletého syna, skotského krále Jakuba VI. Vždy doufala, že jednoho dne uprchne a vrátí se do Skotska, aby sdílela vládu se svým synem, kterého neviděla od doby, kdy mu byl rok. Jakub však necítil ke své matce žádnou náklonnost. Vychovali ho Mariini nepřátelé, kteří mu namlouvali, že matka zabila otce, aby se mohla provdat za svého milence. Jakub jí pohrdal a obával se, že kdyby se vrátila, bude usilovat o jeho korunu. Jeho nenávist k Marii je jasně patrná z toho, že neváhal nabídnout sňatek Alžbětě I., ženě, která dala jeho matku uvěznit (a která byla o třicet let starší než on). Alžběta návrh odmítla.

Marie svému synovi psala ve snaze porozumět si s ním, dopisy však nikdy nedorazily ani na hranice Skotska. To ještě víc prohloubilo Mariinu osamělost: její odchozí poštu zabavovali, dopisy, jež pro ni přicházely, zadržoval žalářník. Mariino odhodlání se vytrácelo, zdálo se jí, že je vše ztraceno. V takovém rozpoložení se *nacházenu*, když dostala 6. ledna 1586 překvapující balíček dopisů.

Pocházely od jejích příznivců z kontinentální Evropy. Do vězení je propašoval katolík Gilbert Gifford, který odešel z Anglie roku 1577 a studoval teologii na Anglické koleji v Římě. Když se v roce1585 vrátil do Anglie, byl očividně odhodlán sloužit Marii Stuartov-ně, a proto navštívil francouzské vyslanectví v Londýně. Tam se pro Marii hromadila korespondence. Na vyslanectví věděli, že odešlou-li dopisy formální cestou, Marie je nikdy nedostane. Gifford se nabídl, že zkusí dopisy propašovat do Chartley Hall, a svému slovu dostál. Byla to první zásilka z mnoha, a tak začal Gifford fungovat jako kurýr - nejen že vozil Marii dopisy, ale přebíral i odpovědi. Měl k tomu účelu vymyšlenu důmyslnou cestu. Dopisy dodával místnímu sládkovi, jenž je uložil do koženého obalu, který vložil do duté zátky. Tou pak uzavřel sud piva a dodal jej do Chartley Hall. Mariini sloužící sud otevřeli, dopisy vyjmuli a donesli je své královně. Odpovědi odcházely stejnou cestou.

V londýnských hostincích mezitím vznikal plán, jak Marii osvobodit - aniž by o tom ona sama zatím věděla. V centru spiknutí stál Anthony Babington, jen čtyřiadvacetiletý, ale už dobře známý jako šarmantní muž a proslulý bonviván. Jeho četní přátelé netušili, že Babington trpce nenávidí současné vládce Anglie, kteří ublížili jemu, jeho rodině a jejich víře. Protikatolická politika státu dosáhla tou dobou hrůzných rozměrů. Kněží bývali obviňováni z velezrady, kdokoli, kdo by je ukryl, musel počítat s mučením, napínáním na skřipec a vyříznutím vnitřností zaživa. Katolická mše byla úředně zakázána, rodiny, jež si zachovaly loajalitu k Římu, byly vysoce zdaňovány. Babingtonův odpor k režimu vzrostl, když byl jeho praděd lord Darcy popraven za účast v katolickém povstání proti Jindřichu VIII. Spiknutí vzniklo jednoho večera v březnu 1586, kdy se Babington sešel se šesti důvěrnými přáteli v krčmě U pluhu poblíž Temple Bar*. Jak poznamenal historik Philip Caraman: „Silou své osobnosti a výjimečným šarmem k sobě připoutal mnoho mladých katolických gentlemanů vyznačujících se postavením, galantností, dobrodružnou povahou a odhodláním bránit katolickou víru v jejích těžkých dnech; plně připravených podstoupit jakékoli dobrodružství, jež by napomohlo katolické věci." Během několika měsíců vznikl ambiciózní plán, který počítal s osvobozením Marie Stuar-tovny, zavražděním Alžběty I. a podnícením rebelie podporované invazí ze zahraničí.

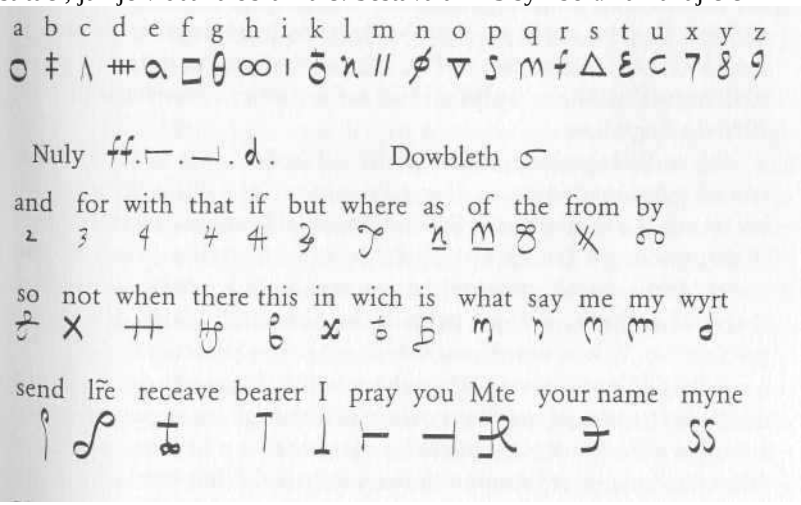
* Temple Bar je historické označení západní hranice města Londýna, nachází se na dnešní Fleet Street. O sto let později byl na tomto místě vztyčen oblouk připomínající tento mezník, v 19. století byl zbourán, dnes se uvažuje o jeho rekonstrukci.

Spiklenci si byli vědomi, že svůj úmysl nemohou provést bez Mariina souhlasu, nebyl však žádný zřejmý způsob, jak s ní *navázat* komunikaci. 6. července 1586 se

však na Babingtonově prahu objevil Gifford, který přinesl dopis od Marie, vysvětlil mu, že se o Ba-bingtonovi dověděl od Mariiných pařížských přívrženců a nabídl mu své služby. Babington sestavil dopis, v němž podrobně popsal plán spiknutí. Zmínil se také o exkomunikaci Alžběty I. papežem Piem V. z roku 1570, což podle něj ospravedlňovalo záměr ji zavraždit:

„Spolu s deseti dalšími gentlemany a stovkou našich příznivců sám zařídím vysvobození Vaší královské výsosti z rukou nepřátel. Pokud jde o to, jak naložit s uchvatitelkou, z věrností jíž jsme vyvázáni její exkomunikací, je zde šest gentlemanů, vesměs mí důvěrní přátelé, kteří v horlivosti, s níž slouží katolické věci a Vaší výsosti, skoncují s touto záležitostí."

Gifford opět použil svůj trik se zátkou pivního sudu a propašoval dopis přes stráže. To lze pokládat za formu steganografie, neboť dopis byl ukryt. Jako další bezpečnostní opatření však Babington svůj dopis zašifroval, takže i kdyby jej žalářník zachytil, nedokázal by zprávu přečíst a spiknutí by nebylo vyzrazeno. Použil šifru, která byla spíše nomenklátorem než prostou monoalfabetickou substitucí, jak je vidět na obrázku 8. Sestávala z 23 symbolů nahrazujících



Obrázek 8: Nomenklátor Marie Stuartovny sestávající z šifrové abecedy a kódových slov.písmena abecedy (bez použití j, v a w) a 35 symbolů reprezentujících slova či fráze. Kromě toho obsahovala čtyři nuly (ff. i—. __,. J,.) a symbol <5~, který indikoval, že následující symbol představuje zdvojené písmeno („dowbleth").

Gifford byl mladý, dokonce mladší než Babington, a přece se staral o své zásilky zkušeně - a záludně. Používal falešná jména jako pan Colerdin, Pietro a Cornelys, díky nimž mohl cestovat po celé zemi, aniž by vzbudil podezření. S využitím kontaktů mezi katolíky disponoval řadou bezpečných úkrytů mezi Londýnem a Chartley Halí. Kdykoli však jel do Chartley Hall, udělal si malou zajížďku. Gifford zdánlivě pracoval jako Mariin agent, ve skutečnosti však byl dvojitým agentem. V roce 1585, ještě před svým návratem do Anglie, napsal dopis siru Francisi Walsinghamovi, tajemníku královny Alžběty I., a nabídl mu své

služby. Gifford si uvědomil, že jeho katolický původ může posloužit jako dokonalá maska k průniku do spiknutí proti Alžbětě. Ve svém dopisu Walsinghamovi napsal: „Slyšel jsem o práci, kterou se zabýváte, a chci vám sloužit. Nemám zábrany ani strach. Vykonám, cokoli mi nařídíte."

Walsingham byl Alžbětiným nejbezohlednějším ministrem - postava jak z Machiavelliho, šéf špionáže odpovědný za bezpečnost panovnice. Zdědil malou síť špionů, kterou rychle rozšířil na evropský kontinent, odkud pocházela většina pokusů o útoky proti Alžbětě. Po jeho smrti se ukázalo, že pravidelně dostával zprávy ze dvanácti míst ve Francii, ze čtyř v Itálii, čtyř ve Španělsku a ze tří v Nizozemsku. Kromě toho měl své informátory v Konstantinopoli,

Alžíru a Tripolisu.

Byl to Walsingham, kdo nařídil Giffordovi, aby zašel na francouzské vyslanectví a nabídl se jako kurýr. Najal Gifforda jako svého špiona. Kdykoli převzal Gifford dopis od Marie, zanesl jej napřed Walsinghamovi. Ten zprávu předal svým padělatelům, kteří zlomili pečeť, dopis opsali, originál znovu zapečetili a vrátili Giffordovi. Zdánlivě nedotčený dopis byl pak doručen buď Marii, nebo jejím partnerům. Nikdo neměl ani tušení, co se ve skutečnosti děje.

Když Gifford donesl Walsinghamovi Babingtonův dopis určený Marii, bylo třeba jej nejdříve rozluštit. Walsingham se poprvé setkal s kódy a šiframi v knize italského matematika a kryptografa Giro-lama Cardana (který mimochodem také navrhl dotykové písmo pro slepé, jež bylo předchůdcem Braillova písma). Cardanova kniha vzbudila Walsinghamův zájem. O užitečnosti celé věci ho však přesvědčil především výkon vlámského kryptoanalytika Philipa van Marnix. Španělský král Filip II. si roku 1577 dopisoval pomocí šifer se svým nevlastním bratrem donem Juanem ďAustria, který ovládal většinu Nizozemí. Jeden z Filipových dopisů popisoval plán invaze do Anglie, zachytil jej však Vilém Oranžský a předal Marnixovi, svému tajemníkovi pro šifry. Marnix plán rozluštil, Vilém předal dopis anglickému agentovi v Evropě Danielu Rogersovi, který varoval Walsinghama před invazí. Anglie zpevnila svou obranu, což stačilo k tomu, aby Filip od plánu upustil.

Walsingham tak pochopil význam kryptoanalýzy. Zřídil v Londýně školu šifrování a jako svého tajemníka pro šifry zaměstnal Thomase Phelippese. Phelippes byl menší postavy, štíhlý, s tmavo-žlutými vlasy a světle žlutým vousem, s tváří rozrytou od neštovic, byl krátkozraký a vypadal na třicet let. Byl znalcem jazyků, domluvil se francouzsky, italsky, španělsky, latinsky a německy. A především byl jedním z nejlepších kryptoanalytiků v Evropě.

Kdykoli Phelippes dostal do rukou nový Mariin dopis, vrhl se na něj. Byl mistrem frekvenční analýzy, a proto bylo jen otázkou času, kdy najde řešení. Stanovil frekvenci každého z použitých znaků a předběžně navrhl významy těch, jež se opakovaly nejčastěji. Když se ukázalo, že použitý postup nikam nevede, vrátil se a zkusil alternativy. Postupně se mu podařilo identifikovat všechny nuly - kryp-tografické falešné stopy. Tak zbyla už jen klíčová slova, jejichž význam šlo uhodnout z kontextu.

Po dešifrování dopisu, v němž Babington navrhl zavraždit Alžbětu, zanesl

Phelippes usvědčující text okamžitě svému pánovi. Walsingham se mohl vrhnout na Babingtona, šlo mu však o víc než o důkaz proti hrstce rebelů. Riskoval a vyčkával. Doufal, že Marie odpoví, vysloví se spiknutím souhlas a tím se sama usvědčí. Smrt Marie Stuartovny si Walsingham přál již dávno, věděl však, že Alžběta se v této věci chová zdrženlivě. Kdyby však mohl dokázat, že Marie usiluje o Alžbětin život, pak by souhlas s popravou jistě získal snadno. A jeho naděje se brzy vyplnily.

Marie odpověděla Babingtonovi 17. července a tím si doslova podepsala rozsudek smrti. Vyslovila souhlas se „záměrem" a vyjádřila starost, aby byla osvobozena před vraždou Alžběty nebo nejpozději souběžně - jinak by mohly novinky dorazit k jejímu žalářníkovi a ten by ji pak mohl *zabít.* Než se dopis dostal k Babingtonovi, obdržel jeho kopii Phelippes. Díky tomu, že již rozluštil předchozízprávy, zvládl i tuto lehce, přečetl obsah a označil ji symbolem n - znakem šibenice.

Walsingham tak měl veškeré důkazy potřebné k uvěznění Marie i Babingtona, a přece pořád nebyl spokojen. Chtěl zničit celé spiknutí beze zbytku, a tak potřeboval jména všech zúčastněných. Požádal Phelippese, aby napsal do Mariina dopisu falešné postskriptum, v němž by chtěla po Babingtonovi seznam jmen. Dalším Phelippe-sovým talentem bylo padělání. Říkalo se o něm, že dovede „psát rukopisem kohokoli, sotva jej byl jednou zhlédl, jako by dotyčný sám ta slova napsal". Obrázek 9 ukazuje postskriptum připsané na konec Mariina dopisu Babingtonovi. Lze jej dešifrovat pomocí Mariina nomenklátoru (viz obrázek 8) a obsahuje následující text:

„Ráda bych seznala jména a kvality oněch pánů, kteří mají záměr vykonati; a to proto, že bych snad mohla, znajíc všechny zúčastněné, pomoci radou, jíž by se v tom mohli říditi, a čas od času snad i blíže říci, jak počínati si mají. Stejně tak, jakmile vám to bude možné, sdělte, kdo již je a do jaké míry se záměrem obeznámen."

Šifra Marie Stuartovny jasně ukazuje, že špatné šifrování je horší než žádné. Marie i Babington se o svých záměrech vyjadřovali zcela otevřeně, neboť věřili, že jejich komunikace je bezpečná. Kdyby si museli korespondovat bez šifry, jistě by volili diskrétnější výrazy. Jejich důvěra ve vlastní šifru rovněž způsobila, že naletěli na Phelip-pesův padělek. Často se stane, že odesilatel i příjemce důvěřují šifře natolik, až jsou přesvědčeni, že nepřítel by ji nikdy nedokázal napodobit a podstrčit jim falešný text. Správné použití kvalitní šifry je

velkou pomocí pro obě komunikující strany, avšak nekorektní zacházení se slabou šifrou může vyvolat velmi falešný pocit bezpečí.

Záhy poté, co dostal dopis s postskriptem, měl Babington odjet do *ciziny, aby* tam organizoval invazi. K tomu potřeboval pas, který mu měli

vydat Walsinghamovi úředníci. To by byl ideální okamžik k zatčení zrádce, ale John Scudamore, který vedl příslušný úřad, nebyl připraven na to, že se nejhledanější zrádce v Anglii klidně dostaví do jeho kanceláře. Scudamore, který si nevěděl rady, zavedl nic netušícího Babingtona do blízkého hostince a hrál o čas, zatímco jeho pomocník sháněl stráže. Za chvíli již poslal Scudamorovi do hostince zprávu, že se *zatčení* blíží. Babington pojal podezření. Lehkým tónem prohodil, že zaplatí za jídlo a pití, a zvedl se od stolu, kde nechal svůj kabát a meč, aby dal najevo, že se hned vrátí. Namísto toho se protáhl zadními dveřmi a utekl, nejprve do St. John's Wood a pak do Harrow. Tam se pokusil přestrojit, ostříhal si vlasy nakrátko a natřel si tváře ořechovou šťávou, aby zakryl své aristokratické vzezření. Unikal po deset dní, ale 15. srpna byl i se šesti ostatními společníky zatčen a odvezen do Londýna. Kostelní zvony po celém městě vyzváněly na znamení triumfu. Poprava spiklenců byla strašlivá. Slovy alžbětinského historika Williama Camdena je „podřízli, odřízli jejich hanbu, vyvrhli zaživa vnitřnosti jejich a rozčtvrtili je".

Mezitím, dne 11. srpna, dostala Marie Stuartovna mimořádné povolení projet se se svým doprovodem po pozemcích Chartley Hall. Při jízdě po vřesovišti uviděla Marie blížící se jezdce a pomyslela si, že to musí být Babingtonovi muži, kteří ji přicházejí osvobodit. Záhy však vyšlo najevo, že ji jdou naopak zatknout. Marii obvinili z účasti v Babingtonově spiknutí a soudili ji podle zákona o spolčo-vání, speciálního zákona schváleného parlamentem v roce 1584 kvůli každému, kdo by konspiroval proti Alžbětě I.

Proces se odehrával na zámku Fotheringhay, v bezútěšném místě uprostřed mokřin hrabství East Anglia. Začátek je datován na středu 15. října. Procesu se zúčastnili dva hlavní soudci, čtyři soudci vedlejší, lord kancléř, lord strážce pokladu, Walsingham, různá hrabata, rytíři a baroni. V zadní části soudní síně bylo vyhrazeno místo pro diváky, jimiž byli místní vesničané a sloužící účastníků soudu, všichni dychtiví vidět pokořenou skotskou královnu, jak prosí o milost a o život. Marie však zůstala po celý proces důstojná a nezlomená. Její hlavní obranou bylo popírat jakýkoli vztah s Ba-bingtonem. „Mohu snad odpovídat za zločinné plány několika vy-vrhelů," ptala se, „jež zosnovali bez mé pomoci a bez mého vědomí?" Toto prohlášení však vážilo málo ve srovnání s tíhou důkazů, které proti ní snesli.

Marie a Babington spoléhali na šifru, jež by udržela jejich plány v tajnosti, žili však v době, kdy kryptoanalýza měla navrch nad kryptografií. Přestože jejich šifra stačila na ochranu před zvědavýma očima amatérů, proti odborníkům znalým frekvenční analýzy neměla šanci. Na galerii mezi diváky stál Phelippes a tiše pozoroval, jak soudci předkládají důkazy, které on vyčaroval ze zašifrovaných do-

pisů.

Následujícího dne proces pokračoval, ale Marie nadále popírala, že by o Babingtonově spiknutí věděla. Když proces skončil, ponechala soudce, ať rozhodnou o jejím dalším osudu, když jim předem hlasitě odpustila nevyhnutelné rozhodnutí. O deset dní později se královský soud sešel ve Westminsteru a rozhodl, že se Marie Stuar-tovna provinila „záměrem a přípravou událostí, jež měly vést ke smrti a zničení anglické královny". Soud doporučil trest smrti a Alžběta rozsudek podepsala.

8. února 1587 se ve velkém sále zámku Fotheringhay sešlo asi tři sta lidí, aby přihlíželi popravě. Walsingham se snažil zabránit tomu, aby Marie získala pověst mučednice. Proto nařídil, aby byl popravčí špalek spálen spolu s jejími šaty a se vším ostatním, co mělo k popravě vztah - nechtěl, aby se z těchto předmětů staly relikvie. Kromě toho naplánoval na následující týden okázalý pohřeb svého synovce sira Philipa Sidneye. Šlo o oblíbenou a hrdinskou osobnost, zabitou v boji s katolíky v Nizozemí. Walsingham doufal, že oslavné pohřební obřady oslabí lidové sympatie vůči Marii. Marie však stejně tak usilovala o to, aby se její poslední veřejné vystoupení stalo gestem vzdoru, připomínkou katolické víry a povzbuzením pro následovníky.

Zatímco děkan z Peterborough předčítal oficiální modlitbu, Marie se nahlas modlila po svém - za zachování anglické katolické církve, za svého syna a za Alžbětu. Připomněla si rodinné motto „V mém konci je můj začátek" a pevným krokem přistoupila k popravčímu špalku. Kati ji požádali o odpuštění a ona odvětila: „Odpouštím vám celým svým srdcem, neboť doufám, že nyní učiníte konec veškerému mému utrpení." Richard Wingfield ve svém *Nar-ration of the Last Days of the Queen of Scots* (Vyprávění o posledních dnech královny skotské) popsal její poslední chvíle takto:

„Potom tiše složila hlavu svou na špalek, ruce i nohy natáhla a několikráte odříkala In manus tuas domine, kdyžtě naposledy slova ta vyřkla, jeden z popravčích ji lehce přidržel jednou svou rukou a ti ostatní dvakráte sekerou udeřili, až téměř oddělili její hlavu od trupu, jen nepatrně upevněna zůstala, a ona nevydala téměř hlásky a její tělo se ani nepohnulo... Její rtové se však ještě po čtvrt hodiny chvěly, než hlava zcela se oddělila od těla. Jeden z popravčích pak rukou sáhl po jejích podvaz-cích, chtě jich sobě uzmouti, a tu se ukázalo, že pod jejími šaty byl jest ukryt malý její psík, jehož nikterak odtrhnouti nemohli, a on neopustil její mrtvé tělo, avšak ulehl mezi její hlavu a ramena, jak později pilně zaznamenáno bylo."**2**

Le chiffre indéchiffrable

Jednoduchá monoalfabetická substituce byla ostatečně bezpečná po celá staletí. To se však změnilo v důsledku rozvoje frekvenční analýzy - nejprve v arabském světě, později v Evropě. Tragická poprava Marie Stuartovny je dramatickou ilustrací slabin monoalfabe-tické substituce. Bylo zřejmé, že v bitvě mezi kryptografy a kryptoa-nalytiky mají navrch ti druzí. Každý, kdo odesílal šifrovanou zprávu, musel počítat s tím, že špičkový nepřátelský kryptoanalytik ji může

rozluštit a přečíst si všechna tajemství v ní obsažená.

Před kryptografy tedy stála úloha vymyslet novou, silnější šifru, na niž by luštitelé nestačili. Přestože se taková šifra objevila až koncem 16. století, její počátky lze vysledovat až k florentskému polyhistorovi Leonu Battistovi Albertimu, který se narodil roku 1404 a patřil ke klíčovým osobnostem renesance. Byl to malíř, skladatel, básník a filozof, rovněž autor prvních vědeckých pojednání o perspektivě, traktátu o mouše domácí a pohřebního oratoria za svého psa. Nejvíce se proslavil jako architekt, postavil první římskou fontánu Trevi a napsal *De re aedificatoria*, první tištěnou knihu o architektuře, jež posloužila jako katalyzátor přechodu od gotického slohu k renesančnímu.

Někdy v 60. letech 15. století se Alberti procházel vatikánskými zahradami, kde potkal svého přítele Leonarda Data, jenž pracoval jako sekretář u papežského stolce. Dali se do řeči o kryptografii. Náhodná konverzace inspirovala Albertiho k eseji na dané téma. V něm popsal šifru, kterou pokládal za zcela novou. V té době se u substituční šifry používala vždy jedna šifrová abeceda k zašifrování celé zprávy. Alberti namísto toho navrhl použít dvou či více šifrových abeced, které by se při šifrování pravidelně střídaly a zmátly tak potenciální krypto analytiky:

Otevřená abeceda abcdefghij klmnopqrstuvwxyz Šifrová abeceda 1 FZBVKIXAYMEPLSDHJORGNQCUTW Šifrová abeceda 2 GOXBFWTHQILAPZJDESVYCRKUHN

Zde máme například dvě šifrové abecedy. Zprávu můžeme zašifrovat tak, že abecedy mezi sebou stále střídáme. Zprávu nazdar zašifrujeme tak, že první písmeno šifrujeme podle první abecedy, *takže* namísto n dostaneme S. Druhé písmeno zprávy pak šifrujeme podle druhé abecedy a dostaneme G. Třetí písmeno šifrujeme opět podle první abecedy, čtvrté podle druhé abecedy, páté podle první, šesté podle druhé. Celý šifrový text pak zní **SGWBFS.** Klíčová výhoda Albertiho systému spočívá v tom, že opakovaný výskyt písmene v otevřeném textu nevede nutně k opakovanému výskytu jiného písmene v šifrovém textu. Například opakující se a ve slově nazdar je jednou šifrováno jako G, podruhé jako F. Stejně tak opakující se S v šifrovém textu znamená jednou n, podruhé r.

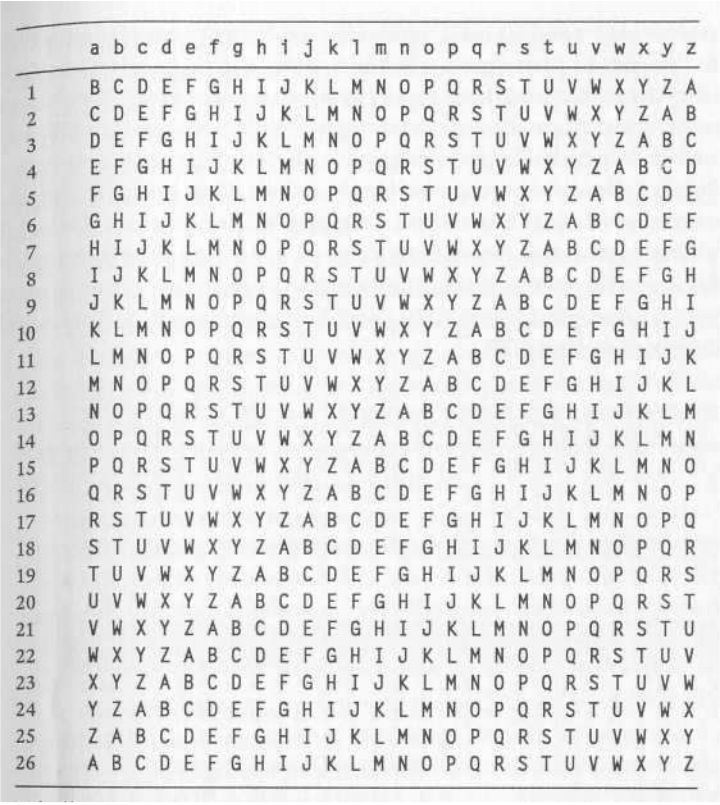
Přestože Alberti narazil v kryptografii na největší objev tisíciletí, dál jej nerozvinul. Tento úkol zbyl na jeho pokračovatele. Prvním z nich byl Johannes Trithemius, německý opat narozený roku 1462, dalším italský vědec Giovanni Porta, jenž se narodil roku 1535, a konečně Blaise de Vigeněre, francouzský diplomat narozený roku 1523. Vigenere se seznámil s pracemi Albertiho, Trithemia a Porty, když byl ve svých šestadvaceti letech vyslán na dvouletou diplomatickou misi do Říma. Je třeba říci, že jeho zájem o krypto-grafii byl zcela praktický, plně svázaný s jeho diplomatickou službou. Ve věku třiceti devíti let Vigenere usoudil, že již našetřil dost peněz, aby pověsil svou kariéru na hřebík a nadále se věnoval jen studiu. Teprve tehdy prozkoumal do detailů práce Albertiho, Tri-themia a Porty, aby spojil jejich příspěvky do návrhu ucelené a silné šifry.

Přes nesporný význam příspěvků Albertiho, Trithemia a Porty se šifra

nazývá po Vigenerovi - muži, který ji dopracoval do konečné podoby. Síla Vigenerovy šifry spočívá v tom, že k zašifrování zprávy nepoužívá jednu, ale 26 odlišných šifrových abeced. První šifrovací krok spočívá v tom, že se vypíše tzv. Vigenerův čtverec (viz tabulka 3), což je otevřená abeceda následovaná 26 šifrovými abecedami, z nichž každá je vůči předchozí posunuta o jedno písmeno. První řádek tedy odpovídá šifrové abecedě s Caesarovým posunem 1 a lze jej použít pro šifrování Caesarovou šifrou, v níž je každé písmeno šifrového textu posunuto o jednu abecední pozici oproti otevřenému textu. Řádek 2 odpovídá šifrové abecedě s Caesarovým posunem 2 a tak dále. Nejvrchnější řádek čtverce reprezentuje otevřený text. Každé jeho písmeno lze zašifrovat kteroukoli z 26 šifrových abeced. Pokud například použijeme abecedu 2, pak písmeno a šifrujeme jako C, použijeme-li abecedu 12, šifrujeme a jako M.

Kdyby odesilatel použil jen jednu šifrovou abecedu, pak půjde o jednoduchou Caesarovu šifru, což je velmi slabý kryptografický prostředek, který lze snadno rozluštit. Podstata Vigenerovy šifry však spočívá v tom, že se pro zakódování každého písmene použije jiný řádek čtverce, tedy jiná šifrová abeceda. Jinými slovy, odesilatel může zašifrovat první písmeno zprávy pomocí řádku 5, druhé podle řádku 14, třetí řádkem 21 a tak dále.

Aby příjemce získal zpět čitelný text, musí vědět, kterým řádkem Vigenerova čtverce šifroval odesilatel každé písmeno zprávy, musí tedy existovat předem dohodnutý systém, podle něhož se řádky střídají. Toho lze dosáhnout pomocí klíčového slova. Pro ilustraci si předvedeme, jak prostřednictvím Vigenerova čtverce zašifrovat krátkou zprávu ďiverttroopstoeastridge („odkloňte jednotky k východnímu hřebenu") za použití hesla WHITE („bílý"). Jako první krok napíšeme heslo nad text zprávy - opakovaně, tolikrát, kolikrát je třeba, abychom ji pokryli celou. Pak šifrujeme následujícím způsobem: k zašifrování prvního písmene, jímž je d, se



	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabulka. 3: Vigeněrův čtverec

nejprve podíváme, jaké písmeno klíče se u něj nachází. Je to W, čímž je dán řádek Vigeněrova čtverce, v daném případě řádek 22, jenž začíná právě písmenem W. V průsečíku sloupce označeného d a řádku označeného W najdeme písmeno Z, což je první písmeno hledaného šifrového textu.

Klíčové slovo WHITEWHITEWHITEWHITEWHI Otevřený text diverttroopstoeastridge Šifrovýtext ZPDXVPAZHSLZBHIWZBKMZNM

Pro zašifrování druhého písmene zprávy, jímž je i, celý proces zopakujeme. Písmeno klíče nad i je H, takže i šifrujeme pomocí řádku 7, jenž začíná písmenem H. Podíváme se na průsečík sloupceoznačeného i a řádku označeného H a najdeme v něm písmeno P. To je tedy druhým písmenem šifrového textu. Každé písmeno klíčového slova indikuje konkrétní šifrovou abecedu uvnitř Vigeněrova čtverce, a protože naše heslo sestává z pěti písmen, odesilatel šifruje za neustálého střídání pěti šifrových abeced. Páté písmeno zprávy šifrujeme přes páté písmeno klíčového slova, jímž je E, ale u šestého písmene se vracíme k prvnímu písmenu klíčového slova. Delší klíčové slovo nebo fráze znamená, že se používá více šifrových abeced a složitost šifry roste. V tabulce 4 vidíme Vigenerův čtverec, v němž je zvýrazněno pět řádků (tedy pět šifrových abeced) definovaných klíčovým slovem WHITE.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabulka 4: Vigeněrův čtverec, v němž je zvýrazněno pět řádků definovaných klíčovým slovem WH **ITE.** Při šifrování se přepíná mezi pěti zvýrazněnými šifrovými abecedami definovanými W , H , I , T a E.

Velkou výhodou Vigenerovy šifry je odolnost vůči frekvenční analýze popsané v první kapitole. Kryptoanalytik používající frekvenční analýzu začne zpravidla tím, že si stanoví, které písmeno v šifrovém textu je nejčetnější. V tomto příkladu je to písmeno Z. Pak učiní předpoklad, že toto písmeno odpovídá nejběžnějšímu písmenu anglické abecedy, jímž je e, což však není pravda. U popsané šifry písmeno Z reprezentuje postupně (na daném vzorku textu, pozn. překl.) písmena d, r a s, v žádném případě e. To je z hlediska kryptoanalytika vážný problém. Skutečnost, že opakované výskyty téhož písmene v šifrovém textu mohou odpovídat různým písmenům v otevřeném textu, představuje obrovskou nejednoznačnost. Stejně matoucí je i opačný princip - totéž písmeno otevřeného textu bude při svých různých výskytech pokaždé šifrováno jinak. Například ve slově troops se o opakuje dvakrát po sobě, v šifrovém textu však toto oo bude zobrazeno jako HS.

Vigenerova šifra je nejen odolná vůči frekvenční analýze, ale také disponuje enormním množstvím klíčů. Odesilatel a příjemce se mohou dohodnout na libovolném slově ze slovníku, na určité kombinaci slov, mohou si dokonce

vytvářet umělá slova. Kryptoanalytik nemůže zkoušet všechna myslitelná klíčová slova - je jich příliš mnoho.

Vrcholem Vigenerovy práce byl jeho *Trakte des chiffres* (Traktát o šifrách), publikovaný roku 1586. Ironií osudu jej vydal téhož roku, kdy Thomas Phelippes prolomil šifru Marie Stuartovny. Kdyby Mariin šifrant četl Vigenerovo pojednání, mohl by Phelippese přelstít -a Marie by možná vyvázla živá.

Vzhledem k tomu, o jak silný šifrovací prostředek jde, zdálo by se přirozené, že se rychle rozšíří do šifrovací praxe po celé Evropě. Sifranti by přece měli být velmi spokojeni, že znovu dostávají do rukou bezpečný nástroj, ne? Stal se však opak: Vigenerova šifra se neujala. Tento zjevně dokonalý systém byl opomíjen po celá dvě následující století.

Od Vigenera k Muži se železnou maskou

Tradiční forma substituční šifry, známá v dobách před Vigenerovým objevem, se nazývá monoalfabetická substituční šifra, protože používá v rámci jedné zprávyjen jednu šifrovou abecedu. Vige-nerova šifra naproti tomu patří mezi *polyalfabetické*, protože zavádí pro jedinou zprávu více abeced. Polyalfabetická povaha dodává Vi-generově šifře sílu, zároveň však ztěžuje její využití. Obtížnější práce s šifrou mnoho lidí odradila.

Pro potřeby 17. století byla monoalfabetická substituce plně adekvátní. Pokud jste chtěli zajistit, aby vaše služebnictvo nečetlo vaši soukromou korespondenci, anebo ukrýt svůj osobní deník před žárlivým pohledem manžela či manželky, byla stará jednoduchá šifra ideální - rychlá, snadná k použití, plně bezpečná proti každému, kdo nebyl odborníkem v kryptoanalýze. Monoalfabetická substituce přetrvala v nejrůznějších formách po staletí (viz dodatek D), avšak v seriózních aplikacích - ve vládní a vojenské komunikaci -byla a je naprosto neadekvátní. Profesionální kryptografové potřebovali v boji s profesionálními kryptoanalytiky lepší nástroj, ač stále odmítali polyalfabetickou šifru pro její složitost. Zvlášť vojenské zpravodajství vyžadovalo rychlost a jednoduchost. Diplomatické služby zase často odesílaly a přijímaly stovky depeší denně; čas byl v obou případech základním kritériem. Kryptografové proto hledali zlatou střední cestu - šifru, která by byla obtížnější na rozluštění než monoalfabetická substituce, avšak snazší na implementaci než substituce polyalfabetická.

Mezi rozmanité kandidáty patřila i mimořádně účinná *homofonní substituční šifra*. Každé písmeno se v ní nahrazuje řadou reprezentací, přičemž jejich počet je úměrný frekvenci písmene. Například písmeno a tvoří asi 8 % psaného textu v angličtině, takže se mu přiřadí osm různých reprezentací. Kdykoli se a objeví v otevřeném textu, nahradí se v šifrovém textu jedním z těchto osmi symbolů, zvoleným náhodně. Na konci šifrování potom dojde k tomu, že každý z těchto symbolů tvoří asi 1 % šifrového textu. Naproti tomu písmeno b tvoří jen asi 2 % otevřeného textu, proto mu přiřadíme jen dva symboly. Kdykoli se v otevřeném textu objeví b, přiřadí se mu jeden z těchto dvou symbolů, takže i jejich četnost v šifrovém textu pak činí kolem 1 %. Stejným způsobem přiřadíme odpovídající počet symbolů každému znaku otevřené abecedy, až dojdeme k písmenu z, jež se vyskytuje tak vzácně, že má jen jeden reprezentující symbol. V příkladu

znázorněném v tabulce 5 jsou jako reprezentující symboly zavedena dvouciferná čísla. Pro každé písmeno otevřené abecedy používáme - v závislosti na jeho relativní četnosti -jeden až dvanáct alternativních symbolů.

Každý ze symbolů odpovídajících písmenu a reprezentuje stejný zvuk, stejnou hlásku; odtud je odvozen název tohoto typu šifry: *homos* znamená řecky „stejný", *phonos* je „zvuk". Více alternativních symbolů se jednomu písmenu přiřazuje proto, aby se vyrovnaly rozdíly mezi frekvencemi hlásek v šifrovém textu. Pokud zašifrujeme zprávu pomocí abecedy z tabulky 5, bude relativní četnost každého symbolu přibližně 1 %. Jestliže se všechny symboly vyskytují zhruba stejně často, zdá se, že frekvenční analýza nemůže fungovat. Dokonalá bezpečnost? Ne tak docela.

I v tomto případě obsahuje šifrový text různé drobné nápovědy, které může chytrý kryptoanalytik využít. Jak jsme viděli v 1. kapitole, v angličtině má každé písmeno svou osobitost, danou vztahem k jiným písmenům. Tyto vazby lze využít i tehdy, je-li zpráva zašifrována homofonní substitucí. V angličtině je nejvýraznějším příkladem osobitého chování hláska q, za níž může následovat jen jedna jediná hláska, a sice u. Pokoušíme-li se dešifrovat homofonní substituci, začneme proto konstatováním, že q je poměrně vzácně se vyskytující písmeno, takže bude pravděpodobně reprezentováno jediným symbolem. Rovněž se dá odhadnout, že u, jehož relativní četnost je asi 3 %, bude reprezentováno třemi různými symboly. Pokud tedy v šifrovém textu najdeme symbol, za nímž se vyskytují pouze tři jiné, pak bude rozumné předpokládat, že jsme našli q a u. Jiná písmena je již těžší vysledovat, ale jejich vztahy k ostatním hláskám je nakonec také zradí. I když lze homofonní substituční šifru rozluštit, je stále mnohem bezpečnější než monoalfabetická substituční šifra.

Homofonní šifra se na první pohled podobá polyalfabetické, přinejmenším v tom, že každý otevřený text lze zašifrovat mnoha různými způsoby, avšak je tu podstatný rozdíl, který způsobuje, že homofonní šifra je ve skutečnosti jen jedním z typů monoalfabetické substituční šifry. Jak je vidět z tabulky 5, písmeno a je reprezentováno osmi různými symboly. Je důležité si uvědomit, že těchto osm symbolů reprezentuje pouze písmeno a. Jinými slovy, písmeno otevřeného textu může být zašifrováno několika rozličnými symboly, ale jeden daný symbol šifrového textu odpovídá vždy jen jedinému jednoznačně určenému písmenu textu otevřeného. U polyalfabetické šifry je konkrétní znak otevřeného textu reprezentován různými znaky šifrového textu a zároveň platí, že stejné symboly šifrového textu mohou být dešifrovány jako různé znaky textu ote-

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
09	48	13	01	14	10	06	23	32	15	04	26	22	18	00	38	94	29	11	17	08	34	60	28	21	02
12	81	41	03	16	31	25	39	70			37	27	58	05	95		35	19	20	61		89		52	
33		62	45	24			50	73			51		59	07			40	36	30	63					
47			79	44			56	83			84		66	54			42	76	43						
53				46			65	88					71	72			77	86	49						
67				55			68	93					91	90			80	96	69						
78				57										99					75						
92				64															85						
				74															97						
				82																					
				87																					
				98																					

vřeného.

Tabulka 5: Příklad homofonní substituční šifry. První řádek znázorňuje otevřenou abecedu, čísla pod ním představují šifrovou abecedu. U většiny písmen je k dispozici více alternativních možností.

Hlavním důvodem, proč řadíme homofonní šifru mezi monoal-fabetické, je však to, že jakmile se jednou ustaví šifrová abeceda, zůstává po celý proces šifrování stejná. Skutečnost, že u většiny písmen máme na vybranou mezi několika symboly, není podstatná. Šifrér pracující s polyalfabetickou šifrou musí naproti tomu při šifrování neustále střídat šifrové abecedy.

Úpravami základní monoalfabetické substituce, například přidáním homofonie, se však dosáhlo vyšší bezpečnosti šifrování, aniž by se bylo třeba ponořit do složitostí polyalfabetické šifry. Jedním z nejvýraznějších příkladů zdokonalené monoalfabetické šifry byla tzv. Velká šifra Ludvíka XIV., která se používala k zašifrování králových nejtajnějších zpráv, chránila detaily jeho plánů, politických záměrů a intrik. Takto zašifrovaná zpráva se *zabývala*, i jednou z nejtajemnějších postav francouzské historie - Mužem se železnou maskou. Síla Velké šifry způsobila, že zpráva zůstala nevyluštěna po dvě století.

Autory Velké šifry byli otec a syn Antoine a Bonaventure Ros-signolové. Antoine se poprvé proslavil roku 1626, kdy dostal k vyluštění šifrovaný dopis, odeslaný po poslovi z obleženého města

Realmontu. Do večera jej přečetl a tak vyšlo najevo, že hugenoti, *držící* město, jsou na pokraji kapitulace. Francouzská armáda, jež si předtím neutěšené situace obránců města nebyla vědoma, poslala dopis zpět s připojeným vyluštěním. Hugenoti pochopili, že nepřítel neustoupí, a vzdali se. Dešifrování dopisu vedlo k vítězství bez boje.

Síla kryptoanalýzy se tak projevila naplno a Rossignolové poté získali významné postavení u dvora. Nejprve sloužili Ludvíku XIII., pak Ludvíku XIV, na něhož udělali takový dojem, že přemístil jejich kanceláře do blízkosti svých vlastních komnat, aby tak *pere et ftls* (otec a syn) Rossignolové mohli lépe hrát svou klíčovou úlohu ve francouzské diplomacii. Jednou z největších poklon, které

se jejich schopnostem dostalo, bylo zdomácnění slova *rossignol* ve slangové francouzštině jako označení pro šperhák, tedy pro nástroj schopný odemknout jakýkoli zámek stejně snadno, jako si oni dovedli poradit s cizí šifrou.

Schopnost Rossignolů dešifrovat zprávy jim pomohla přijít na to, jak navrhnout silnější kryptografické prostředky, a tak vznikla Velká šifra. Byla tak bezpečná, že plně odolala všem snahám zahraničních kryptoanalytiků ukrást francouzská tajemství. Po smrti obou Rossignolů však bohužel rychle upadla v zapomnění, takže šifrované zprávy ve francouzských archivech neuměl nikdo přečíst. Velká šifra spolehlivě odolávala i úsilí dalších generací kryptoanalytiků.

Historici si byli vědomi toho, že dokumenty zašifrované Velkou šifrou mohou poskytnout unikátní pohled na události, jež se ve Francii odehrály v 17. století. Ani o 200 let později je však neuměl nikdo přečíst. Roku 1890 se stalo, že Victor Gendron, vojenský historik zkoumající válečná tažení Ludvíka XIV., našel svazek do té doby neznámých dopisů zašifrovaných Velkou šifrou. Protože si s nimi nevěděl rady, předal je zkušenému expertovi z kryptografic-kého oddělení francouzské armády Etiennu Bazeriesovi. Ten přijal dopisy jako nejvyšší možnou výzvu a pokusy o jejich dešifrování strávil následující tři roky života.

Zašifrované stránky obsahovaly tisíce čísel, mezi nimi však bylo jen 587 čísel navzájem různých. Z toho bylo jasně vidět, že Velká šifra je víc než pouhá jednoduchá substituční šifra, neboť ta by vyžadovala jen 26 rozdílných čísel - pro každé písmeno abecedy jedno. Bazeries se zpočátku domníval, že nadbytečná čísla jsou homofon-ní, že tedy více čísel reprezentuje totéž písmeno. Průzkum tohoto předpokladu zabral několik měsíců a nepřinesl pozitivní výsledek. Velká šifra nebyla homofonní.

Dále se Bazeries soustředil na předpoklad, že by každé číslo mohlo reprezentovat dvojici písmen, *digraf*. V anglické abecedě je jen 26 jednotlivých písmen, avšak existuje 676 jejich možných dvojic, což je počet, který se zhruba rovná počtu rozdílných znaků v šifrovém textu. Bazeries vyhledal nejčastěji se vyskytující znaky v šifrovém textu (což byla čísla 22, 42, 124, 125 a 341) a zkoumal předpoklad, zda odpovídají nejčastějším dvojhláskám, které se vyskytují ve francouzštině, tedy dvojhláskám es, en, ou, de a nt. Prakticky vzato, aplikoval frekvenční analýzu na úrovni dvojic písmen. Po měsících práce se však bohužel ukázalo, že ani tato teorie neposkytuje žádné použitelné výsledky.

Bazeries se už přiblížil bodu, kdy by své úsilí určitě vzdal, když dostal další nápad. Co kdyby myšlenka s digrafy nebyla tak docela mylná? Začal zvažovat možnost, že každé z čísel reprezentuje nikoli dvojhlásku, ale slabiku. Zkusil přiřadit čísla slabikám, opět podle četnosti výskytu - nejčastěji se vyskytující čísla nejčastějším slabikám ve francouzštině. Zkusil různé permutace, ale nic nevycházelo - až se mu podařilo identifikovat jedno konkrétní slovo. Na každé stránce se několikrát opakoval shluk číslic 124-22-125-46-345. Bazeries zkusil předpokládat, že

jde o slabiky les-en-ne-mi-s, tedy slova „les ennemis" (nepřátelé). To byl rozhodující průlom.

Bazeries mohl nyní zkoumat další části šifrového textu, kde se tyto slabiky vyskytovaly v jiných slovech. Jak ví každý luštitel křížovek, když už je zřejmá část slova, dá se jeho zbytek často uhodnout. Doplňováním slov se ozřejmoval význam dalších slabik, ty bylo možné použít k rozluštění dalších slov a tak dále. Často se přitom Bazeries zarazil, jednak bylo rozdělení do slabik málokdy očividné, jednak některá čísla reprezentovala jen písmena, a nikoli celé slabiky - a také proto, že Rossignolové nastražili do šifry pasti. Například jedno z čísel nereprezentovalo ani slabiku ani písmeno, ale výmaz předchozího znaku.

Když bylo dešifrování dokončeno, stal se Bazeries prvním člověkem po dvou stech letech, který poznal tajemství Ludvíka XIV. Nově dešifrovaný materiál fascinoval historiky, kteří se soustředili především na nejpřitažlivější dopis. *Zdálo* se totiž, že řeší jednu z největších záhad 17. století: identitu Muže se železnou maskou.

Muž se železnou maskou byl předmětem mnoha spekulací již od chvíle, kdy byl poprvé uvězněn v savojské pevnosti Pignerole. Když jej převáželi roku 1698 do Bastily, pokoušeli se ho rolníci spatřit aspoň na chvíli. Pak o něm vyprávěli nejrůznějším způsobem - že je vysoký či malý, hezký na pohled či odpudivý, mladý či starý. Někteří dokonce tvrdili, že jde o ženu. Při tak malém množství konkrétních informací nepřekvapí, že svou teorii o Muži se železnou maskou měl každý od Voltaira po Benjamina Franklina. Nejběžnější konspirační teorie tvrdila, že jde o dvojče Ludvíka XIV., uvězněné proto, aby se předešlo jakémukoli sporu o trůn. Podle jedné z variant této teorie existovali i potomci Muže se železnou maskou, a tedy příslušná skrytá linie královské krve. Brožura publikovaná roku 1801 tvrdila, že potomkem Muže se železnou maskou je sám Napoleon. Tato fáma zvyšovala císařovu autoritu, proto ji nikdy nepopřel.

Mýtus Muže se železnou maskou inspiroval poezii, prózu i drama. Victor Hugo začal psát roku 1848 divadelní hru nazvanou Dvojčata, ale když se dověděl, že si stejné téma zvolil Alexander Dumas, zahodil dvě již napsaná jednání a práci nedokončil. Od té doby je to právě Dumasovo jméno, jež si s Mužem se železnou maskou spojujeme nejčastěji. Díky úspěchu jeho románu se oživila myšlenka příbuzenského vztahu mezi vězněm a králem. Přežila dodnes, navzdory důkazům, jež objevil Bazeries.

Mezi rozšifrovanými dopisy byl i jeden, který napsal Francois de Louvois, ministr války Ludvíka XIV. Dopis začíná výčtem zločinů, jichž se měl dopustit Vivien de Bulonde, velitel odpovědný za útok na město Cuneo ležící na francouzsko-italských hranicích. Ač měl nařízeno zůstat na

přiděleném stanovišti, Bulonde se polekal blížících se nepřátelských jednotek z Rakouska a uprchl. Munici a raněné vojáky zanechal na místě. Podle ministra války tak ohrozil celé piedmontské tažení. Dopis jasně líčil králi Bulondovy činy jako projev nejvyšší zbabělosti:

Jeho Veličenstvo lépe než kdokoli jiný chápe důsledky takového činu a je si rovněž plně vědomo, jak těžce tato ztráta pozice ohrozí naši věc. Jde o chybu, jíž je nutno během zimy neprodleně napravit. Jeho Veličenstvo žádá, abyste generála Bulonda neprodleně zatkl a uvěznil v pevnosti Pignerole, kde bude uzavřen v nepřetržitě střežené cele, z níž bude smět vyjít pouze v masce."To je jasná zmínka o maskovaném vězni v Pignerole a zároveň o značně závažném zločinu. Datum odpovídá vzniku mýtu o Muži se železnou maskou. Je tím tajemství vyřešeno? Nepřekvapí nás, že ti, kteří dávají přednost konspiračním teoriím, našli v této úvaze mezery. Existuje například hypotéza, že Ludvík XIV. skutečně tajné věznil své nepřiznané dvojče, a proto zanechal falešné stopy. Možná to bylo tak, že zašifrovaný dopis měl být rozluštěn úmyslně. Možná, že Bazeries, kryptoanalytik 19. století, upadl do pasti nastražené v 17. století.

Černé komnaty

Zdokonalení monoalfabetické šifry jejím nasazením na úrovni slabik nebo homofonní substitucí mohlo v 17. století ještě postačovat, avšak v 18. století se kryptoanalýza již dostala na průmyslovou úroveň. Působily v ní týmy vládních kryptoanalytiků, kteří společným úsilím dovedli vyluštit i nejsložitější šifry. Každá evropská mocnost měla svou tzv. černou komnatu - mozkové centrum pro dešifrování zpráv a shromažďování zpravodajských informací. Nejslavnější, nejdisciplinovanější a nejvýkonnější z nich byla Geheime Kabinets-Kanzlei ve Vídni.

Fungovala podle pevně daného časového řádu, neboť bylo třeba, aby její nekalé aktivity nenarušily hladký chod poštovní služby. Dopisy určené vídeňským ambasádám byly nejprve doručeny do černé komnaty, a to přesně v sedm ráno. Tajemníci je odpečetili a tým paralelně pracujících stenografů pořídil opisy. Pokud to bylo třeba, účastnili se opisování i jazykoví specialisté, aby pomohli s neobvyklými abecedami. Během tří hodin byly dopisy opět zapečetěny a vráceny na hlavní poštu, aby je mohla doručit adresátům. Pošta, která Rakouskem jen procházela, putovala do černé komnaty v deset dopoledne, odchozí pošta z vídeňských velvyslanectví ve čtyři odpoledne. I z této korespondence se rutinně pořizovaly opisy. Vídeňskou černou komnatou prošla denně asi stovka dopisů.

Kopie dopisů se předávaly kryptoanalytikům. Ti seděli po jednom v malých přístavcích, připraveni hledat význam jednotlivých depeší. Vídeňská černá komnata nejen že dodávala rakouskému panovnickému dvoru neocenitelné informace, ale také umožňovala prodávat získané poznatky jiným evropským mocnostem. V roce

1774 byla například uzavřena smlouva s tajemníkem francouzského vyslanectví opatem Georgelem, na jejímž základě dostával za tisíc zlatých dvakrát týdně zpravodajský souhrn. Získané informace posílal přímo králi Ludvíku XV.

Černé komnaty způsobily, že všechny varianty monoalfabetické šifry byly rázem zastaralé. Tváří v tvář takové kryptoanalytické přesile museli kryptografové konečně přejít na složitější, ale bezpečnější Vigeněrovu šifru. Sifranti začali postupně používat polyalfabetic-ké šifry. Kromě potřeby účinnější kryptoanalýzy zde byla ještě jedna motivace, která souvisela s vývojem telegrafu a snahou zabezpečit telegramy před odposlechem a dešifrováním.

Přestože telegraf a s ním spjatá telekomunikační revoluce je dílem 19. století, kořeny telegrafie sahají již do roku 1753. Anonymní článek v časopise vydávaném ve Skotsku popisoval, jak lze zasílat zprávy na velkou vzdálenost, spojíme-li odesilatele a příjemce svazkem 26 kabelů, jedním pro každé písmeno abecedy. Odesilatel by pak mohl zaslat zprávu pomocí elektrických pulsů. Například slovo ahoj by se odeslalo tak, že nejprve by prošel signál kabelem odpovídajícím písmenu a, pak kabelem odpovídajícím písmenu h a tak dále. Tato „rychlá metoda sdělování informací", jak ji vynálezce nazval, nebyla nikdy realizována, protože se nepodařilo překonat s ní spojené technické potíže.

Jedním z problémů byla absence dostatečně citlivého systému pro detekování elektrického signálu. Sir Charles Wheatstone a William Fothergill Cooke dokázali v Anglii sestavit detektory ze zmagnetizovaných jehel, které se vychylovaly, pokud blízkým okruhem procházel elektrický proud. Roku 1839 byl Wheatstoneův-Cookeův systém použit pro zasílání zpráv mezi železničními stanicemi West Drayton a Paddington, tedy na vzdálenost 29 km. Dobrá pověst telegrafu se brzy rozšířila a pozornost vzbudila mimořádná rychlost komunikace. Nic mu neposloužilo lépe než narození druhého syna královny Viktorie prince Alfréda, který přišel na svět dne 6. srpna 1844 na zámku Windsor. Zprávu odeslali telegraficky do Londýna a do hodiny se na ulicích prodávalo zvláštní vydání *The Times.* Článek upozorňoval na technologii, jež tento výkon umožnila, výslovnou zmínkou, že za něj „vděčíme mimořádné výkonnosti elektro-magnetického telegrafu". Následujícího roku si telegraf vydobyl ještě větší proslulost, když byl s jeho pomocí polapen John Tawell - vrah, jenž zabil svou milenku ve městě Slougha pak ve snaze uprchnout naskočil do londýnského vlaku. Místní policie telegrafovala jeho popis do Londýna, kde byl vrah při vystupování z vlaku zatčen.

V téže době postavil v Americe Samuel Morse svou první telegrafní linku spojující Baltimore a Washington. Pro zesílení signálu použil elektromagnet, takže signál u příjemce byl dost silný, aby zaznamenal na kus papíru krátké a dlouhé značky - tečky a čárky. Morse také sestavil známou Morseovu abecedu pro kódování písmen do teček a čárek (viz tabulka 6). Svůj systém završil akustickým měničem, který umožnil příjemci tečky a čárky slyšet.

Morseův vynález postupně nabyl vrchu nad Wheatstoneovým-Cookeovým systémem i v Evropě. Roku 1851 se na celé evropské pevnině začala používat mírně modifikovaná forma Morseovy abecedy obsahující dodatečné kódy pro písmena s diakritikou. Každým rokem rostl vliv Morseovy abecedy a telegrafu na celém světě. Policie díky těmto vymoženostem dostihla více zločinců, noviny otiskovaly nejčerstvější zprávy, podnikatelé disponovali

A	·–	W	·––
B	–···	X	–··–
C	–·–·	Y	–·––
D	–··	Z	––··
E	·	0	–––––
F	··–·	1	·––––
G	––·	2	··–––
H	····	3	···––
I	··	4	····–
J	·–––	5	·····
K	–·–	6	–····
L	·–··	7	––···
M	––	8	–––··
N	–·	9	––––·
O	–––	tečka	·–·–·–
P	·––·	čárka	––··––
Q	––·–	otazník	··––··
R	·–·	dvojtečka	–––···
S	···	středník	–·–·–·
T	–	pomlčka	–····–
U	··–	lomítko	–··–·
V	···–	uvozovky	·–··–·

Tabulka 6: Mezinárodní Morseův kód.

aktuální mi informacemi z finančního trhu a podniky mohly obchodovat na velké vzdálenosti.

Ochrana této často citlivé komunikace však představovala vážný problém. Morseova abeceda sama o sobě nepatří mezi kryptografic-ké nástroje, protože obsah zprávy nijak nechrání. Tečky a čárky nejsou ničím jiným než výhodnou reprezentací písmen pro přenos prostřednictvím telegrafu. Morseovka není nic jiného než jiná formy obyčejné abecedy. Problém utajení vznikl především proto, že kdo chtěl poslat telegram, musel se obrátit na operátora, který si zprávu nutně musel přečíst, aby ji mohl odeslat. Telegrafisté měli přístup ke všem zprávám v systému. Existovalo proto riziko, že například firma může operátora podplatit, aby se dostala k depeším své konkurence. Podstatu problému shrnuje článek o telegrafii publikovaný roku 1853 v anglickém časopisu *Quarterly Review:*

„Rovněž je třeba přijmout opatření týkající se vážného problému, jímž je v dnešní době obtěžkána komunikace telegrafní, a sice narušení veškerého soukromí. Za současného stavu věcí je vždy dobrý půltucet lidí obeznámen s obsahem zprávy, již zasílá jedna osoba druhé. Jakkoli jsou úředníci Anglické telegrafní společnosti *vázáni* přísahou, je zřejmé, že často píšeme sdělení, u nichž nelze tolerovati, aby je četl kdokoli cizí dříve než zamýšlený adresát. Toto je těžká vada telegrafie, již je třeba napraviti tím či oním způsobem."

Řešení spočívá v zašifrování zprávy předtím, než se předá telegra-fistovi. Ten pak převede do morseovky šifrový text. Nejen že se tím zabrání operátorovi ve čtení citlivého textu, ale rovněž se zmaří úsilí každého špiona, který by odposlouchával telegrafní komunikaci. Prokazatelně nejlepším způsobem utajení

důležité obchodní korespondence byla polyalfabetická Vigenerova šifra. Protože byla pokládána za nerozluštitelnou, vešla ve známost jako *le chiffre indéchiffrable* (nerozluštitelná šifra). Kryptografové získali - přinejmenším na nějakou dobu - převahu nad kryptoanalytiky.

Pan Babbage versus Vigeněrova šifra

Nejpozoruhodnější postavou kryptoanalýzy 19. století je Charles Babbage, výstřední britský génius, jenž se proslavil především koncepčním návrhem moderního počítače. Narodil se roku 1791,jeho otcem byl bohatý londýnský bankéř Benjamin Babbage. Když se Charles proti otcově vůli oženil, ztratil přístup k rodinnému majetku, ale stále měl dost peněz na to, aby zůstal finančně *zabezpečen* a aby mohl strávit život jako nezávislý učenec, jenž se zabývá jakýmkoli problémem, který ho právě zaujme. K jeho vynálezům patří rychloměr stejně jako lapač krav - zařízení, jež se připevňovalo na přední část parní lokomotivy, aby odehnalo dobytek z kolejí. Pokud jde o vědecké objevy, Babbage si jako první povšiml souvislosti mezi letokruhy a stářím stromu, přičemž správně usoudil, že z velmi starých stromů lze získat poznatky o klimatu dávných dob. Rovněž se zajímal o statistiku a pro rozptýlení si sestavil první tabulky úmrtnosti, dnes základní nástroj v pojišťovnictví.

Babbage se neomezoval jen na vědecké a technické problémy. V jeho době se výše poštovného u dopisu odvozovala od vzdálenosti, na kterou je dopis odesílán. Babbage upozornil, že práce spojená s výpočtem vzdálenosti stojí víc, než kolik činí poštovné. Navrhl systém poštovného, který používáme v rámci jedné země dnes - jednotnou cenu bez ohledu na bydliště adresáta. Zajímal se rovněž o politické a sociální otázky, ke konci svého života uspořádal kampaň za vyhnání flašinetářů a potulných muzikantů z Londýna. Stěžoval si, že jejich hudba „nikoli zřídka povzbuzuje k tanci malé otrhané ničemy, někdy i osoby podnapilé, jež se pak často přidávají a svými dis-harmonickými hlasy ještě zvětšují množství hluku. Jinou třídou společenskou, jež patří k zastáncům pouliční hudby, jsou dámy, jejichž ctnost je pozoruhodně vrtkavá, dámy kosmopolitních sklonů, jež tak získávají vhodnou záminku, jak ukájet vlastní zvědavost u otevřených oken". Babbage se však dočkal pomsty, neboť hudebníci se na oplátku scházeli ve velkých skupinách kolem jeho domu a tam hráli, jak jen nejhlasitěji dovedli.

Obrat v Babbagově vědecké kariéře nastal roku 1821, kdy se spolu s astronomem Johnem Herschelem zabýval sadou matematických tabulek používaných při astronomických, technických a navigačních výpočtech. Oba muži byli znechuceni množstvím chyb, jež v tabulkách našli. Tyto chyby mohly vést k závažným nepřesnostem při výpočtech. Jedna sada

takových tabulek *(Nautické efemeridy pro nalezení zeměpisné šířky a délky na moří)* obsahovala přes tisícovku chyb. Těmto chybám se přičítalo mnoho ztroskotání lodí a technických katastrof.

Matematické tabulky se sestavovaly ručně, chyby byly důsledkem selhání lidského faktoru. Babbage prohlásil: „Kéž by Bůh dal a tyto výpočty mohla pohánět pára!" Tím začalo podivuhodné dobrodružství, snaha postavit stroj schopný sestavit takové tabulky bezchybně a s vysokou přesností. Roku 1823 navrhl Babbage tzv. *Dif-ference Engine No. 1* - obrovský kalkulátor sestávající z 25 000 mechanických součástek, jenž měl být postaven za vládní peníze. Babbage, ač geniální vynálezce, nedovedl své projekty uvést do života. Po deseti letech pachtění zcela opustil *Difference Engine No. 1*, sestavil nový plán a zahájil práce na *Difference Engine No. 2.*

Když Babbage zanechal práce na prvním stroji, vláda ztratila důvěru v jeho záměry, rozhodla se omezit své ztráty a z projektu se stáhla. Tou dobou již výdaje dosáhly 17 470 liber, což by stačilo na stavbu dvou bitevních lodí. Patrně právě proto si Babbage později postěžoval: „Navrhněte Angličanovi jakýkoli princip, jakýkoli nástroj, třeba sebeobdivuhodnější, a seznáte, že veškeré úsilí jeho mysli je obráceno k tomu, aby na novince našel obtíž, chybu či nemožnost realizace. Budete-li mu vyprávět o stroji na škrábání brambor, prohlásí, že něco takového je nemožné. Když stroj oškrábe bramboru před jeho očima, řekne, že to je stejně k ničemu, protože nedovede oloupat ananas."

Kvůli nedostatku prostředků Babbage nikdy nedokončil svůj *Difference Engine No. 2.* Vědecká tragédie spočívala v tom, že tentostroj byl přímým předstupněm tzv. *Analytical Engine.* Ten už neměl sestavovat předem danou sadu tabulek, ale řešit širokou škálu matematických problémů podle vložených instrukcí. *Analytical Engine* je předobrazem dnešních počítačů. Struktura stroje obsahovala „sklad" (paměť) a „mlýnici" (procesor), *což* mu umožňovalo činit rozhodnutí a opakovat instrukce, přesně jako to dělají dnešní počítače pomocí příkazů IF ... THEN ... a LOOP.

O století později, během druhé světové války, to byla právě první elektronická realizace Babbagova stroje, která se zasloužila o velký pokrok v kryptoanalýze. Avšak již za svého života přispěl Babbage k rozvoji této oblasti zásadním způsobem: dokázal rozluštit Vige-nerovu šifru a učinil tak největší pokrok v kryptoanalýze od 9. století, kdy arabští učenci objevili frekvenční analýzu a rozluštili s její pomocí monoalfabetickou substituční šifru. Babbagův postup nevyžadoval žádné složité výpočty ani mechanické pomůcky. Stačila jen dobrá hlava.

Babbage se o šifry zajímal od dětství. Později napsal, jak ho tato záliba občas dostala do potíží: „Starší chlapci vymýšleli šifry, ale mně se obvykle už z několika slov podařilo najít klíč. Důsledky této dovednosti bývaly bolestivé: tvůrci takové

šifry mě dost často zbili, přestože chyba spočívala jen v jejich vlastní hlouposti." Výprasky ho neodradily, kryptoanalýza byla pro něj i nadále přitažlivá. Ve své autobiografii napsal, že „luštění šifer je podle mého názoru tou nejvíce fascinující ze všech dovedností".

V londýnské společnosti si Babbage brzy vydobyl pověst krypto-analytika připraveného zdolat každou šifrovanou zprávu, a proto se na něj cizí lidé obraceli s nejrůznějšími problémy. Bezradnému ži-votopisci pomohl například rozluštit rukopisné poznámky prvního anglického královského astronoma Johna Flamsteeda. Stal se spásou pro historika, jenž potřeboval přečíst šifru Henrietty Marie, manželky anglického krále Karla I. Roku 1854 spolupracoval s advokátem a použil kryptoanalýzu k odhalení klíčového důkazu v právní při. Během let nashromáždil silný svazek dešifrovaných zpráv, jež hodlal použít jako základ autorské knihy o kryptoanalýze, pro niž zvolil název *The Philosophy ofDecyphering* (Filozofie dešifrování). Kniha měla obsahovat po dvou příkladech každého typu šifry, jeden ukázkově rozluštěný, druhý ponechaný jako cvičení pro čtenáře. Bohužel, kniha dopadla stejně jako mnoho jeho dalších grandiózních plánů - zůstala nedokončena.

Zatímco většina kryptoanalytiků se vzdala veškeré naděje na rozluštění Vigeněrovy šifry, Babbage byl k takovému pokusu inspirován výměnou korespondence s bristolským zubařem jménem John Hall Brock Thwaites, jehož pohled na šifrování byl poněkud přímočarý. Roku 1854 Thwaites prohlásil, že vytvořil zcela novou šifru, která však ve skutečnosti byla ekvivalentem Vigenerovy šifry. Napsal sdělení do časopisu *Journal of the Society of Arts* (List Společnosti nauk) se záměrem patentovat svůj nápad, přičemž si očividně nebyl vědom, že je starý několik set let. Babbage pak Společnosti sdělil, že „tato šifra je velmi stará a dá se najít ve většině knih". Thwaitese to nijak nerozházelo a vyzval Babbage, ať se pokusí jeho šifru rozluštit. To, zda lze šifru rozluštit nebo ne, nemělo samozřejmě žádný vztah k otázce jejího autorství, avšak *výzva,* vzbudila Babbagovu zvědavost. Začal tedy hledat ve Vigenerově šifře slabiny.

Luštění obtížné šifry se podobá zlézání strmé skalní stěny. Krypto-analytik hledá každou sebemenší škvíru a skulinu, která by mohla pomoci v cestě vzhůru. U monoalfabetické šifry se lze chytit frekvence hlásek, neboť nejběžnější písmena jako e, t a a se nakonec prozradí, ať už byla ukryta jakkoli. U polyalfabetické Vigenerovy šifry jsou frekvence daleko vyrovnanější, protože se při šifrování přepíná mezi abecedami pomocí klíče. Skalní stěna je na první pohled dokonale hladká.

Připomeňme si, že zásadní výhoda Vigenerovy šifry spočívá v tom, že stejné písmeno lze zašifrovat více způsoby. Zní-li například klíčové slovo KING („král"), pak může být každé písmeno otevřeného textu potenciálně šifrováno čtyřmi různými způsoby, neboť klíčové slovo sestává ze čtyř písmen. Každé písmeno klíčového slova definuje jinou šifrovou abecedu - součást Vigeněrova čtverce - jak je to vidět v tabulce 7. Zvýraznili jsme sloupec e, aby bylo patrné, jak se toto písmeno zašifruje čtyřmi různými způsoby v závislosti na tom, který znak klíčového slova byl použit:

Jestliže šifrování definuje písmeno K slova KING,

pak znaku e v otevřeném textu odpovídá 0 v šifrovém textu. Jestliže šifrování definuje písmeno I slova KING,

pak znaku e v otevřeném textu odpovídá M v šifrovém textu. Jestliže šifrování definuje písmeno N slova KING,

pak znaku e v otevřeném textu odpovídá R v šifrovém textu. Jestliže šifrování definuje písmeno G slova KING,

pak znaku e v otevřeném textu odpovídá K v šifrovém textu.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabulka 7: Vigeněrův čtverec použitý v kombinaci s klíčovým slovem KING. Klíčové slovo definuje čtyři různé šifrové abecedy, takže písmeno **e** se může zašifrovat jako O, M, R nebo **K.**

Z toho plyne, že i celá slova budou šifrována různými způsoby. Například slovo the (anglický určitý člen) se zašifruje jako DPR, BUK, GNO nebo ZRM podle toho, v jaké se nachází poloze vůči klíčovému slovu. Kryptoanalýza se tím komplikuje, není však nemožná. Je důležité si uvědomit, že existují jen čtyři způsoby, jak zašifrovat the. Pokud otevřený text obsahuje toto slovo několikrát, pak je velmi pravděpodobné, že některé ze čtyř jeho možných zašifrování se budou v šifrovém textu opakovat. To vidíme na následující ukázce, kde je fráze The Sun and the Man in the Moon (Slunce a muž na Měsíci) zašifrována pomocí Vigenerovy šifry a klíčového slova KING.

Klíčové slovo KINGKINGKINGKINGKINGKING Otevřený text thesunandthemaninthemoon šifrovýtext DPRYEVNTNBUKWIAOXBUKWWBT

Slovo the je zde poprvé zašifrováno jako DPR, podruhé a potřetí jako BUK. Důvod, proč se BUK opakuje dvakrát, spočívá v tom, že třetí the je v otevřeném textu vzdáleno osm písmen od druhého a osm je násobkem délky klíčového slova, tedy čtyř. Jinými slovy, druhé the bylo šifrováno podle písmen ING klíčového slova, třetí the pak podle týchž písmen, protože než jsme k němu dospěli, klíčové slovo se zopakovalo přesně dvakrát.

Babbage si povšiml, že tato pravidelnost mu může poskytnout právě ten opěrný bod, který potřeboval, aby mohl začít Vigenerovu šifru dobývat. Podařilo se mu definovat řadu poměrně jednoduchých kroků, jež mohl zopakovat každý kryptoanalytik zápasící s *chiffre indécbiffrable.* Abychom si předvedli jeho brilantní techniku, předpokládejme, že jsme zachytili šifrový text, jenž je na obrázku 13. Víme, že byl šifrován Vigeněrovou šifrou, nevíme však nic o původní zprávě a klíč je rovněž neznámý.

První krok Babbagovy kryptoanalýzy spočívá v hledání sekvencí, jež se opakují v šifrovém textu vícekrát. Takové opakování může vzniknout dvěma způsoby. Nejpravděpodobnější je, že táž sekvence

Obrázek 13: Šifrový text vzniklý aplikací Vigeněrovy šifry.písmen v otevřeném textu byla zašifrována touž částí klíče. Vedle toho však existuje i méně pravděpodobná možnost, že dvě odlišné sekvence písmen v otevřeném textu byly zašifrovány rozdílnými částmi klíče a náhodou poskytly týž výsledek - stejné pořadí písmen v šifrovém textu. Omezíme-li se na delší sekvence, pak je druhá možnost velmi nepravděpodobná. Proto bychom si měli všímat jen sekvencí o délce čtyř znaků a více. V tabulce 8 najdeme seznam takových opakujících se sekvencí včetně vzdáleností mezi nimi. Například sekvence E-F-I-Q se nachází v prvním a pak v pátém řádku šifrového textu, vzdálenost mezi oběma výskyty činí 95 písmen.

Klíčové slovo se nepoužívá jen k šifrování, ale samozřejmě také k dešifrování.

Pokud jej tedy dokážeme identifikovat, je dešifrování snadné. Zatím nemáme dost informací, abychom dokázali nalézt klíčové slovo, ale tabulka 8 poskytuje dobrou nápovědu, pokud jde o jeho délku. Vedle toho, které sekvence se opakují a jak jsou od sebe vzdáleny, obsahuje zbytek tabulky pomocné údaje, tzv. *faktory opakování* - čísla, jež jsou děliteli vzdálenosti mezi opakováním sekvencí. Například sekvence W-C-X-Y-M se opakuje po dvaceti písmenech, faktory jsou proto čísla 1, 2, 4, 5 a 20, protože ta jsou celočíselnými děliteli čísla 20 (dělí jej beze zbytku). Z toho plyne šest možností:

Klíč tvoří 1 písmeno a opakuje se 20x mezi sekvencemi. Klíč tvoří 2 písmena a opakuje se l0x mezi sekvencemi. Klíč tvoří 4 písmena a opakuje se 5x mezi sekvencemi. Klíč tvoří 5 písmen a opakuje se 4x mezi sekvencemi. Klíč tvoří 10 písmen a opakuje se 2x mezi sekvencemi. Klíč tvoří 20 písmen a opakuje se lx mezi sekvencemi.

Opakovaná sekvence	Interval mezi opakováním	Možná délka klíče																	
		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
E-F-I-Q	95				✓														✓	
P-S-D-L-P	5				✓															
W-C-X-Y-M	20	✓		✓	✓					✓										✓
E-T-R-L	120	✓	✓	✓	✓	✓		✓		✓		✓			✓					✓

Tabulka 8: Opakování a intervaly mezi nimi uvnitř šifrového textu.

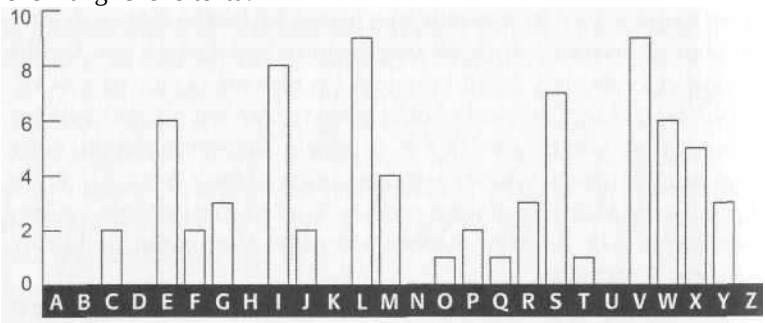
První možnost lze vyloučit, protože klíč o délce 1 znaku odpovídá monoalfabetické šifře - použil by se k ní jen jeden řádek Vigenerova čtverce a šifrová abeceda by se neměnila. Je nepravděpodobné, že by kryptograf udělal právě tohle. Všechny další možnosti jsou označeny v příslušném sloupci tabulky 8 zaškrtnutím. To indikuje možnou délku klíče.

Abychom určili, zda je klíč dlouhý 2, 4, 5,10 či 20 písmen, musíme se podrobněji podívat na faktory u ostatních sekvencí. Zdá se, že klíč tvoří maximálně 20 písmen, proto se tabulka 8 *zabývá*, jen hodnotami opakování menšími nebo rovnými dvaceti a obsahuje všechny faktory u všech sekvencí, jež se do tohoto rozmezí vejdou. Tendence k opakování klíče, jehož délka je dělitelná pěti, je zřejmá: v podstatě mu odpovídají všechny výskyty opakujících se sekvencí. První z nich E-F-I-Q lze vysvětlit jako účinek klíčového slova o délce 5, jež se mezi prvním a druhým zašifrováním zopakovalo 19x. Druhá opakující se sekvence P-S-D-L-P může být objasněna jako účinek klíče o délce 5, který se mezi oběma výskyty téže fráze zopakoval jen jednou. Třetí sekvence W-C-X-Y-M odpovídá klíčovému slovu o délce 5, jež se mezi oběma výskyty zopakovalo čtyřikrát. Čtvrtá E-T-R-L je vysvětlitelná klíčovým slovem o délce 5, jež se mezi oběma výskyty zopakovalo 24x. Zkrátka a dobře, vše nasvědčuje tomu, že klíčové slovo má 5 písmen.

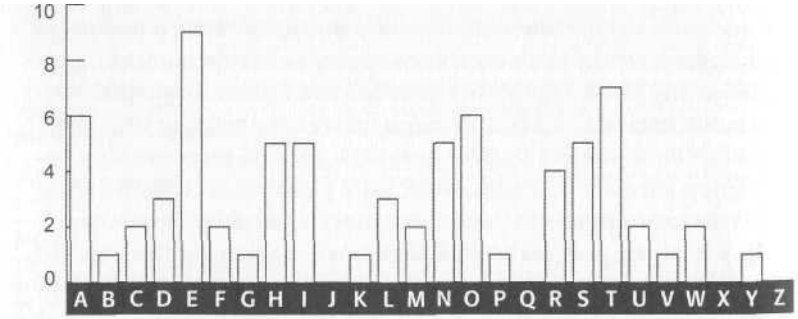
Za tohoto předpokladu se pokusíme zjistit, jak klíčové slovo zní. Prozatím si jej označíme jako L1-L2-L3-L4-L5, přičemž *L1* označuje první písmeno klíče a tak

dále. Šifrování probíhalo tak, že první písmeno otevřeného textu bylo zašifrováno pomocí prvního písmene klíče, tedy L1. Je to právě *L1*, které definuje jeden z řádků Vigenerova čtverce a tím určuje monoalfabetickou substituční šifru pro první znak zprávy. Druhý znak otevřeného textu se šifruje pomocí L_2, jež definuje jiný řádek Vigeněrova čtverce a tím i jinou monoalfabetickou substituční šifru. Třetí písmeno otevřeného textu se šifruje pomocí L_3, čtvrté pomocí L_4, páté pomocí L_5. Každé písmeno klíče určuje jinou šifrovou abecedu. Avšak šesté písmeno otevřeného textu se šifruje znovu pomocí L1 sedmé pomocí L_2 a cyklus se dál opakuje. Jinými slovy, polyalfabetická šifra sestává z pěti monoalfabetic-kých šifer a každá z nich šifruje jednu pětinu textu zprávy. Monoalfabetickou substituční šifru, jak známo, luštit dovedeme.

Dál pokračujeme následujícím způsobem: víme již, že jeden z řádků Vigenerova čtverce, definovaný písmenem L1, tvoří šifrovou abe-cedu pro 1., 6., 11., 16.,... znak *zprávy*. Pokud tedy vezmeme z šifrového textu právě tyto znaky, budeme je moci podrobit staré dobré frekvenční analýze. Obrázek 14 ukazuje, jak dopadla frekvenční analýza těchto znaků, jimiž jsou W, I, R, E. Připomeňme si na tomto místě, že každá šifrová abeceda ve Vigenerově čtverci je obyčejnou abecedou posunutou o nějakou hodnotu mezi 1 a 26. Frekvenční distribuce na obrázku 14 má proto stejné vlastnosti jako frekvenční distribuce obyčejné anglické abecedy, jen s tím rozdílem, že její počátek je posunut o nějakou neznámou hodnotu. Porovnáním distribuce L1 s distribucí normální abecedy by se nám mohlo podařit zjistit, o jaké posunutí se jedná. Obrázek 15 ukazuje standardní frekvenční rozložení anglického textu.

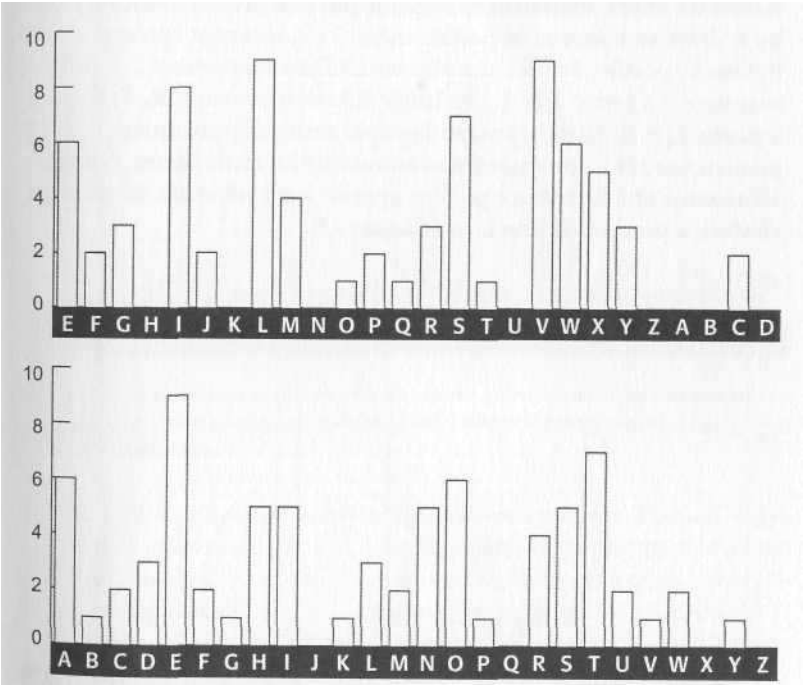


Obrázek 14: Frekvenční rozložení písmen v šifrovém textu, jež jsou šifrovány pomocí abecedy *L1* (na svislé ose jsou počty výskytů jednotlivých znaků).



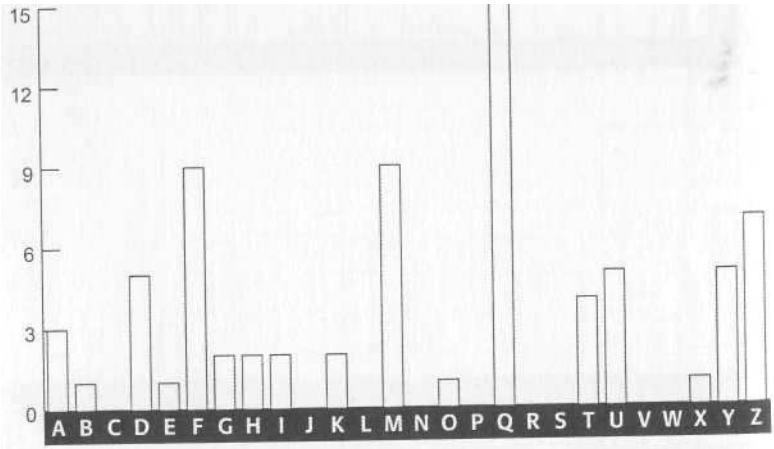
Obrázek 15: Standardní frekvenční rozložení (počet výskytů písmen v ukázce otevřeného textu stejné délky, jakou má šifrový text).

Standardní rozložení má své vrcholy, údolí a náhorní plošiny. Když se je snažíme srovnat s rozložením L1 je třeba se zaměřit na jeho nejvýraznější rysy. Tak například tři vrcholy R-S-T v normálním *rozložení* (obrázek 15) a napravo od nich dlouhý pokles, jež se táhne přes šest písmen od U až po Z, představuje velmi zřetelný vzor. Jediným podobným útvarem v rozložení L1 (obrázek 14) jsou tři vrcholy u V-W-X následované poklesem přes šest písmen od Y po D. Z toho by se dalo usoudit, že všechny znaky šifrované pomocí L1 jsou oproti normální abecedě posunuty o čtyři písmena (čili že L1 je abecedou, která zní E, F, G, H,...) a že samo L1 - první písmeno klíčového slova - je písmeno E. Tuto hypotézu je možné testovat tak, že posuneme rozložení L1 o čtyři písmena nazpět a porovnáme je se standardním rozložením. Obrázek 16 ukazuje takové srovnání. Shoda je značná a dá se z ní usoudit, že L1 můžeme skutečně pokládat za E.

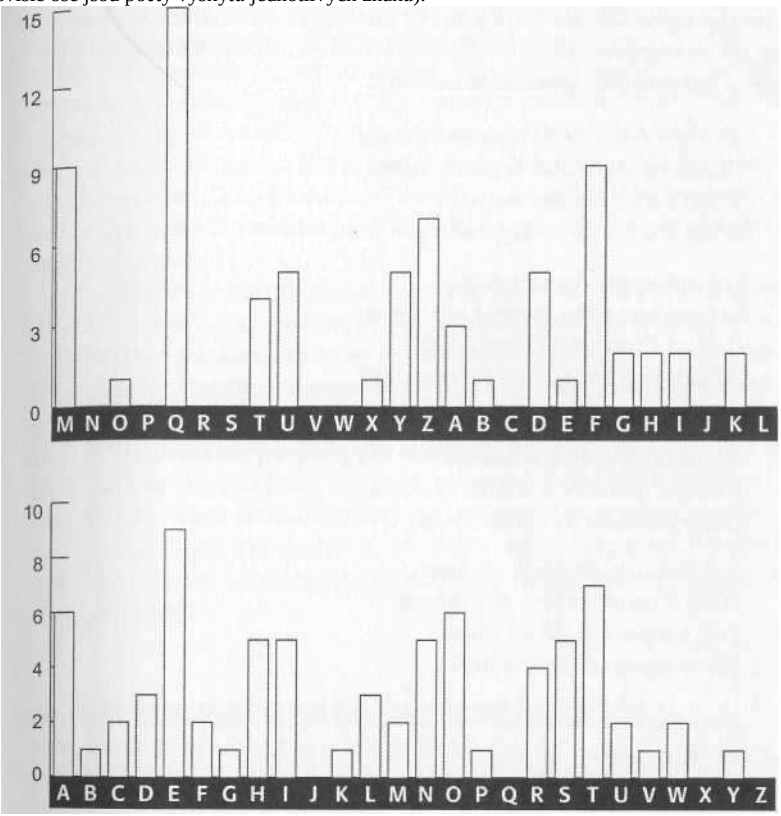


Obrázek 16: Rozložení L1 posunuté o čtyři písmena zpět (nahoře) porovnané se standardním frekvenčním rozložením (dole). Všechny hlavní vrcholy a poklesy si vzájemně odpovídají.Shrňme dosavadní postup. Hledání opakujících se sekvencí v šifrovém textu nám umožnilo identifikovat délku klíče; ten má pět znaků. Díky této znalosti jsme mohli rozdělit šifrový text na pět částí, z nichž každá je šifrována jednou monoalfabetickou substituční šifrou. Analýzou té části šifrového textu, jež odpovídá prvnímu písmenu klíče, jsme zjistili, že toto písmeno *L1* je patrně E. Tento proces můžeme nyní zopakovat pro 2., 7., 12., 17.,... znak šifrového textu. Odpovídající rozložení, jež vidíme na obrázku 17, je třeba znovu porovnat se standardním rozložením a zkusit uhodnout délku posunutí.

Tentokrát je to těžší. Žádné tři vrcholy odpovídající R-S-T nejsou vidět. Na druhou stranu, pokles mezi G a L je velmi výrazný a mohl by odpovídat písmenům U až Z z normálního rozložení. Pokud by tomu tak bylo, pak by se tři vrcholy R-S-T měly objevit u D-E-F, avšak vrchol u E chybí. Prozatím to budeme považovat za statistickou chybu a držet se názoru, že pokles mezi G a L ukazuje správný směr. Potom by platilo, že všechna písmena šifrovaná pomocí L_2 jsou posunuta o 12 pozic a že L_2 definuje šifrovou abecedu M, N, 0, P,..., a proto L_2= M. Tuto hypotézu lze opět testovat posunutím L_2 o 12 písmen nazpět a porovnáním se standardním rozložením. Obrázek 18 ukazuje obě distribuce po této operaci a je z něj vidět, že shoda je značná, a proto můžeme L_2 pokládat za M.



Obrázek 17: Frekvenční rozložení písmen v šifrovém textu, jež jsou šifrována pomocí abecedy L_2 (na svislé ose jsou počty výskytů jednotlivých znaků).



Obrázek 18: Rozložení L_2 posunuté o 12 písmen zpět (nahoře) a porovnané se standardním frekvenčním rozložením (dole). Většina hlavních vrcholů a poklesů si vzájemně odpovídá.

Dál již v podrobné analýze nebudu pokračovat. Postačí, když uvedu, že analýzou 3., 8., 13.,... znaku zjistíme, že třetím písmenem klíče je I, analýza 4., 9., 14.,... znaku ukáže, že čtvrtým písmenem klí-če je L, akonečně z 5., 10., 15.,... znaku zjistíme, že pátým písmenem je Y. Klíčové slovo zní EM ILY. Teď již lze Vigenerovu šifru normálním způsobem dešifrovat. První písmeno šifrového textu je W a bylo zašifrováno pomocí prvního písmene klíče, jímž je E. Podíváme se do Vigenerova čtverce, najdeme W v řádku, jenž *začíná*, písmenem E, a zjistíme, které písmeno je na vrcholu příslušného sloupce. Jde o s, které tak je prvním písmenem ote-vřeného textu. Opakováním procesu zjistíme, že otevřený text začíná písmeny sittheedownandhavenoshamecheekbyjowl...Vložíme-limezislovame-zery a interpunkci, dostaneme nakonec:

Sit thee down, and háve no shame, Cheek by jowl, and knee by knee: What care I for any name? What for order or degree?

Let me screw thee up a peg: Let me loose thy tongue with wine: Callest thou that thing a leg? Which is thinnest? thine or mine?

Thou shalt not be saved by works: Thou hast been a sinner too: Ruined trunks on withered forks, Empty scarecrows, I and you!

Fill the cup, and fill the can: Háve a rouše before the morn: Every moment dies a man, Every moment one is born.

Jde o verše z básně Alfreda Tennysona, jež se jmenuje *The Vision ofSin* (Představa hříchu). Klíčové slovo je křestním jménem Ten-nysonovy manželky Emily Sellwoodové. Tento úryvek jsem zvolil právě proto, že se stal příčinou kuriózní korespondence mezi Babbagem a velkým básníkem. Babbage jako nadšený statistik a autor tabulek mortality byl podrážděn veršem „Every moment dies a man/Every moment one is born" (Každou chvíli člověk zemře/a jiný se narodí). Navrhl proto vylepšení Tennysonovy „jinak pěkné" básně:

‚Je třeba zdůraznit, že kdyby toto byla pravda, pak by celková populace světa zůstávala neměnná... Dovoluji si navrhnout, abyste v příštím vydání své verše opravil na znění: ‚Každou chvíli člověk zemře/a 1 1/16 jiného se narodí.'... Přesná hodnota má příliš mnoho desetinných míst, než aby se vešla na jeden řádek, avšak mám za to, že číslo 1 1/16 představuje přesnost dostatečnou pro účely poezie.

S pozdravem,

Charles Babbage."

Babbage si s Vigenerovou šifrou úspěšně poradil patrně roku 1854; krátce po střetu s Thwaitesem, avšak o jeho objevu se nikdo nedověděl, protože jej nepublikoval. Vyšel najevo až při průzkumu jeho poznámek ve 20. století. Stejný postup mezitím objevil nezávisle na Babbagovi vysloužilý důstojník pruské armády Friedrich Wil-helm Kasiski. Od roku 1863, kdy jej publikoval v knize *Die Geheim-schriften und die Dechiffrirkunst* (Tajné šifry a umění je dešifrovat), je příslušná technika známa jako Kasiského test. Babbagův vklad byl zcela ignorován.

Proč Babbage nepublikoval prolomení tak silné šifry? Je známo, že měl ve zvyku zanechávat projekty v nedokončeném stavu a nepublikovat výsledky, takže by se mohlo jednat o další projev jeho flegmatické povahy. Existuje však i jiné

vysvětlení. Babbagův objev přišel krátce poté, co vypukla krymská válka. Podle jedné z teorií tím získala britská rozvědka převahu nad Rusy. Je klidně možné, že výzvědná služba požádala Babbage, aby svůj objev utajil, a poskytl jí tak před zbytkem světa devítiletý náskok. Je-li tento názor pravdivý, zapadá dobře do dlouholeté tradice utajování kryptoanalytických objevů v zájmu národní bezpečnosti - tradice, jež pokračuje do dnešních dnů.

Od sloupků utrpení k zakopanému pokladu

Díky objevům, jichž dosáhli Charles Babbage a Friedrich Kasiski, již nebyla Vigenerova šifra bezpečná. Kryptografové nemohli nadále zaručit stoprocentní utajení a převahy v komunikační válce nabyli opět kryptoanalytici. Přestože se kryptografové snažili navrhnout nové šifry, nic podstatného se v druhé polovině 19. století již neobjevilo a profesionální kryptografie byla v úpadku. V téže době však došlo k velkému nárůstu zájmu o kryptografii mezi veřejností.

Hlavní příčina tohoto nárůstu byla stejná jako u obchodní sféry: byl jí rozvoj telegrafu. Veřejnost si uvědomovala, že citlivé osobní zprávy je třeba chránit a v případě potřeby je i zašifrovat, přestože se tím zpomalovalo odeslání a rostla cena telegramu. Tehdejší telegrafisté dovedli odesílat běžné zprávy rychlostí kolem 35 slov za minutu, protože si při přepisu zapamatovali celou frázi a tu pak odeslali najednou. Změť písmen tvořící šifrový text se převáděla do morseovky mnohem obtížněji, protože telegrafista musel neustálenahlížet do blanketu a kontrolovat jedno písmeno po druhém. Šifry, jež používala veřejnost, by před profesionálním kryptoanalyti-kem neobstály, ale před náhodnými čmuchaly představovaly dostatečnou ochranu.

Čím více byla veřejnost s šiframi obeznámena, tím rozmanitější způsoby utajené komunikace používala. Tak například mladé páry ve viktoriánské Anglii zpravidla nesměly dávat veřejně najevo svou vzájemnou náklonnost ani si nemohly posílat dopisy, neboť by jim je četli rodiče. Proto mladí milenci často komunikovali pomocí šifrovaných sdělení otiskovaných v inzertních rubrikách novin. Tyto „sloupky utrpení", jak se jim říkalo, provokovaly zvědavost kryptoanalytiků, kteří často zkoušeli rozluštit jejich choulostivý obsah. Liboval si v tom i Charles Babbage spolu se svými přáteli sirem Charlesem Wheatstonem a baronem Lyonem Playfairem. Rovněž společně vyvinuli zajímavou Playfairovu šifru (popsanou v příloze E). Jednou se stalo, že Wheatstone dešifroval sdělení, jež zaslal do *The Times* student z Oxfordu. Navrhoval v něm své milé, že by mohli společně utéci z domova. O několik dní později zveřejnil Wheatstone své vlastní sdělení, v němž mladému páru tuto odbojnou a neuváženou akci rozmlouval. Krátce poté se objevila třetí zpráva, tentokrát nešifrovaná a psaná řečenou dámou: „Drahý Charlie, už nepiš. Náš kód byl prozrazen."

Postupem času se v novinách objevovalo stále více šifrovaných sdělení. Kryptografové tak často *vyzývali* své kolegy k soutěži. Jindy se zas šifrovaných sdělení používalo ke kritice jednotlivců i organizací. *The Times* jednou nevědomky otiskly šifrované sdělení: „*The Times* jsou tiskovým Jeffreysem." Soudce Jeffreys, k němuž tak byly noviny přirovnány, žil v 17. století; přirovnání říkalo zhruba tolik, že jde o bezohlednou tiskovinu sloužící jako hlásná trouba vlády.

Jiným dokladem dobré obeznámenosti s kryptografií bylo všeobecné používání dírkového kódu. Starověký řecký historik Aeneas Tacticus navrhl, jak zaslat tajnou zprávu vypichováním drobných dírek pod vybraná písmena na jinak očividně nevinné stránce textu stejným způsobem, jako jsou pod některými písmeny tohoto odstavce umístěny tečky. Písmena označená vpichem dohromady tvořila tajnou zprávu, již si určený příjemce mohl snadno přečíst. Posel nebo jiný zprostředkovatel by si však drobných dírek patrně vůbec nevšiml. O dva tisíce let později používali Britové při psaní dopisů stejnou metodu - ne kvůli utajení, ale kvůli poštovnému. Až do přebudování poštovního systému v polovině 19. století stálo odeslání dopisu asi šilink za každých sto mil, což bylo nad možnosti většiny lidí- Noviny se však doručovaly zdarma, což poskytlo šetrným vik-toriáncům šikovnou únikovou cestu. Namísto psaní a odesílání dopisů lidé píchali špendlíkem do titulní stránky novin, jež pak mohli odeslat poštou a přitom nezaplatit ani penny.

Díky rostoucímu zájmu veřejnosti o kryptografické techniky si kódy a šifry rychle našly cestu do literatury 19. století. Ve Vernově *Cestě do středu Země je* prvním krokem dobrodružné výpravy dešifrování runového nápisu ze starého pergamenu. Znaky jsou součástí substituční šifry, která ukrývá latinský text, jenž dává smysl, je-li čten pozpátku: „Sestoupíš-li do toho kráteru Sneffelsu, který polí-bí stín Skartarisu prvého července, odvážný cestovateli, dospěješ středu Země." Roku 1885 použil Jules Verne šifru jako klíčovou rekvizitu v románu *Matyáš Sandorf.* V Británii patřil k předním průkopníkům prózy s kryptografickými motivy sir Arthur Conan Doyle. Nepřekvapí, že Sherlock Holmes byl odborníkem na poli kryptografie a také že, jak jednou vysvětlil dr. Watsonovi, „je autorem drobné monografie na toto téma, analyzující sto šedesát rozličných šifer". Nejslavnějším z Holmesových dobrodružství, v nichž hrají roli šifry, je příběh *Tančící figurky* (The Adventure of the Dancing Man) z knihy *Návrat Sherlocka Holmese,* kde se objevuje šifra složená z drobných lidských postaviček, jejichž různé pozice znázorňují různá písmena.

Na druhé straně Atlantiku popularizoval kryptografii Edgar Allan Poe. Ve filadelfském týdeníku *Alexander's Weekly Messenger zveřejnil* výzvu čtenářům, v níž uvedl, že dokáže rozluštit každou mo-noalfabetickou substituční šifru. Své šifrované texty zaslaly stovky čtenářů - a Poe je všechny rozluštil. Přestože nešlo o nic jiného než o prostou frekvenční analýzu, Poeovi čtenáři byli jeho dovedností ohromeni. Jeden z obdivovatelů ho prohlásil za „nejdovednějšího luštitele šifer, jaký kdy žil".

Obrázek 19: Část šifrového textu z povídky *Tančící figurky* z knihy sira Arthura Conana Doyla *Návrat Sherlocka Holmese.*Roku 1843 se Poe pokusil využít takto vzbuzeného zájmu a napsal povídku, jež je dodnes profesionálními kryptografy pokládána za nejdokonalejší prózu týkající se jejich oboru. *Zlatý skarabeus*

(The Gold Bug) vypráví příběh Williama Legranda, který objeví neobvyklého brouka, chytí jej a *zabalí* do kusu papíru, který najde poblíž. Téhož večera si brouka načrtne na týž papír, který pak přidrží u ohně, aby na jasném světle ověřil přesnost kresby. Namísto kresby však uvidí nápis tajným písmem, který se objevil po nahřáti na papíře. Legrand prozkoumá nápis a nabude přesvědčení, že jde o šifrované instrukce udávající, kde nalézt ukrytý poklad kapitána Kidda. Zbytek povídky je klasickou ukázkou frekvenční *analýzy*, *jež* vyvrcholí rozluštěním všech tajemství kapitána Kidda a nalezením pokladu.

Přestože je *Zlatý skarabeus* čistá fikce, existuje pravdivý příběh z 19. století, jenž se mu velmi podobá. Případ Bealových šifer popisuje dobrodružství z Divokého západu - vypráví o kovboji, který pohádkově zbohatl, o zakopaném pokladu v hodnotě 20 milionů dolarů a o tajemné sadě šifrovaných textů, v nichž je umístění pokladu popsáno. Většina toho, co o příběhu víme, pochází z brožury publikované roku 1885. Přestože má jen 23 stran, byla hádankou pro celé generace kryptoanalytiků a neodolatelným lákadlem pro stovky hledačů pokladů.

Příběh začíná v hotelu Washington v Lynchburgu ve státě Virgi-nia, a to 65 let před vydáním zmíněné brožury. Podle jejího textu se hotel i jeho majitel Robert Morriss těšili vynikající pověsti: Jeho příhodné umístění, dokonalá bezúhonnost, vynikající vedení i obsluha jej brzy proslavily a jeho reputace se šířila i do sousedních států. Byl nejlepším domem ve městě a žádný z dýchánků lepší společnosti se nepořádal jinde." V lednu 1820 přijel do Lynchburgu cizinec jménem Thomas J. Beale aubytoval se v hotelu Washington. „Byl vysoký asi šest stop," vzpomínal na něj Morriss, „s očima černýma jako uhel a vlasy téže barvy, delšími, než bylo tou dobou v módě. Postavu měl souměrnou a bylo na něm znát, že je silný a aktivní; jeho hlavním znamením však byl snědý vzhled, jako by dlouho pobýval na slunci a větru. To mu však neubíralo na pěkném vzhledu, byl patrně nejpřitažlivějším mužem, jakého jsem kdy potkal." Přestože Beale strávil zbytek zimy v Morrissově společnosti a „byl velmi oblíben u všech, zejména pak u dam", nikdy nemluvil o své minulosti, o rodině ani o účelu své návštěvy. Koncem března pak zmizel stejně náhle, jako se objevil.

O dva roky později, v lednu 1822, se Beale vrátil do hotelu Washington, „snědší a temnější než předtím". Znovu strávil zbytek zimy v Lynchburgu a zmizel na jaře, avšak předtím svěřil Morrisso-vi zamčenou železnou skříňku, v níž podle něj byly „hodnotné a důležité listiny". Morriss zamkl skříňku do sejfu a pustil ji z hlavy, dokud však nedostal od Beala dopis datovaný 9. května 1822 a odeslaný ze St. Louis. Po několika zdvořilostech a odstavci o záměru vydat se „lovit bizony a potkat divokého grizzlyho"

odhalil Beale význam skříňky:„Obsahuje dokumenty, na nichž závisí bohatství jak moje, tak mnoha dalších, kteří jsou mými společníky. Kdybych zemřel, ztráta těchto dokumentů by byla nenahraditelná. Střežte je proto důkladně a s péčí, aby se takovému neštěstí předešlo. Kdyby se nikdo z nás nevrátil, opatrujte prosím skříňku po dobu deseti let ode dne, jímž je datován tento dopis. Když do té doby nepřijdu ani já, ani nikdo mnou pověřený, odstraňte zámek a otevřete skříňku. Kromě dokumentů adresovaných přímo vám tam najdete i jiné, nečitelné bez klíče. Odpovídající klíč jsem zanechal v rukou přítele na tomto místě, zapečetěný a adresovaný vám, s pokynem neodesílat jej do června 1832. S pomocí klíče snadno pochopíte, co je třeba udělat."

Morriss pečlivě opatroval skříňku, čekal na jejího majitele, ale snědý muž se do Lynchburgu nikdy nevrátil. O deset let později se měl Morriss řídit instrukcemi a otevřít skříňku, ale patrné se zdráhal rozbít zámek. Beale uvedl ve svém dopisu, že v červnu 1832 dostane Morriss zprávu s dešifrovacím klíčem. Ta však nikdy nepřišla, a Morriss se tedy patrně domníval, že nemá cenu skříňku otvírat, když její obsah stejně nepůjde přečíst. Roku 1845 však Morrisse přemohla zvědavost a zámek rozbil. Skříňka obsahovala tři listy šifrovaných znaků a dopis, jenž Beale napsal běžnou angličtinou.

Dopis odhalil pravdu o Bealovi, o skříňce a šifrách. Vysvětloval, že v dubnu 1817, tedy téměř tři roky před svým prvním setkáním s Morrissem, cestoval Beale spolu s 29 dalšími osobami napříč Amerikou. Projeli bohaté lovecké oblasti Západu a dorazili do Santa Fé. V tomto „mexickém městečku" přezimovali. V březnu vyrazili na sever a sledovali „velké stádo buvolů" ve snaze jich co nejvíce postřílet. Pak na ně narazilo štěstí:

Jednoho dne při pronásledování buvolů se skupina utábořila v malé rokli asi 250 nebo 300 mil na sever od Santa Fé. Uvázali koně a připravovali večeři, když tu jeden z mužů spatřil ve skalní rozsedlině něco, co vypadalo jako zlato. Když si nález prohlédli ostatní společníci, shledali, že jde vskutku o zlato, což přirozeně vyvolalo velké vzrušení."

Dopis dále vysvětloval, jak Beale a ostatní muži s pomocí místního kmene po osmnáct měsíců kopali, přičemž nashromáždili velké množství zlata a rovněž stříbro, jež našli opodál. Pak se dohodli, že je třeba jejich nově nabyté bohatství přestěhovat na bezpečnější místo, a proto se rozhodli převézt jej domů do Virginie, kde by

poklad ukryli. Roku 1820 odjel Beale do Lynchburgu se zlatem a stříbrem, nalezl vhodné místo a poklad zakopal. Učinil tak při příležitosti, kdy poprvé bydlel v hotelu Washington a seznámil se s Morrissem. Když Beale na konci zimy odjel, vrátil se ke svým mužům, kteří v jeho nepřítomnosti dále dolovali.

Po osmnácti měsících se Beale vrátil do Lynchburgu, aby zvětšil ukryté zásoby. Tentokrát k tomu měl ještě jeden důvod:

„Než jsem opustil své společníky na pláních, hovořili jsme o tom, že kdyby se nám přihodilo neštěstí, ukrytý poklad by zůstal nedostupný našim rodinám, a že je třeba se pro takový případ nějak pojistit. Proto jsem byl pověřen, abych vybral zcela důvěryhodnou osobu, najdu-li takovou, která by - pokud by to pro všechny

společníky bylo přijatelné -byla pověřena úlohou vykonavatele našich posledních vůlí v poměru našich podílů."

Beale usoudil, že Morriss je čestný muž, a proto mu svěřil skříňku se třemi šifrovanými listy, tzv. Bealovými šiframi. Každý list obsahoval řadu čísel (jsou zde přetištěny jako obrázky 21, 22 a 23), všechny potřebné detaily však mělo odhalit až dešifrování. První list popisoval umístění pokladu, druhý byl soupisem jeho složení a třetí seznamem příbuzných, kteří měli obdržet podíl. Když si Morriss tohle všechno přečetl, uplynulo již 23 let od chvíle, kdy viděl Thomase Bea-la naposled. *Vycházel z* předpokladu, že Beale a jeho muži jsou všichni mrtvi, a proto se Morriss cítil povinen najít zlato a rozdělit je mezi jejich příbuzné. Bez slíbeného klíče však byl nucen luštit šifru od nuly. Tento úkol jej trápil po dvacet let a skončil nezdarem.

Roku 1862, ve věku osmdesáti čtyř let, cítil Morriss, že se jeho dny již nachylují a že by měl tajemství Bealových šifer někomu předat, aby spolu s ním nezemřela i naděje na splnění Bealova přání. Morriss se svěřil příteli, jehož identita bohužel zůstává zahalena tajemstvím. Víme jen tolik, že to byl právě tento přítel, kdo roku 1885 napsal zmíněnou brožuru, takže nadále o něm budu hovořit jako o *Autorovi.* Autor vysvětlil v brožuře důvod své anonymity:

„Předpokládám, že tyto dokumenty dosáhnou velkého nákladu, a chtěje zabránit záplavě dopisů, jež by na mne pršely ze všech částí Unie s otázkami všeho druhu a žádostmi o odpověď, dopisů, jež by zabraly můj veškerý čas a změnily mou pracovní náplň, kdybych se jim chtěl rádně věnovat, rozhodl jsem se neuvést své jméno v této publikaci. Roz-hodnutí jsem učinil poté, co jsem všechny, jež to může zajímat, ujistil, že jsem do ní vložil vše, co o věci vím, a že nemohu dodat ani jedno slovo k prohlášením zde obsaženým."

71, 194, 38. 1701. 89. 76. 11. 83. 1629, 48. 94, 63. 132, 16, 111. 95. 84. 341. 975, 14, 40, 64, 27. 81, 139, 213, 63, 90, 1120, 8. 15, 3. 126. 2018. 40. 74, 758. 485, 604. 230. 436, 664, 582, 150, 251. 284. 308. 231, 124. 211. 486. 225, 401. 370. 11. 101. 305. 139, 189, 17. 33. 88, 208, 193. 145. 1. 94.

73. 416. 918. 263, 28. 500, 538. 356, 117. 136. 219, 27. 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200. 283. 118, 320, 138, 36, 416. 280. 15. 71. 224, 961. 44, 16. 401, 39, 88. 61, 304. 12. 21. 24. 283. 134. 92. 63. 246. 486. 682. 7, 219. 184, 360, 780, 18, 64, 463. 474. 131. 160. 79, 73, 440. 95. 18. 64. 581. 34. 69. 128. 367, 460. 17, 81, 12, 103. 820. 62, 116. 97. 103. 862, 70, 60. 1317. 471. 540. 208. 121. 890. 346. 36. 150. 59. 568, 614. 13. 120. 63, 219. 812. 2160. 1780. 99. 35. 18. 21. 136. 872, 15. 28. 170, 88, 4. 30. 44. 112, 18. 147. 436. 195, 320. 37, 122, 113, 6, 140, 8, 120. 305. 42, 58, 461, 44, 106. 301, 13, 408, 680, 93, 86. 116, 530, 82. 568, 9. 102, 38. 416. 89, 71, 216, 728, 965, 818. 2. 38. 121, 195, 14, 326, 148. 234, 18, 55, 131. 234. 361. 824. 5, 81, 623, 48, 961, 19. 26. 33, 10, 1101. 365, 92, 88, 181, 275, 346, 201. 206. 86. 36, 219, 324, 829, 840. 64. 326. 19. 48, 122, 85, 216, 284, 919, 861. 326, 985, 233. 64, 68, 232, 431, 960, 50. 29. 81. 216. 321. 603. 14. 612. 81. 360, 36. 51, 62, 194. 78, 60. 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921. 1060, 464. 895. 10. 6. 66. 119. 38. 41, 49, 602. 423, 962. 302. 294, 875. 78, 14, 23. 111. 109. 62. 31, 501. 823. 216. 280. 34. 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19. 242. 31. 86, 234. 140, 607. 115. 33, 191, 67, 104. 86. 52, 88, 16. 80. 121, 67, 95, 122. 216, 548. 96, 11. 201. 77, 364, 218, 65, 667. 890. 236. 154, 211, 10, 98, 34, 119, 56, 216, 119, 71. 218. 1164. 1496. 1817. 51. 39. 210, 36, 3, 19, 540, 232, 22, 141. 617. 84, 290, 80, 46, 207, 411, 150, 29. 38, 46, 172, 85, 194, 39, 261. 543, 897, 624, 18, 212, 416, 127, 931, 19. 4, 63, 96, 12, 101, 418,

16, 140, 230, 460, 538, 19, 27. 88. 612, 1431. 90. 716, 275,

74, 83, 11. 426. 89, 72, 84, 1300, 1706. 814. 221. 132, 40. 102, 34, 868, 975, 1101, 84, 16. 79. 23, 16. 81. 122. 324. 403, 912. 227. 936, 447, 55. 86. 34, 43, 212. 107, 96, 314, 264. 1065, 323, 428, 601, 203. 124. 95. 216, 814, 2906, 654, 820, 2, 301. 112. 176. 213. 71. 87. 96. 202. 35, 10, 2, 41,

17. 84. 221. 736. 820. 214. 11. 60. 760.

Obrázek 21: První Bealova šifra.

115, 73. 24, 807, 37, 52. 49, 17, 31, 62. 647, 22, 7, 15. 140. 47. 29, 107. 79,84. 56. 239. 10. 26. 811, 5, 196. 308. 85, 52. 160, 136, 59. 211, 36. 9. 46^ 316. 554, 122, 106, 95. 53, 58, 2. 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140, 287. 28, 353, 37, 1005, 65, 147. 807, 24. 3, 8, 12> 47, 43, 59. 807, 45, 316, 101. 41. 78. 154. 1005, 122. 138, 191, 16, 77, 49! 102, 57, 72, 34, 73, 85, 35, 371, 59, 196. 81. 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287. 63. 3. 6. 191. 122, 43, 234. 400, 106, 290, 314, 47, 48, 81, 96, 26, 115. 92, 158. 191. 110, 77. 85, 197. 46. 10. 113. 140, 353, 48. 120, 106, 2, 607, 61, 420, 811, 29. 125. 14. 20, 37, 105, 28, 248, 16. 159, 7. 35, 19. 301, 125, 110, 486, 287. 98. 117, 511, 62, 51. 220. 37. 113, 140, 807, 138. 540. 8, 44, 287, 388. 117. 18, 79, 344. 34. 20. 59, 511, 548, 107, 603, 220. 7, 66, 154, 41, 20. 50, 6. 575, 122, 154, 248, 110. 61, 52, 33, 30, 5, 38. 8. 14. 84. 57. 540. 217. 115, 71. 29, 84, 63, 43, 131, 29, 138. 47. 73, 239. 540, 52. 53. 79, 118. 51. 44. 63. 196. 12. 239, 112. 3. 49. 79, 353, 105, 56, 371, 557. 211, 515, 125, 360. 133. 143, 101. 15, 284, 540. 252. 14. 205, 140, 344, 26. 811, 138, 115, 48, 73, 34, 205, 316, 607, 63. 220. 7. 52. 150. 44, 52. 16. 40, 37, 158, 807, 37, 121, 12. 95. 10, 15, 35, 12, 131. 62. 115, 102, 807. 49. 53, 135, 138. 30. 31. 62. 67, 41, 85, 63, 10. 106. 807. 138, 8, 113. 20. 32, 33, 37, 353, 287, 140, 47, 85, 50. 37. 49. 47. 64. 6. 7, 71. 33, 4, 43, 47, 63. 1. 27. 600. 208. 230, 15. 191. 246, 85, 94, 511, 2, 270, 20. 39. 7. 33. 44. 22. 40. 7.

10, 3. 811. 106. 44. 486, 230, 353, 211. 200. 31. 10. 38. 140. 297, 61, 603, 320, 302, 666. 287. 2. 44, 33, 32, 511, 548, 10, 6, 250, 557, 246, 53, 37, 52. 83, 47, 320. 38. 33. 807, 7. 44. 30. 31. 250, 10, 15, 35, 106. 160. 113, 31. 102. 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301. 316. 353. 320. 220. 37. 52. 28. 540, 320, 33, 8, 48, 107, 50, 811, 7. 2, 113. 73. 16. 125.

11, 110, 67, 102, 807, 33, 59. 81, 158, 38, 43, 581. 138. 19. 85. 400. 38.

43, 77, 14, 27. 8. 47. 138. 63. 140. 44. 35. 22, 177. 106. 250. 314, 217, 2. 10, 7, 1005, 4. 20, 25, 44, 48. 7, 26. 46. 110. 230. 807, 191. 34, 112. 147,

44, 110, 121, 125. 96. 41. 51. 50. 140, 56, 47, 152, 540, 63, 807, 28, 42. 250. 138. 582. 98. 643. 32, 107, 140. 112. 26. 85. 138, 540, 53. 20, 125. 371. 38. 36. 10, 52, 118, 136. 102. 420, 150. 112. 71, 14. 20, 7. 24, 18,

12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102. 811. 30. 83. 84. 305, 620, 15, 2, 108. 220. 106, 353, 105, 106, 60, 275, 72, 8, 50, 205. 185. 112, 125, 540. 65, 106, 807, 188, 96, 110, 16, 73, 33. 807. 150. 409, 400, 50, 154. 285. 96. 106, 316, 270, 205. 101. 811. 400. 8, 44, 37, 52, 40, 241. 34. 205. 38. 16. 46. 47. 85. 24. 44. 15. 64. 73. 138, 807. 85. 78, 110, 33. 420. 505, 53, 37, 38, 22, 31, 10, 110, 106, 101, 140, 15. 38, 3, 5. 44, 7. 98. 287, 135, 150, 96, 33, 84, 125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220. 275, 30, 150, 105, 49, 53, 287. 250. 208, 134, 7, 53. 12, 47. 85. 63. 138. 110, 21, 112, 140, 485, 486, 505. 14. 73. 84. 575, 1005, 150. 200, 16, 42, 5. 4, 25. 42. 8. 16, 811, 125, 160, 32, 205, 603. 807. 81. 96. 405, 41, 600, 136, 14, 20, 28. 26, 353, 302, 246, 8. 131, 160, 140, 84, 440, 42, 16, 811, 40. 67, 101, 102. 194. 138. 205. 51. 63. 241. 540, 122, 8, 10, 63. 140, 47, 48, 140, 288.

Obrázek 22: Druhá Bealova šifra.317. 8. 92, 73, 112, 89, 67, 318. 28, 96, 107, 41, 631, 78, 146. 397, 118, 98. 114, 246, 348, 116, 74, 88, 12, 65, 32, 14, 81, 19. 76. 121. 216. 85, 33, 66, 15, 108. 68. 77, 43, 24, 122, 96, 117. 36. 211, 301. 15. 44. 11, 46, 89, 18, 136, 68, 317, 28, 90, 82, 304. 71, 43, 221, 198, 176, 310, 319, 81. 99, 264, 380, 56, 37,

319, 2, 44, 53, 28, 44. 75, 98. 102. 37. 85. 107. 117. 64, 88. 136, 48. 154. 99. 175. 89, 315, 326, 78. 96. 214. 218. 311. 43. 89. 51, 90. 75. 128. 96. 33. 28. 103. 84. 65. 26, 41. 246. 84. 270, 98, 116, 32, 59, 74, 66, 69, 240, 15. 8, 121. 20. 77, 89, 31, 11. 106. 81, 191, 224, 328. 18, 75, 52, 82. 117, 201. 39, 23,

217. 27. 21, 84. 35. 54, 109. 128, 49, 77, 88. 1, 81. 217, 64,

55, 83. 116. 251, 269. 311, 96, 54, 32. 120. 18. 132. 102, 219, 211, 84, 150. 219, 275. 312. 64. 10. 106. 87. 75. 47. 21. 29. 37. 81. 44. 18. 126, 115, 132,

160, 181, 203, 76, 81, 299, 314, 337, 351, 96. 11. 28. 97, 318, 238, 106, 24. 93. 3. 19. 17. 26, 60, 73. 88. 14. 126. 138. 234. 286. 297. 321. 365. 264, 19. 22. 84.

56. 107, 98, 123, 111, 214, 136, 7, 33, 45, 40, 13, 28. 46, 42. 107. 196, 227, 344, 198. 203. 247. 116, 19, 8, 212, 230. 31. 6, 328. 65. 48, 52, 59, 41, 122. 33, 117, 11, 18, 25, 71. 36. 45. 83. 76. 89. 92. 31. 65. 70. 83, 96, 27, 33, 44, 50, 61. 24. 112. 136, 149, 176. 180. 194. 143. 171, 205. 296. 87. 12, 44. 51, 89, 98, 34, 41. 208. 173, 66, 9, 35, 16, 95, 8. 113, 175. 90. 56. 203, 19, 177, 183, 206, 157, 200, 218. 260, 291, 305. 618, 951,

320, 18, 124, 78, 65, 19, 32, 124, 48, 53, 57, 84, 96, 207. 244, 66, 82, 119. 71. 11. 86. 77. 213. 54, 82. 316. 245, 303, 86, 97. 106, 212, 18, 37, 15, 81. 89, 16, 7, 81, 39, 96, 14, 43, 216, 118, 29, 55, 109, 136. 172. 213, 64, 8, 227, 304. 611. 221, 364, 819. 375. 128. 296. 1. 18, 53, 76, 10, 15, 23, 19, 71. 84. 120, 134, 66, 73, 89. 96. 230, 48, 77, 26, 101, 127, 936, 218, 439, 178. 171. 61, 226, 313, 215. 102. 18. 167. 262. 114. 218. 66. 59, 48. 27, 19, 13. 82. 48, 162, 119, 34. 127, 139, 34. 128. 129. 74. 63. 120, 11, 54, 61, 73, 92, 180, 66, 75, 101, 124, 265. 89. 96. 126. 274. 896. 917. 434. 461. 235, 890, 312, 413, 328, 381, 96, 105, 217, 66, 118, 22, 77, 64, 42, 12, 7. 55, 24, 83, 67, 97, 109, 121, 135. 181. 203. 219, 228, 256, 21, 34, 77. 319, 374, 382, 675, 684, 717, 864. 203, 4. 18. 92, 16, 63, 82, 22, 46. 55, 69, 74, 112, 134, 186. 175. 119, 213, 416, 312, 343, 264, 119, 186, 218, 343, 417. 845. 951, 124, 209, 49, 617. 856, 924. 936. 72, 19, 28. 11. 35, 42, 40, 66, 85, 94, 112, 65. 82. 115, 119, 236, 244, 186, 172, 112, 85, 6, 56, 38, 44, 85, 72, 32. 47, 73, 96, 124, 217, 314, 319, 221. 644, 817, 821, 934, 922, 416, 975. 10, 22, 18, 46. 137, 181. 101, 39, 86, 103, 116, 138, 164. 212.

218. 296. 815, 380. 412, 460, 495, 675, 820. 952.

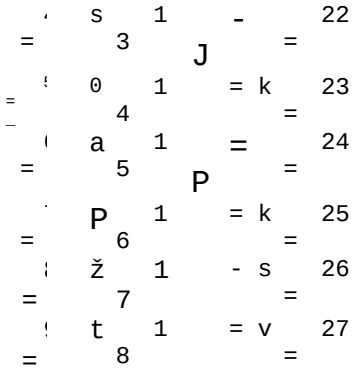
Obrázek 23: Třetí Bealova šifra.

Aby ochránil svou identitu, požádal Autor místního váženého občana a okresního zeměměřiče Jamese B. Warda, aby působil jako jeho agent a vydavatel.

Vše, co víme o podivném příběhu Bealových šifer, je uvedeno v brožuře, takže díky Autorovi máme k dispozici šifry a Morrissovo vyprávění. Autor rovněž dokázal úspěšně rozluštit druhou Bealovu šifru. Stejně jako první a třetí i druhá šifra je tvořena celou stránkou čísel. Autor předpokládal, že každé z čísel odpovídá jednomu písmenu. Rozsah čísel však daleko přesahuje počet písmen v abecedě, takže Autor usoudil, že má co do činění s šifrou, která reprezentuje jedno písmeno více různými čísly. Jednou z šifer, jež splňuje tento předpoklad, je takzvaná knižní šifra, pro niž slouží jako klíč kniha nebo jiný text.

Kryptograf při použití takové šifry nejprve očísluje všechna slova v klíčovém textu. Každé číslo pak slouží jako náhrada za počáteční písmeno příslušného slova. 'Například [2]dohodnou-[3]li [4]se Odesilatel [6]a [7]příjemce, [8]že [9]tato "Věta "bude [12]sloužit [13]jako [14]klíč, [15]pak [16]každé [17]slovo [18]v [19]ní "číselně "označíme [Z2]a "čísla [24]se "stanou "základem "šifrování. V dalším kroku sestavíme seznam, který ukáže, jak jsou čísla přiřazena písmenům:

```
   :   n   1    = v   19
 =       0           =
   :   d   1    = b   20
 =       1           =
   :   1   1    = s   21
 =       2           =
```



Zprávu lze nyní zašifrovat tak, že písmena v otevřeném textu nahradíme čísly podle seznamu. V případě tohoto seznamu bude písmeno d nahrazeno číslem 2, zatímco písmeno S můžeme nahradit jako 4, 12, 17, 24 nebo 25. Protože jsme jako klíč použili krátkou větu, nemáme k dispozici všechna písmena. Už s tím, co máme, však můžeme zašifrovat například slovo poklad, a to například jako 7-21-16-3-6-2. Má-li příjemce svou kopii klíčového textuje dešifrování triviální. Pokud však je k dispozici jen šifra, pak kryptoanalýza spočívá v nalezení klíčového textu. Autor k tomu píše: „S touto myš-lenkou v hlavě jsem zkoušel všechny knihy, jež jsem si jen mohl pořídit, čísloval jsem jejich slova a porovnával čísla s rukopisy. Bezvýsledně, dokud se nepodařilo jednu z šifer vyluštit pomocí *Deklarace nezávislosti,* což znovu oživilo mé naděje."

Ukázalo se, že *Deklarace nezávislosti je* klíčovým textem druhé Bealovy šifry a že očíslováním jejích slov lze tuto šifru přečíst. Obrázek 24 obsahuje počátek *Deklarace nezávislosti* (v angličtině), v níž je očíslováno každé desáté slovo, aby čtenář lépe viděl, jak funguje dešifrování. Na obrázku 22 je šifrový text - prvním číslem je 115, v dokumentu zní 115. slovo „instituted", takže první písmeno otevřeného textu je i. Druhé číslo je 73, na této pozici je v Deklaraci slovo „hold", takže druhým písmenem je h. Zde uvádíme (v českém překladu - pozn. překl.) celý dešifrovaný text, jak je otištěn v Autorově brožuře:

V bedfordském okrese, asi čtyři míle od Buforďs, ve výkopu šest stop pod zemí jsem uložil tyto položky, náležející společně osobám, jejichž jména jsou sepsána v čísle *„3":*

„První deponát obsahuje tisíc čtrnáct liber zlata a tři tisíce osm set dvacet liber stříbra. Uložil jsem je v listopadu 1819. Druhý deponát byl ukryt v prosinci 1821 a obsahuje devatenáct set sedm liber zlata, jakož i dvanáct set sedm liber stříbra; také šperky, zakoupené v St. Louis za stříbro, aby se zjednodušila doprava, v hodnotě třináct tisíc dolarů.

To vše je bezpečně zabaleno v železných nádobách s železnými víky. Výkop je zhruba vyložen kameny, nádoby stojí na kamenech a jinými jsou překryty.

Dokument „1" popisuje přesné umístění výkopu, takže nebude těžké jej najít."

Stojí za zmínku, že v šifrovém textu jsou chyby. Dešifrování obsahuje například slova „four miles" (čtyři míle), jejichž význam závisí na tom, že 95. slovo Deklarace nezávislosti začíná písmenem u. Toto slovo však správně zní „malienable" (nezadatelný). Chyba může být důsledkem nepřesného šifrování, je však rovněž možné, že Beale měl výtisk Deklarace, v němž 95. slovo znělo „wwalienable", což se vyskytovalo v některých vydáních z počátku 19. století. V každém případě z úspěšného vyluštění druhé šifry jasně plynula hodnota pokladu - přinejmenším dvacet milionů dolarů v dnešních cenách.

Asi nás nepřekvapí, že když už jednou Autor znal hodnotu pokladu, věnoval o to více času *analýze* dalších dvou šifer, a to především první z nich, jež popisuje umístění pokladu. Navzdory velkému úsilí to nedokázal a šifry mu přinesly jen zármutek:

„Vzhledem k množství času, který jsem výše popsaným výzkumům věnoval, jsem byl uvržen z relativního dostatku do úplné chudoby a strádání postihlo i ty, o něž jsem měl pečovat, a to i navzdory jejich námitkám. Nakonec se mi otevřely oči a rozhodl jsem se přerušit rázně a navždy všechny své vztahy k této záležitosti a napravit své chyby, je-li to možné. Abych toho všeho dosáhl a abych odstranil předmět pokušení ze svého dosahu, rozhodl jsem se celou záležitost zveřejnit a sejmout tak ze svých beder odpovědnost, již cítím vůči panu Morrissovi."

Tak se stalo, že šifry byly roku 1885 publikovány spolu se vším ostatním, co Autor věděl. Ačkoli požár skladu zničil většinu nákladu, i to, co zbylo, dokázalo způsobit v Lynchburgu rozruch. K nejhorlivějším hledačům pokladů, které přitáhly Bealovy šifry, patřili bratři George a Clayton Hartové. Po léta se zabývali dvěma zbylými šiframi a zkoušeli nejrůznější formy kryptoanalytického útoku, přičemž občas propadli iluzi, že již mají řešení. Nesprávně vedený postup někdy náhodou vytvoří několik elektrizujících slov uprostřed moře nesmyslů, což kryptoanalytika povzbudí, aby v započatém úsilí pokračoval a zbylé nesmysly nějak odstranil. Nezaujatému pozorovateli bývá jasné, že přání je tu otcem myšlenky, ale zaslepený lovec pokladů to vidí jinak. Jeden z pokusů o rozluštění, jenž Hartové podnikli, vedl k tomu, že vyhodili dynamitem do povětří zeminu na místě, jež pokládali za správné. V kráteru, který tak vznikl, se bohužel žádné zlato neobjevilo. Clayton Hart vzdal své úsilí roku 1912, George však pokračoval až do roku 1952. Ještě nezlomnějším bealeovským fanatikem byl Hiram Herbert jr., který se s problémem seznámil roku 1923 a pokračoval až do 70. let. Ani on nedošel k žádnému výsledku.

Na stezku vedoucí k Bealovu zlatu se vydali i profesionální kryptoanalytici. Bealova šifra přitahovala například Herberta O. Yard-leye, zakladatele Amerického úřadu pro šifry (U.S. Cipher Bureau -„americká

černá komnata"), stejně jako plukovníka Williams Fried-tnana, který byl vedoucí osobností americké kryptoanalýzy po první polovinu 20. století. Když řídil Signál Intelligence Service, zařadil Bealovy šifry do výcvikového programu patrně proto, že - jak se jednou zmínila jeho žena - byl přesvědčen, že jde o šifry „ďábelsky vynalézavé, navržené speciálně proto, aby svedly nezkušené". DoWhen, in the course ofhuman events, ic becomes [10]necessary for one people to dissolve the political bands which [20]have connected them with another, and to assume among the "powers of the earth, the separate and equal station to [40]which the laws of nature and of nature's God entitle [so]them, a decent respect to the opinions of mankind requires [60]that they should declare the causes which impel them to [70]the separation.

We hold these truths to be self-evident, [so]that all men are created equal, that they are endowed [90]by their Creator with certain inalienable rights, that among these [100]are life, liberty and the pursuit of happiness; That to ""secure these rights, governments are instituted among men, deriving their [120]just powers from the consent of the governed; That whenever [130]any form of government becomes destructive of these ends, it [140]is the right of the people to alter or to [150]abolish it, and to institute a new government, laying its [160]foundation on such principles and organizing its powers in such [170]form, as to them shall seem most likely to effect [180]their safety and happiness. Prudence, indeed, will dictate that governments [190]long established should not be changed for light and transient [200]causes; and accordingly all experience hath shewn, that mankind are [210]more disposed to suffer, while evils are sufferable, than to [220]right themselves by abolishing the forms to which they are [230]accustomed.

But when a long train of abuses and usurpations, [240]pursuing invariably the samé object evinces a design to reduce them [250]under absolute despotism, it is their right, it is their [260]duty, to throw off such government, and to provide new [270]Guards for their future security. Such has been the patient [2s0]sufferance of these Colonies; and such is now the necessity [29°]which constrains them to alter their former systems of government. [300]The history of the present King of Great Britain is [310]a history of repeated injuries and usurpations, all having in [320]direct object the establishment of an absolute tyranny over these [330]States. To prove this, let facts be submitted to a [340]candid world.

Obrázek 24: První tři odstavce anglického textu *Deklarace nezávislosti,* v němž je očíslováno každé desáté slovo. Jde o klíč k dešifrování druhé Bealovy šifry.

Friedmanova archivu, založeného po jeho smrti ve Výzkumném centru George C. Marshalla, často nahlížejí vojenští historici, ale velkou většinu návštěvníků tvoří nadšenci Bealových šifer, kteří doufají, že zde najdou nějakou nápovědu. Později byl jednou z vedoucích postav na cestě k Bealovu pokladu Carl Hammer, bývalý ředitel pro počítačovou vědu ve firmě Sperry UNIVAC a jeden z průkopníků počítačové kryptoanalýzy. Hammer uvádí: „Bealovy šifry zabírají nejméně deset procent kapacity nejlepších kryptoanalytických mozků země. Ani kousek toho úsilí však nebyl zbytečný. Celá ta práce -i ty její části, jež vedly do slepých uliček - se bohatě vyplatila, proto"

f e vedla k pokrokům v počítačovém výzkumu." Hammer byl prominentním členem Společnosti Bealových šifer a pokladu, založené v 60. letech 20. století s cílem dál povzbuzovat zájem o Bealovo tajemství. Společnost zpočátku vyžadovala, aby se kterýkoli její člen, jemuž se podaří objevit poklad, o něj podělil s ostatními členy, tento závazek však mnohé prospektory od vstupu odradil, takže podmínka byla nakonec zrušena.

Navzdory společnému úsilí Společnosti, amatérských lovců pokladů a profesionálních kryptoanalytiků zůstává první a třetí Bea-lova šifra už více než sto let tajemstvím. Zlato, stříbro a šperky na svého objevitele dosud čekají. Mnohé pokusy o dešifrování se točily kolem *Deklarace nezávislosti* - klíče k druhé

Bealově šifře. Prosté očíslování slov Deklarace k ničemu nevedlo, a proto kryptoanalytici zkoušeli různá jiná schémata jako číslování odzadu nebo číslování každého druhého slova, ale zatím nic nevyšlo. Problém je i v tom, že první šifra obsahuje vysoká čísla, až 2 906, zatímco *Deklarace nezávislosti* má jen 1 322 slov. V roli klíče se zkoušely i jiné knihy a texty, a mnoho kryptoanalytiků dokonce zvažovalo možnost, že jde o zcela odlišný šifrovací systém.

Možná vás překvapí, jak se Bealova šifra ukázala být silná, zejména když si připomeneme, že v bitvě mezi kryptografy a kryptoanaly-tiky to byli ti druzí, kdo měli navrch. Babbage a Kasiski našli způsob, jak rozluštit Vigeněrovu šifru, a kryptografové za ni marně hledali adekvátní náhradu. Jak mohl Beale přijít s něčím tak účinným? Odpověď zní, že Bealovy šifry vznikaly za okolností, jež jsou pro kryptografa velmi příznivé. Zprávy byly určeny pro jedno použití a vzhledem k tomu, že se vztahovaly k tak cennému pokladu, zřejmě se Bealovi vyplatilo připravit pro první a třetí šifru speciální jednorázový klíčový text. Pokud byl autorem klíčového textu sám Beale, je jasné, proč se jej nepodařilo najít pročesáváním publikovaného materiálu. Lze si představit, že Beale napsal pojednání o lovu bizonů dlouhé 2 000 slov, jež existovalo v jediné kopii. Nikdo jiný než majitel textu - unikátního klíče - by pak nemohl první a třetí šifru rozluštit. Beale se zmínil, že klíč zanechal „v rukou přítele" [v] St. Louis, pokud však tento přítel klíč zničil nebo ztratil, pak se nemusí podařit Bealovy šifry rozluštit nikdy.

Vytvoření jednorázového textu je pro zprávu mnohem bezpečnější technika než použít klíč vycházející z publikovaného textu, postup je však prakticky použitelný jen tehdy, má-li odesilatel dostčasu takový text připravit a může-li jej bezpečně doručit adresátovi. V rutinní každodenní komunikaci tyto požadavky nebývají splněny. Beale však mohl svůj text v klidu připravit, doručit jej příteli do St. Louis a dohodnout s ním doručení určenému adresátovi někdy v budoucnu.

Jiná teorie vysvětlující nerozluštitelnost Bealových šifer spočívá v tom, že Autor brožury záměrně šifry pozměnil, než je publikoval. Možná bylo autorovým cílem získat klíč, jenž spočíval v rukou Bea-lova přítele v St. Louis. Kdyby zveřejnil přesná znění šifer, mohl by je dotyčný přítel rozluštit a vybrat zlato. Autor by pak nezískal za své úsilí žádnou odměnu. Pokud by však šifry byly poškozeny, pak by přítel zjistil, že se neobejde bez Autorovy pomoci, kontaktoval by vydavatele a ten zas Autora. Autor by pak mohl vyměnit přesná znění šifer za podíl na pokladu.

Je také možné, že poklad byl již před lety nalezen a že jej objevitel dokázal odnést nepovšimnut. Nadšenci Bealových šifer se sklonem ke konspiračním teoriím naznačili, že poklad již našla National Security Agency (NSA). Tato nejdůležitější americká instituce na poli šifer disponuje nejvýkonnějšími počítači a některými z nejlepších mozků světa, takže by se mohlo stát, že objeví něco, co všem ostatním uniklo. To, že agentura nic podobného neoznámila, se zdá korespondovat s její vášní pro extrémní utajení; říká se, že zkratka NSA ve skutečnosti znamená „Never Say Anything" (nikdy nic neříkej) nebo „No Such Agency" (taková agentura neexistuje).

Konečně nemůžeme vyloučit ani možnost, že Bealovy šifry jsou důmyslným

podvodem a že Beale nikdy neexistoval. Skeptici se domnívají, že se neznámý Autor nechal inspirovat Poeovým *Zlatým skarabem*, vymyslel si celý příběh a publikoval brožuru ve snaze vydělat na lačnosti ostatních. Ti, kdo tento názor zastávají, hledají v Bealově příběhu nekonzistence a chyby. Tak například Bealův dopis - jenž měl být napsán roku 1822 a od té doby ležet zamčený v kovové skříňce - obsahuje slovo „stampede" (splašený útěk), jež se v tisku objevilo až roku 1834. Je však možné, že na Západě se používalo mnohem dříve a že se mu Beale naučil na svých cestách.

Jedním z předních nevěřících je kryptograf Louis Kruh, který tvrdí, že našel důkazy o tom, že autor brožury je rovněž autorem Bealových dopisů - jak toho, jenž měl být odeslán ze St. Louis, tak toho, který ležel ve skříňce. Provedl textovou analýzu stylu obou autorů. Porovnával přitom takové aspekty jako počet vět *začínajících* slovy „The", „Of' či „And", průměrný počet čárek a středníků a další složky stylu - používání záporných tvarů, záporného pasiva sloves, infinitivů, podmínkových vedlejších vět a podobně. Kromě porovnání stylu Autora a Beala byly do analýzy zahrnuty také texty z 19. století napsané třemi jinými obyvateli Virginie. Z těchto pěti sad vykázaly největší vzájemnou podobnost texty Beala a Autora. To by naznačovalo, že sám Autor napsal dopisy, jejichž autorem má být *Beale,* a celý příběh si vymyslel.

Na druhou stranu existují i důkazy integrity Bealových šifer. Za prvé, kdyby šifry vznikly jako podvod, pak lze předpokládat, že by jeho autor vybral čísla náhodně a nepozorně. Čísla z Bealových šifer však vykazují různé spletité zákonitosti. Jednu z nich lze nalézt, když použijeme *Deklaraci nezávislostí* jako klíč první šifry. Nedostaneme žádná rozpoznatelná slova, zato vznikají sekvence jako abfdefghiijklmmnohpp. Přestože nejde o dokonale utříděnou abecedu, sotva se to dá vysvětlit jako náhoda. James Gillogly z Americké asociace pro kryptogramy není přesvědčen, že jsou Bealivy šifry autentické, přesto uvádí, že pravděpodobnost náhodného výskytu takové sekvence je menší než jedna ke stovce miliard, takže se zdá být jisté, že první šifra je postavena na nějakém kryptografickém principu. Jedna z teorií říká, že *Deklarace nezávislosti* je skutečně klíčem, ale že výsledný text vyžaduje další stupeň rozšifrování. To by jinými slovy znamenalo, že první Bealova šifra byla zašifrována dvoustupňové, pomocí tzv. *superšifrování.* Je-li tomu tak, pak je i možné, že abecední sekvence má sloužit jako povzbuzení, jako známka, že první stupeň byl dešifrován úspěšně.

Další důkazy pravosti šifer pocházejí z historického výzkumu, jenž se snažil ověřit Bealův příběh. Místní historik Peter Viemeister shrnul většinu tohoto materiálu do své knihy *The Beale Treasure -History ofa Mystery* (Bealův poklad - Historie tajemství). Viemeister začal tím, že si položil otázku, zda lze prokázat, že Thomas Beale opravdu existoval. Pomocí sčítání lidu z roku 1790 a dalších dokumentů našel několik mužů toho jména, kteří se narodili ve Virginii a jejichž osudy nebyly v rozporu s těmi několika málo známými životopisnými daty. Viemeister se rovněž pokoušel ověřit další detaily uvedené v brožuře, jako Bealovu cestu do Santa Fé a objev zlata. Existuje například čejenská legenda, datovaná zhruba do roku 1820, o zlatě a stříbře, jež byly odvezeny ze Západu a zakopány v horách na

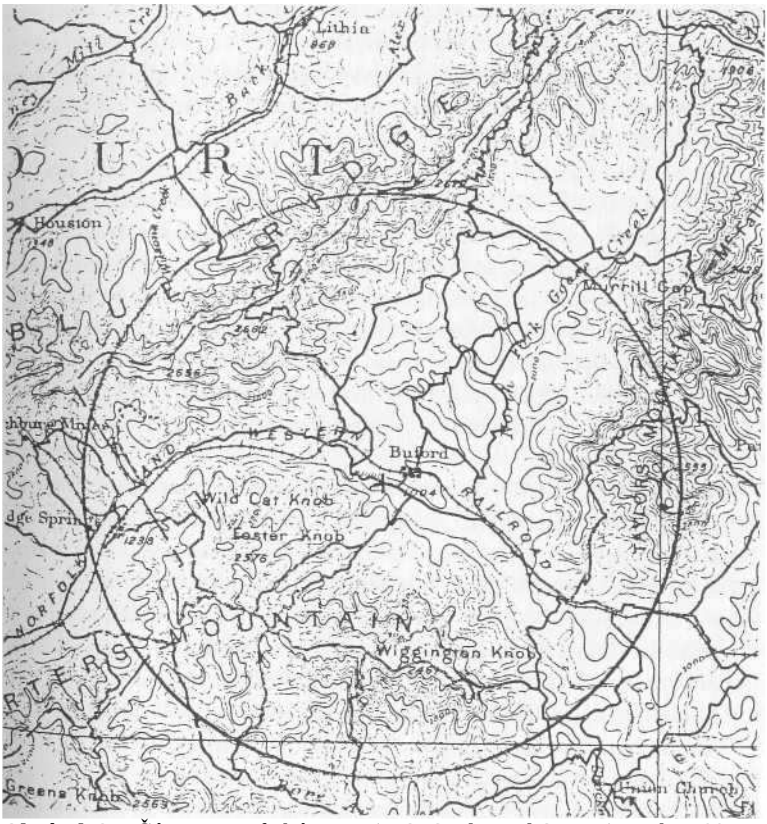
Východě. Poštovní seznam města St. Louis z roku 1820 uvádíosobu jménem „Thomas Beall", což odpovídá tvrzení z brožury, že roku 1820 pobýval Beale ve městě na své cestě na Západ poté, co odjel z Lynchburgu. Brožura rovněž uvádí, že Beale odeslal ze St. Louis dopis roku 1822.

Základ Bealova příběhu tedy nesporně existuje a nadále přitahuje jak kryptoanalytiky, tak hledače pokladů. K těm druhým patřili například Joseph Jancik, Marilyn Parsonsová a jejich pes Vdolek. Roku 1983 byli obviněni z „narušení hrobky", když je chytli, jak kopají o půlnoci na hřbitově v Mountain View. Nenarazili na nic jiného než na rakev, strávili však zbytek víkendu v okresním vězení a dostali 500 dolarů pokuty. Tito amatérští vykrádači hrobů se mohou uklidňovat vědomím, že nebyli o nic méně úspěšní než Mel Fis-her, profesionální lovec pokladů, který vylovil zlato za 40 milionů dolarů z potopené španělské galeony *Nuestra Seňora de Atocha,* kterou objevil u Key West na Floridě roku 1985. Fisher dostal tip od jednoho z expertů na Bealovy šifry žijícího na Floridě, že by poklad mohl být zakopán v Grahamově mlýně v bedfordském okrese. Fisher za podpory zámožných investorů koupil pozemek pod falešným jménem, aby nevzbudil podezření. Ani po dlouhém kopání se nic nenašlo.

Někteří hledači pokladů se již naděje na rozluštění dvou zbývajících šifer vzdali a namísto toho se soustředili na hledání nápovědy v té šifře, která byla rozluštěna. V ní je například napsáno, že poklad se *nachází* „asi čtyři míle od Buforďs", čímž se patrně míní obec Buford nebo, ještě přesněji, Bufordova hospoda (Buforďs Tavern -na obrázku 25 umístěna v jeho středu). V textu je zmínka o tom, že výkop je vyložen kameny, takže mnozí hledači pátrají kolem Husího potoka, jenž je vydatným zdrojem velkých kamenů. Každé léto celá oblast ožívá hledači, z nichž někteří jsou vyzbrojeni detektorem kovů, jiní spoléhají na věštce a duchovní síly. Blízké město Bedford oplývá podniky, jež ochotně půjčují potřebné vybavení včetně průmyslových vrtných souprav. Méně nadšeni jsou místní farmáři, protože lovci pokladů často bez dovolení vstupují na jejich pozemky, poškozují ploty a kopou jámy.

Když jste si teď přečetli příběh Bealových šifer, možná byste to chtěli zkusit sami. Přitažlivost nerozluštěné šifry z 19. století v kombinaci s dvacetimilionovým pokladem může být nesnesitelná. Než se však vydáte na hledačskou stezku, věnujte pozornost radě Autora brožury:

„Než odevzdám tyto dokumenty do rukou veřejnosti, chci říci pár slov těm, jejichž zájem vzbudí, a udělit malou radu, získanou hořkou zkušeností. Zní takto: věnujte hledání jen tolik času, kolik můžete vyšetřit vedle svých běžných povinností. A pokud nemáte žádný volný čas, nechte celou věc být. ... Znovu opakuji: nikdy neobětujte své vlastní zájmy a zájmy své rodiny věci, jež se může ukázat jako iluze. Avšak, jak jsem již řekl, když máte svou denní práci hotovu a pohodlně sedíte u krbu, pak trocha času věnovaného této věci nikomu neuškodí a může přinést odměnu."



Obrázek 25: Část topografické mapy (U.S. Geological Survey) z roku 1891. Zakreslený kruh má poloměr čtyři míle a jeho středem je Buforďs Tavern, místo zmíněné ve druhé šifře.**3**

Mechanizace utajení

Koncem 19. století kryptografie upadala. Od chvíle, kdy Babba-ge a Kasiski prolomili bezpečnost Vigenerovy šifry, kryptografové hledali způsob, jak obnovit utajení komunikací a tím umožnit obchodní a vojenské sféře užívat výhod telegrafu bez rizika odposlechu a dešifrování. Na přelomu století vynalezl italský fyzik Guglielmo Marconi ještě výkonnější formu telekomunikace, čímž potřeba utajení dále vzrostla.

Roku 1894 začal Marconi experimentovat se zajímavou vlastností elektrických obvodů. Elektrický proud v jednom obvodu může za určitých podmínek indukovat proud v jiném obvodu, vzdáleném a izolovaném od prvního. Po zdokonalení konstrukce, zvýšení výkonu a přidání antén dokázal Marconi vysílat a přijímat informace na vzdálenost do 2,5 km. Vynalezl tak rádio. Telegraf byl zavedenou záležitostí již po půl století, neobešel se však bez elektrického vedení spojujícího odesilatele a příjemce. Marconiho systém měl velkou výhodu v tom, že byl

bezdrátový - signál putoval vzduchem, jakoby kouzlem.

Marconi emigroval roku 1896 do Británie ve snaze najít finanční *zázemí* pro svůj vynález. Tam jej také nakonec nechal patentovat. Nadále pokračoval ve svých experimentech a zvyšoval vzdálenost, na jakou se dalo komunikovat. Nejprve přenesl zprávu přes 15 km široký Bristolský záliv, poté přes 53 km široký průliv La Manche do Francie. Současně hledal pro svůj vynález obchodní využití, přičemž potenciálním investorům zdůrazňoval dvě hlavní výhody rádia: tento způsob přenosu jednak nevyžaduje stavbu nákladných telegrafních vedení a umožňuje také komunikovat mezi izolovanými lokalitami. Roku 1899 upoutal Marconi velkou pozornost veřejnosti, když vybavil dvě lodi rádiovým zařízením, takže novináři sledující nejdůležitější světovou regatu America's Cup mohli posílat své zpravodajství do New Yorku a následujícího dne si je lidé mohli přečíst v novinách.

Zájem dále vzrostl, když Marconi vyvrátil mýtus, že rádiová komunikace je omezena čarou obzoru. Kritikové tvrdili, že rádiové vlny se šíří přímočaře a nemohou sledovat zakřivení zemského povrchu, takže je lze použít jen asi do vzdálenosti sta kilometrů. Marconi dokázal, že to není pravda, když zaslal zprávu z Poldhu v anglickém hrabství Cornwall do St. John's na Newfoundlandu, tedy na vzdálenost 3 500 km. V prosinci 1901 vysílala stanice v Poldhu denně po tři hodiny stále dokola písmeno S (tečka-tečka-tečka), zatímco Marconi stál na větrných útesech Newfoundlandu a pokoušel se zachytit rádiové vlny. Den za dnem zápolil s větrem ve snaze vypustit do výše velkého draka, který zvedal anténu. Krátce po poledni dne 12. prosince zachytil Marconi tři nezřetelné tečky, první rádiovou zprávu přenesenou přes Atlantik. Jev zůstal tajemstvím až do roku 1924, kdy fyzikové objevili ionosféru - vrstvu atmosféry, jejíž spodní hranice se nachází ve výšce asi 60 km nad zemí. Ionosféra působí jako zrcadlo, rádiové vlny se od ní odrážejí. Současně se také odrážejí od zemského povrchu, takže se rádiové vlny mohou šířit pomocí odrazů od země a ionosféry na kterékoli místo zeměkoule.

Marconiho vynález upoutal vojáky, kteří na něj hleděli s nadějí i obavami zároveň. Taktické výhody rádia jsou zřejmé: umožňuje přímou komunikaci mezi libovolnými dvěma body, aniž by je bylo třeba spojovat elektrickým vodičem. Pokládání kabelu je často nepraktické, někdy i nemožné. Do vynálezu rádia neexistovala žádná možnost komunikovat s loděmi na moři, rádio však velitelům umožnilo koordinovat pohyby celých flotil. Stejně tak poskytlo generálům možnost řídit pohyby vojsk a udržovat kontakt s jednotlivými pluky, ať se nacházejí kdekoli. To vše je možné díky povaze rádiových vln, jež se šíří všemi směry a své přijímače si najdou bez ohledu na jejich polohu. Tato vlastnost rádia je však z vojenského hlediska zároveň jeho největší slabinou, protože zprávy nevyhnutelně dorazí k nepříteli stejně jako k vlastním jednotkám. Spolehlivé šifrování je proto nezbytností. Jestliže má nepřítel možnost odposlouchávat veškerou komunikaci, pak musí kryptografové zařídit, aby ji nemohl rozluštit.

Dvojsečná povaha rádia - snadná komunikace a snadný odposlech - se dostala do popředí zájmu na začátku první světové války. Všechny bojující strany měly

velký zájem rádio využít, nikdo si však nevěděl rady, jak s jistotou zaručit jeho bezpečnost. Vzestup rádia a válka se staly faktory, které zesílily úsilí o účinné šifrování.Mnozí badatelé si dělali naději, že dojde k průlomu a bude objevena nová šifra, která zajistí utajení vojenských komunikací. Mezi rokem 1914 a 1918 však k ničemu takovému nedošlo, spíš by se z těchto let dal sestavit katalog kryptografických selhání. Krypto-grafové přišli s několika novými šiframi, ty však byly jedna po druhé prolomeny.

Jednou z nejslavnějších válečných šifer byla německá *ADFGVX šifra*, která byla zavedena 5. března 1918, krátce před velkou německou ofenzivou, jež začala 21. března. Stejně jako každý jiný útok i tento chtěl těžit z momentu překvapení. Komise kryptografii vybrala šifru ADFGVX z několika kandidátů v přesvědčení, že zaručuje nejvyšší utajení. Byli dokonce přesvědčeni, že ji nelze rozluštit. Síla šifry spočívala v její spletité povaze kombinující substituci a transpozici (viz dodatek F).

Začátkem června 1918 stálo německé dělostřelectvo jen sto kilometrů od Paříže a chystalo se na závěrečný úder. Jediná naděje Dohody spočívala v tom, že se podaří rozluštit šifru ADFGVX a zjistit, kde přesně Němci chtějí prolomit jejich obranu. Naštěstí disponovali tajnou zbraní, jíž byl kryptoanalytik Georges Painvin. Tento snědý útlý Francouz nadaný pronikavou myslí rozpoznal svůj talent pro kryptografické hlavolamy díky náhodnému setkání s pracovníkem Bureau du chiffre, k němuž došlo až po vypuknutí války. Svůj neocenitelný talent zaměřil na hledání slabin německých šifer. S šifrou ADFGVX zápasil dnem i nocí a zhubl přitom o 15 kg.

Nakonec se mu ji podařilo rozluštit pozdě večer 2. června. Následovala záplava dalších rozluštěných zpráv, mezi nimi i jedna, jež obsahovala rozkaz: „Rychle navážejte munici. I ve dne, nebude-li to vidět." Podle záhlaví zprávy se dalo určit, že byla odeslána někde mezi Montdidierem a Compiègne, asi 80 km na sever od Paříže. Naléhavá potřeba munice poukazovala na to, že půjde o oblast, kde hrozí bezprostřední německý úder. Rádiový odposlech potvrdil, že je tomu tak. Spojenečtí vojáci posílili příslušnou část linie obrany a o týden později *začala* řež. Němci ztratili moment překvapení a po pěti dnech těžkých bojů byli odraženi.

Prolomení šifry ADFGVX bylo typickou epizodou pro kryptografii během první světové války. Přestože se objevilo mnoho nových šifer, šlo vesměs o variace a kombinace vycházející ze šifer 19. století, jež byly již dříve rozluštěny. Některé z nich poskytly utajení na přechodnou dobu, avšak kryptoanalytici nad nimi nakonec vždy

zvítězili. Největším problémem krypto analytiků bylo zvládnout sám objem rádiového provozu. Před vzestupem rádia byla každá odposlechnutá zpráva vzácností a kryptoanalytici si jich vážili. Během první světové války byl však objem rádiového přenosu enormní, bylo možné zachytit prakticky každou zprávu, takže do rukou krypto-analytiků proudil nepřetržitý přísun šifrových textů. Odhaduje se, že během války zachytili Francouzi asi sto milionů slov německých komunikací.

Francouzi byli nejvýkonnější ze všech válečných kryptoanalyti-ků. Již na

začátku války měli nejsilnější kryptoanalytický tým v Evropě, což patřilo k důsledkům zdrcující porážky v prusko-francouzské válce. Napoleon III. ve snaze povzbudit svou klesající popularitu zaútočil roku 1870 na Prusko, ale nečekal vznik spojenectví mezi Pruskem a jihoněmeckými státy. Prusové vedení Bismarckem převálcovali francouzskou armádu, anektovali Alsasko a Lotrinsko a ukončili francouzskou dominanci v Evropě. Neustálá hrozba nově sjednoceného Německa se stala pro francouzské kryptoanalytiky podnětem, aby zdokonalili své dovednosti a mohli Francii poskytnout přesné informace o záměrech nepřítele.

V této atmosféře napsal Auguste Kerckhoffs své pojednání *La cryptographie militaire* (Vojenská kryptografie). Přestože byl Nizozemec, strávil většinu života ve Francii. Jeho dílo se stalo pro Francouze vynikajícím průvodcem principy kryptoanalýzy. Když o třicet let později *začínala* první světová válka, francouzská armáda již uplatnila Kerckhoffsovy myšlenky v průmyslovém měřítku. Zatímco osamělí géniové jako Painvin zápolili s novými šiframi, týmy expertů, z nichž každý byl specializován na konkrétní šifru, se zabývaly denní rutinní dešifrovací prací. Čas hrál klíčovou roli a kryptoanalytici, pracující jako na běžícím pásu, dodávali informace rychle a efektivně.

Sun-c', autor knih O *válečném uměni,* textů o vojenské strategii vytvořených ve 4. století před naším letopočtem, píše o informacích a zvědech: „Tak mezi lidmi z celého vojska/tobě nejbližšími/nikdo ti nesmí být bližší/než právě oni/Nikdo nesmí být štědřeji obdarován/než právě oni/a nic nesmí být ve větší tajnosti drženo/než to, co oni činí.*" Francouzi těmto jeho slovům pevně věřili a vedle zdoko* Český překlad Oldřicha Krále dle vydání Mistr Sun: *O válečném umění,* Votobia, Olomouc 1995.nalování svých kryptoanalytických dovedností vyvinuli i několik doplňkových technik pro získávání informací z rádiového vysílání, aniž by depeše bylo třeba dešifrovat. Francouzské stanice specializované na odposlech se například naučily rozpoznávat telegrafistův *rukopis.* Když je zpráva zašifrovaná a odesílá se v morseovce jako řada teček a čárek, lze každého operátora identifikovat podle jeho rytmu, pauz, rychlosti vysílání, relativní délky teček a čárek. Jde o ekvivalent normálního rukopisu. Francouzi vedle běžných odposlechových stanic postavili šest specializovaných pracovišť na stanovení směru, odkud vysílání přichází. Každá stanice natáčela anténu, dokud nenaladila nejsilnější signál a tím neurčila směr. Kombinací takto určeného směru ze dvou nebo více stanic se dala přesně určit pozice nepřátelské vysílačky. Kombinací rukopisu operátora a místa vysílání se dala určit jak identita, tak přesné umístění například konkrétního pluku. Francouzská rozvědka mohla jednotlivé útvary nepřítele takto sledovat v pohybu po několik dní a postupně odhadnout jejich cíl a určení. Tento způsob sběru zpravodajských informací, známý jako analýza provozu, nabýval na významu zejména tehdy, když nepřítel zavedl novou šifru. Ta sice na čas vyřadila kryptoanalýzu, avšak i nedešifrovatelná zpráva mohla pomocí *analýzy* provozu poskytnout cenné informace.

Bdělost francouzské strany byla v příkrém protikladu k přístupu Němců, kteří vstoupili do války, aniž by měli jakýkoli útvar vojenské kryptografie. Teprve roku 1916 zřídili Abhorchdienst - organizaci zaměřenou na odposlech spojeneckých

depeší. Toto zpoždění lze částečně vysvětlit tím, že německá armáda již na začátku války vstoupila na francouzské území. Francouzi při ústupu zničili pozemní komunikační spoje a Němci se tak museli spoléhat na rádiovou komunikaci. Francouzi měli tudíž stálý přístup k odposlechnutým německým depeším, zatímco opačně to neplatilo. Francouzi se stahovali na vlastní území, kde měli stále k dispozici telegraf a nemuseli komunikovat bezdrátově. Němci je proto nemohli odposlouchávat a neměli tudíž ani důvod zřídit příslušné oddělení dříve než po dvou letech války.

K pokrokům spojenecké kryptoanalýzy významně přispěli také Britové a Američané. Převahu spojeneckých kryptoanalytiků a jejich vliv na výsledek války lze nejlépe ilustrovat na dešifrování německého telegramu zachyceného Brity 17. ledna 1917. Příběh tohoto dešifrování ukazuje, jak může kryptoanalýza ovlivnit válečné události na nejvyšší úrovni. Rovněž poukazuje na důsledky spojené s použitím nedostatečné šifry. Dešifrovaný telegram způsobil, že během několika týdnů Amerika opustila svou politiku neutrality a způsobila tak zvrat v rovnováze sil.

Navzdory naléhání britských i amerických politiků odmítal prezident Woodrow Wilson po první dva roky války vyslat americká vojska na pomoc Dohodě. Jednak nechtěl, aby americká mládež krvácela na evropských válečných polích, jednak věřil, že válku může ukončit jen jednání, a předpokládal, že nejlépe světu poslouží, když si zachová neutralitu a bude vystupovat v roli zprostředkovatele. V listopadu 1916 spatřil Wilson naději na dohodu s Německem v nástupu nového ministra zahraničí Arthura Zimmermanna, žo-viálního mohutného muže, který působil dojmem hlasatele nové,osvícené éry německé diplomacie. Americké noviny tiskly titulky jako NÁŠ PŘÍTEL ZIMMERMANN A LIBERALIZACE V NĚMECKU, jeden z článků jej označil za „jedno z nejnadějnějších znamení pro budoucnost německo-amerických vztahů". Zimmermann však - aniž by o tom Američané věděli - neměl v úmyslu směřovat k míru. Namísto toho plánoval, jak německou agresi dále rozšířit.

Již v roce 1915 potopila německá ponorka plující pod hladinou parník *Lusitania*, na němž zahynulo 1198 cestujících, z toho 128 amerických civilistů. Tato událost by vedla ke vstupu USA do války, nebýt německého ujištění, že napříště se budou ponorky před útokem vynořovat na hladinu, čímž by se mělo předejít nechtěným útokům na civilní lodě. 9. ledna 1917 se však Zimmermann zúčastnil zásadní porady na německém zámku Pless, kde se velení vojsk snažilo přesvědčit císaře, že je na čase tento slib porušit a zahájit neomezenou ponorkovou válku. Němečtí velitelé věděli, že budou-li odpalovat svá torpéda pod hladinou, jsou jejich ponorky téměř ne-zranitelné, a proto věřili, že právě to by se mohlo stát klíčovým faktorem, jenž by rozhodl o výsledku války. Německo stavělo flotilu dvou set ponorek a nejvyšší velení tvrdilo, že neomezená ponorková válka by zcela odřízla britské zásobování a během šesti měsíců přivedla Británii až ke kapitulaci.

V takovém případě bylo z německého hlediska nezbytné, aby bylo vítězství dosaženo opravdu rychle. Neomezená ponorková válka a nevyhnutelné útoky na americké civilní lodi by téměř určitě měly za následek to, že by Amerika vyhlásila

válku Německu. Němci si toho byli vědomi, a proto potřebovali, aby Dohoda kapitulovala dříve, než by Amerika mohla mobilizovat své síly a vstoupit na evropská bojiště. Když porada v Pless končila, byl císař přesvědčen, že rychlé vítězství je možné, a tak podepsal rozkaz zahájit neomezenou ponorkovou válku. Rozkaz měl vstoupit v platnost 1. února.

Během tří týdnů, jež do tohoto data zbývaly, navrhl Zimmermann zabezpečení. Protože neomezená ponorková válka zvyšovala riziko, že USA vstoupí do boje, Zimmermann potřeboval plán, jak oddálit a oslabit americké angažmá v Evropě, případně jak mu úplně zabránit. Zimmermann vymyslel, že se Německo spojí s Mexikem. Měl v úmyslu přesvědčit mexického prezidenta, aby zaútočil na USA a snažil se získat území Texasu, Nového Mexika a Arizony. Německo by podporovalo Mexičany v boji proti společnému nepříteli, pomáhalo by jim finančně a vojensky.

Kromě toho Zimmermann chtěl, aby mexický prezident působil jako prostředník a přesvědčil Japonsko, aby rovněž zaútočilo na Ameriku. Německo by pak ohrožovalo americké východní pobřeží, Japonsko by zaútočilo na západě a Mexiko by provedlo invazi z jihu. Hlavním Zimmermannovým záměrem bylo způsobit Americe doma tak velké problémy, že by si nemohla dovolit poslat vojska do Evropy. Německo by pak mohlo vyhrát válku na moři, válku v Evropě a poté se stáhnout z amerického dobrodružství. 16. ledna shrnul Zimmermann svůj návrh v telegramu adresovaném německému velvyslanci ve Washingtonu, který jej měl poslat dál velvyslanci v Mexiku a ten předat mexickému prezidentovi. Na obrázku 28 je faksimile šifrovaného telegramu. Jeho text zní takto:

„Máme v úmyslu zahájit k prvnímu únoru neomezenou ponorkovou válku. Navzdory tomu se chceme snažit zachovat neutralitu Spojených států. Pro případ, že by se to nepodařilo, předkládáme Mexiku návrh spojenectví na následujícím základě: společný postup ve válce, společný postup v míru, štědrá finanční podpora a náš souhlas s tím, aby Mexiko získalo zpět ztracená území v Texasu, Novém Mexiku a Arizoně. Detaily takového ujednání jsou na vás.

Informujte prezidenta [Mexika] co nejdiskrétněji ve chvíli, kdy bude zřejmé, že k válce se Spojenými státy dojde. Navrhněte mu rovněž, že byz vlastní iniciativy mohl přizvat Japonsko k bezprostřední spolupráci a zároveň působit jako prostředník mezi Japonskem a námi.

Prosím, soustřeďte prezidentovu pozornost na fakt, že neomezené nasazení našich ponorek skýtá vyhlídku přimět Anglii uzavřít mírovou smlouvu během několika měsíců. Potvrďte příjem.

Zimmermann."

Zimmermann musel telegram zašifrovat, protože Němci věděli, že jejich protivníci odposlouchávají veškerou komunikaci přes Atlantik. Toho dosáhli nepřátelé Německa již při první britské útočné akci celé války. Před úsvitem prvního dne první světové války se pod rouškou tmy přiblížila britská loď *Telconia* k německému pobřeží, spustila kotvu a vyzvedla nahoru svazek podmořských kabelů. Šlo o německé transatlantické kabely - komunikační spojení Německa se zbytkem světa. Než vyšlo slunce, byly kabely poškozeny. Cílem této sabotáže bylo

zničit nejbezpečnější součást německých komunikací, takže Němci museli nadále komunikovat prostřednictvím zranitelnějšího rádia anebo přes kabely ve vlastnictví jiných zemí. Proto byl Zimmermann nucen poslat svůj telegram přes Švédsko a vedle toho i přímým kabelem vlastněným Američany. Obě trasy procházely přes Anglii, takže text Zimmermannova telegramu, jak mělo brzy vyjít najevo, padl do britských rukou.

Zachycený telegram byl předán do tzv. Kanceláře č. 40, šifrovacího oddělení admirality, jež neslo jméno podle svého původního umístění. Kancelář č. 40 představovala podivnou směs jazykovědců, klasických vědců a nadšených luštitelů hádanek, kteří tvořili jako celek sílu schopnou nejvyšších kryptoanalytických výkonů. Tak například reverend Montgomery, nadaný překladatel německých teologických děl, dešifroval tajnou zprávu ukrytou na pohlednici, jejíž adresa zněla Sir Henry Jones, 184 King's Road, Tigh-nabruaich, Skotsko. Pohlednice byla odeslána z Turecka, takže sir Henry předpokládal, že odesilatelem je jeho syn, kterého Turci zajali. Byl však zmaten, protože na pohlednici nebyl žádný text a adresa byla podivná - vesnice Tighnabruaich byla tak malá, že domy v ní neměly čísla a nikde byste tam nenašli žádnou King's Road (Královská ulice). Reverend Montgomery nakonec rozluštil ukryté poselství. Adresa odkazovala na *Bibli*, její *První knihu královskou*, kapitolu 18, verš 4: „Ujal se Obadjáš sta proroků, schoval je po padesáti mužích v jeskyni a opatřoval je chlebem a vodou." Syn sira

Henryho se prostě snažil ujistit svou rodinu, že jeho věznitelé se o něj starají přijatelně.

Když dorazil šifrovaný Zimmermannův telegram do Kanceláře *c.* 40, byl to právě Montgomery, komu byl svěřen k vyluštění. Spolupracoval s ním Nigel de Grey, vydavatel z firmy Williama Heinemanna. Oba okamžitě zjistili, že mají co dělat s šifrou určenou výhradné pro diplomatickou komunikaci nejvyšší úrovně, proto nakládali s telegramem jako s prioritním úkolem. Dešifrování nebylo triviální, ale mohli při něm těžit ze zkušeností, které získali s podobnými depešemi již dříve. Během několika hodin měli odděleny jednotlivé úseky textu a pochopili, že jde o zprávu mimořádného významu. Pokračovali a do večera se jim začal rýsovat Zimmermannův zákeřný plán. Nakonec před sebou viděli děsivé důsledky neomezené ponorkové války a zároveň jim bylo zřejmé, že německý ministr zahraničí zvažuje útok na Ameriku, což by prezidenta Wilso-na patrně přimělo zrušit neutralitu. Telegram obsahoval smrtelnou hrozbu, zároveň však naději, že by se Amerika mohla přidat k Dohodě.

Montgomery a de Grey odnesli částečně rozluštěný telegram veliteli námořní rozvědky, jímž byl admirál sir William Hall, a očekávali, že jej předá Američanům a tím je přiměje vstoupit do války. Admirál Hall však uložil výsledek jejich práce do trezoru a požádal je, ať napřed vyluští i zbytek. Nechtěl odevzdat Američanům částečně vyluštěný text pro případ, že by v dosud nerozluštěné části byla skryta další neznámá hrozba. Kromě

toho měl i jinou starost. Kdyby Britové předali Američanům rozluštěný Zimmermannův telegram a kdyby Američané reagovali veřejně, pak by se Němci dověděli, že jejich šifra byla prolomena. To by je vedlo k tomu, že by vyvinuli novou, silnější šifru a odřízli by tak britskou rozvědku od informací. Hall si byl v každém případě vědom toho, že za dva týdny má začít neomezená ponorková válka. Ta by sama o sobě mohla stačit k tomu, aby prezident Wilson vyhlásil Německu válku. Nebyl žádný důvod ohrozit cenný zdroj zpravodajských informací, když žádoucí účinek se měl dostavit tak jako tak.

Prvního února zahájilo Německo podle rozkazu císaře neomezený námořní boj. O den později svolal Woodrow Wilson svůj kabinet, aby se rozhodli, jak má Amerika reagovat. 3. února promluvil ke Kongresu a oznámil, že USA zůstanou neutrální a budou působit jako mírotvůrce, ne jako jedna z bojujících stran. Tím překvapil jak Němce, tak jejich protivníky. Admirál Hall teď neměl jinou volbu než zveřejnit Zimmermannův telegram.

Montgomery a de Grey dokončili dešifrování do čtrnácti dnů od chvíle, kdy se poprvé obrátili na svého nadřízeného. Hall mezitím našel způsob, jak neuvést Němce v podezření, že jejich utajení není dokonalé. Zjistil, že německý velvyslanec v USA von- Bernstorff měl odeslat telegram německému velvyslanci v Mexiku von Eckhardto-vi až po několika malých úpravách. Měl například odstranit instrukce, jež byly určeny jemu samému, a samozřejmě také změnit adresu.

Von Eckhardt měl pak dodat takto pozměněný telegram v dešifrované podobě mexickému prezidentovi. Kdyby Hall získal mexickou verzi Zimmermannova telegramu, pak by jej bylo možné publikovat v novinách a Němci by předpokládali, že text byl ukraden v Mexiku, nikoli zachycen a dešifrován Brity. Hall kontaktoval britského agenta v Mexiku, známého pouze pod jménem pan H., který pronikl do mexické telegrafní služby a získal, co bylo třeba - mexickou verzi Zimmermannova telegramu.

Tuto verzi Hall předal britskému ministru zahraničí Arthuru Balfourovi. Ten si 23. února povolal amerického velvyslance Walte-ra Page a předložil mu Zimmermannův telegram, což později nazval „nejdramatičtějším okamžikem mého života". O čtyři dny později si sám prezident Wilson prohlédl „výmluvný důkaz", jak telegram sám nazval, že Německo chystá přímou agresi vůči USA.

Telegram byl předán tisku a americká veřejnost se mohla konečně seznámit se skutečnými německými záměry. Američané byli celkem zajedno v tom, že je třeba reagovat, v amerických vládních kruzích se však objevila obava, že by telegram mohl být podvodem,který mohli vymyslet

Britové, aby dostali USA do války. Otázka autenticity však brzy ztratila smysl, když Zimmermann veřejně připustil autorství. Na tiskové konferenci v Berlíně se dostal pod tlak a řekl: „Nemohu to popřít. Je to pravda."

Německé ministerstvo zahraničí začalo vyšetřovat, jak Američané Zimmermannův telegram získali. Chytili se přitom do Hallovy pasti a došli k závěru, že „z různých náznaků plyne, že ke zradě došlo v Mexiku". Hall mezitím dále odvracel pozornost od práce britských kryptoanalytiků. Zařídil, aby britský tisk zveřejnil komentář kritizující jeho vlastní organizaci, že Zimmermannův telegram nezachytila, což vedlo k sérii článků, které napadaly britské tajné služby a velebily Američany.

Ještě počátkem roku Wilson řekl, že by bylo „zločinem proti civilizaci" vést národ do války, avšak 2. dubna 1917 změnil názor: „Doporučuji, aby Kongres shledal, že současné kroky říšské vlády nejsou ničím menším než válkou proti vládě a lidu Spojených států, a aby formálně akceptoval statut válčící strany, kterou jsme se takto stali." Jedna prolomená šifra v Kanceláři č. 40 uspěla tam, kde se to nepovedlo po tři roky intenzivní diplomacii. Americká historička Barbara Tuchmanová, autorka knihy *The Zimmermann Telegram* (Zimmermannův telegram), analyzuje situaci takto:

„Kdyby nebyl telegram zachycen nebo kdyby nebyl publikován, udělali by Němci nevyhnutelně nakonec něco jiného, *co* by nás přimělo vstoupit do války. Času však již zbývalo málo, a kdybychom se opozdili ještě více, mohla by být Dohoda přinucena vyjednávat. V tomto smyslu změnil Zimmermannův telegram dějiny.... Sám o sobě byl Zimmermannův telegram jen oblázkem na dlouhé cestě historie. Oblázek však může zabít Goliáše a tento oblázek zničil americkou iluzi, že se můžeme starat o své záležitosti bezstarostně a odděleně od ostatních národů. Z hlediska mezinárodní politiky to bylo drobné spiknutí vymyšlené německým ministrem. Z hlediska amerického lidu to byl konec nevinnosti."

Svatý grál kryptografie

Během první světové války došlo k řadě kryptoanalytických vítězství, jež vyvrcholila Zimmermannovým telegramem. Již od prolomení Vigenerovy šifry v 19. století měli kryptoanalytici trvalou

převahu nad tvůrci šifer. Ke konci války, když byla deprese mezi kryptografy největší, dosáhli američtí vědci významného zvratu. Zjistili, že Vigenerovu šifru lze použít jako základ nové, odolnější formy šifrování. Nová šifra mohla dokonce poskytnout zcela dokonalé utajení.

Základní slabinou Vigenerovy šifry je její cyklická povaha. Má-li klíčové slovo pět písmen, pak každé páté písmeno otevřeného textu se šifruje pomocí téže šifrové abecedy. Podaří-li se kryptoanalytiko-vi stanovit délku klíče, pak lze s šifrovým textem nakládat jako se sadou monoalfabetických šifer a jednu po druhé rozluštit pomocí frekvenční analýzy. Zvažme však, co se stane, vzroste-li délka klíče.

Představte si text o délce 1 000 písmen zašifrovaný Vigeněrovou šifrou, který se snažíme rozluštit. Pokud má použitý klíč jen 5 písmen, vede luštění ke frekvenční analýze pěti sad po 200 písmenech, což je snadné. Pokud je klíč dlouhý 20 písmen, půjde o 20 sad po 50 písmenech, což je mnohem těžší. Pokud by však

klíč sestával z 1 000 písmen, pak stojíme před frekvenční analýzou 1 000 sad po jednom písmenu - a ta je nemožná. Jinými slovy, pokud je klíč stejně dlouhý jako zpráva, pak nelze použít techniku, kterou vymysleli Babbage a Ka-siski.

Klíč dlouhý jako zpráva sama - to zní dobře, ale je zřejmé, že s ním budou problémy. Má-li zpráva stovky písmen, musí je mít i klíč. Než takový klíč vytvářet od nuly, může být lákavé založit jej například na slovech písně. Kryptograf může také vzít například knihu o pozorování ptáků a vytvořit klíč pomocí náhodně vybraných ptačích jmen. Takové klíče však mají jednu zásadní chybu.

V následujícím příkladu jsem zašifroval úsek textu pomocí Vigeněrovy šifry a použil jsem klíčové slovo stejně dlouhé jako zpráva. Všechny dosud popsané kryptoanalytické metody v této situaci selžou. Přesto lze zprávu rozluštit.

Klíč ??????????????????????

Otevřený text ?????????????????????? Šifrový text VHRMHEUZNFQDEZRWXFIDK

Kryptoanalýza vychází z předpokladu, že text obsahuje některá běžná slova, jako například the (anglický určitý člen). Postupujeme tak, že náhodně umístíme slovo the na různá místa otevřeného textu, jak je to patrné z ukázky níže, a odvodíme, které písmeno v klíči by převedlo the na odpovídající šifrový text. Předpokládáme-li na-příklad, že the je prvním slovem otevřeného textu, co z toho vyplývá pro první tři písmena klíče? První písmeno klíče má převést t na V. Abychom zjistili první písmeno klíče, vezmeme Vigenerův čtverec, prohlédneme si sloupec, v jehož záhlaví je t, a hledáme v něm V. Zjistíme, že na začátku příslušného řádku je C. Stejný postup opakujeme s písmeny h a e, jež jsou šifrována jako H a R, a tak najdeme kandidáty na první tři písmena klíče: CAN. To vše *vychází* z předpokladu, že the je prvním slovem otevřeného textu. Zkusíme umístit the na jiná místa textu a znovu odvodíme odpovídající znaky klíče. (Můžete si je nalézt sami pomocí Vigeněrova čtverce v tabulce 9).

Klíč CAN???BSJ?????YPT????

Otevřený text the???the?????the???? Šifrový text VHRMHEUZNFQDEZRWXFIDK

Vyzkoušeli jsme the na třech různých, místech šifrového textu a vytvořili jsme tři možné úseky klíče. Jak zjistit, zda je některé the umístěno správně? Máme-li podezření, že klíč je tvořen slovy, jež dávají smysl, můžeme toho zkusit využít. Pokud je the na nesprávné pozici, pak dostaneme v klíči pravděpodobně chaotickou změť písmen. Pokud je umístěno správně, může daná část klíče dávat smysl. Například první the nám poskytlo písmena CAN, což je povzbudivé, neboť jde o běžnou anglickou slabiku, která je součástí mnoha slov. Je tedy možné, že toto the jsme umístili správně. Druhé the poskytlo BSJ, velmi neobvyklou kombinaci písmen, která naznačuje, že tady jsme asi sáhli vedle. Třetí the vedlo k Y PT, což je také neobvyklá kombinace, stojí však za bližší prozkoumání. Jestliže je Y PT součástí klíče, pak by mohlo být částí delšího slova. Jako jediné možnosti [v angličtině, pozn. překl.] připadají v úvahu slova APOCALYPTIC, CRYPT a EGYPT a slova od nich odvozená. Jak zjistíme, zda některé z těchto slov je součástí klíče? Každou z těchto hypotéz můžeme ověřit tím, že vložíme příslušná

slova do klíče a odvodíme odpovídající otevřený text:

Klíč CAN?????APOCALYPTIC??

Otevřený text the?????nqcbeothexg?? Šifrový text VHRMHEUZNFQDEZRWXFIDK

Klíč CAN??????????CRYPT????

Otevřený text the?????????cithe???? Šifrový text VHRMHEUZNFQDEZRWXFIDK

Klíč CAN??????????EGYPT????

Otevřený text the?????????atthe???? Šifrový text VHRMHEUZNFQDEZRWXFIDK

Pokud testované slovo není součástí klíče, dostaneme patrně náhodnou změť písmen, pokud je, bude část otevřeného textu dávat $_{sm}$ysl. Ze slova APOCALYPTIC získáme ryzí blábol. Se slovem CRYPT se *nabízejí* písmena cithe, což by mohla být součást otevřeného textu. Avšak slovo EGYPT nám poskytne písmena atthe, což je velmi slibné - patrně jde o slova at the [vazba odpovídající české předložce „v", „na"-pozn. překl.].

Prozatím budeme předpokládat, že nejpravděpodobnější možností je slovo EGYPT jako součást klíče. Možná je klíč seznamem názvů států. Potom by CAN na začátku klíče mohlo být součástí slova CANADA. Hypotézu můžeme ověřit, zkusíme-li s její pomocí vytvořit další úsek otevřeného textu:

Klíč CANADA??????EGYPT????

Otevřený text themee??????atthe???? Šifrový text VHRMHEUZNFQDEZRWXFIDK

Předpoklad podle všeho funguje. CANADA vede k tomu, že otevřený text začíná písmeny themee, což by mohl být začátek slov the meeting (schůzka). Když jsme uhodli další písmena otevřeného textu, tedy ting, můžeme odvodit odpovídající část klíče, což je BRAZ, zcela jistě začátek slova BRAZIL (Brazílie). Pomocí kombinace CANADABRAZILEGYPT dešifrujeme text: themeetingis atthe???? (schůzka se koná v ????).

Abychom nalezli poslední slovo otevřeného textu, kterým je místo konání schůzky, bude nejlépe pokusit se klíč dokončit testováním možných jmen zemí a pozorováním, jaký otevřený text poskytují. Jediný text, který dává smysl, se dá odvodit v případě, že posledním kouskem klíče je slovo ČUBA:

Klíč CANADABRAZILEGYPTCUBA

Otevřený text themeetingisatthedock Šifrový text VHRMHEUZNFQDEZRWXFIDK

Je vidět, že klíč stejně dlouhý jako zpráva sám o sobě nestačí k záruce utajení. Zranitelnost šifry v předchozím příkladu je dána titn, že klíč se skládá ze smysluplných slov. Začali jsme tím, že

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

jsme

Tabulka 9: Vigeněrův čtverec

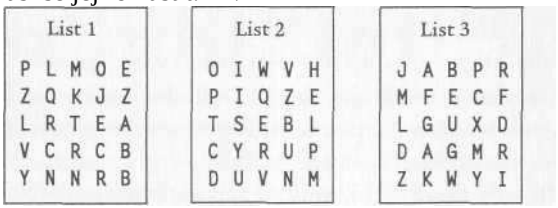
náhodně rozmístili v textu the a nalezli odpovídající písmena klíče. Mohli jsme stanovit, zda je the umístěno správně, protože pokud bylo, daly se v klíči rozpoznat úseky slov. Ty jsme pak použili, abychom našli celá slova klíče. Z nich se podařilo odvodit některá slova otevřeného textu, z nich zas další úseky klíče a tak dále. Celý postup přeskakování sem a tam mezi klíčem a textem fungoval jen díky tomu, že klíč měl jasnou strukturu a sestával z rozpoznatelných slov. Roku 1918 však kryptografové začali experimentovat s klíči, jež strukturu postrádají. To vedlo k nerozluštitelné šifře.

V době, kdy se první světová válka chýlila ke konci, přišel major Joseph Mauborgne, šéf kryptografického výzkumu v americké armádě, s konceptem náhodného klíče - takového, jenž není tvořen

rozpoznatelnými slovy, ale náhodným sledem znaků. Byl zastáncem náhodného klíče použitého spolu s Vigenerovou šifrou, čímž by vznikl bezprecedentní stupeň bezpečnosti. Prvním krokem jeho systému bylo sestavení tlustého sešitu tvořeného stovkami listů, z nichž každý obsahoval unikátní klíč ve formě řádků náhodně seřazených písmen. K dispozici musely být dvě kopie takového sešitu, jedna pro odesilatele, druhá pro příjemce. Pro zašifrování zprávy měl odesilatel použít Vigenerovu šifru, přičemž jako klíč vzal první list sešitu. Obrázek 30 ukazuje tři

listy takového sešitu (při reálném použití by však každý z listů obsahoval stovky písmen) a dále zprávu zašifrovanou pomocí prvního z nich. Příjemce může zprávu snadno dešifrovat pomocí téhož listu. Jakmile byla zpráva úspěšně zašifrována, odeslána a dešifrována, zničí odesilatel i příjemce list, jenž sloužil jako klíč, takže jej již nikdy znovu nepoužijí. Příští zpráva bude zašifrována pomocí dalšího náhodného klíče a tak dále. Protože se každý klíč použije jen jednou, systému se říká *jednorázová tabulková šifra*.*

Tato šifra řeší všechny dosavadní nesnáze. Představte si, že zpráva attack the vaTley at dawn („zaútočte na údolí za úsvitu") byla zašifrována podle obrázku 30, odeslána rádiem a zachycena nepřítelem. Šifrový text dostane kryptoanalytik a pokusí se jej rozluštit. První



Klíč PLMOEZQKJZLRTEAVCRCBY

Otevřený text attacktheval 1 eyatdawn Šifrový text PEFOGJJRNULCEIYVVUCXL

Obrázek 30: Tři listy, z nichž každý je potenciálním klíčem pro jednorázovou tabulkovou šifru. Zpráva je zašifrována pomocí listu č. 1.

*V češtině se pro anglický výraz „one-time pad" používá také termín „jednorázové heslo", které může být realizováno tabulkou nebo například proudem znaků na děrné pásce nebo CD-ROM apod. (Pozn. odborného lektora.)obtíž spočívá v tom, že v náhodném klíči neexistuje žádné opakování, takže metoda, kterou vymysleli Babbage a Kasiski, u jednorázové tabulkové šifry nefunguje. Jako další možnost může kryptoana-lytik zkusit postup s náhodným rozmisťováním slova the a odvodit odpovídající část klíče, jak jsme to udělali u předchozího příkladu. Když umístí the na začátek zprávy, což není správně, dostane jako odpovídající úsek klíče náhodnou posloupnost písmen WXB. Když umístí the na sedmou pozici zprávy, což je náhodou správně, pak odpovídajícím úsekem klíče je QKJ - rovněž náhodná posloupnost písmen. Jinými slovy, nelze nijak zjistit, zda je zkušební slovo umístěno správně či špatně.

V nouzi může kryptoanalytik zvážit, zda nevyzkoušet všechny myslitelné klíče. Šifrový text má 21 písmen, takže klíč je stejně dlouhý. To znamená, že existuje přibližně 500 000 000 000 000 000 000 000 000 000 možných klíčů, což naprosto přesahuje možnosti člověka či mechanického zařízení. I kdyby však kryptoanalytik dokázal otestovat všechny klíče, je zde další - a ještě větší - překážka. Testováním každého myslitelného klíče odhalí kryptoanalytik ukrytou zprávu, avšak nejen ji. Následující klíč aplikovaný na stejný šifrový text dává například zcela odlišnou zprávu, a sice defend the hill at sunset (braňte pahorek za západu slunce).

Klíč MAAKTGQKJNDRTIFDBHKTS

Otevřený text defendthehillatsunset Šifrový text PEFOGJJRNULCEIYVVUCXL

Je-li možné testovat všechny klíče, bude generována každá myslitelná zpráva o délce 21 písmen a kryptoanalytik nebude moci odlišit tu pravou od všech ostatních.

Tato potíž by nevznikla, kdyby klíčem byla řada slov či věta, protože nekorektní zprávy by téměř určitě odpovídaly klíči, který by nenesl žádný význam, zatímco korektní zprávu by prozradil smysluplný klíč.

Bezpečnost jednorázové tabulkové šifry je plně dána náhodným charakterem klíče. Klíč vnáší tento náhodný charakter i do šifrového textu, takže v něm nejsou žádné zákonitosti, žádná struktura, prostě nic, čeho by se kryptoanalytik mohl chytit. Je dokonce možné dokázat matematicky, že jednorázovou tabulkovou šifru nelze rozluštit. Jinými slovy, nejde jen o věc víry, jako tomu bylo u Vige-nerovy šifry v 19. století: jednorázová tabulková šifra je *skutečně absolutně bezpečná*. Nabízí plnou záruku: svatý grál kryptografie.

Kryptografové tedy konečně našli systém, který nelze rozluštit, Dosažení této dokonalosti však neukončilo boj o utajení. Po pravdě řečeno, tato šifra se *užívá*, jen málo. V teorii funguje perfektně, ale z hlediska praxe má dvě velké slabiny. První z nich je problém s vytvářením velkého množství náhodných klíčů. Armáda si během jediného dne může vyměnit stovky zpráv, každou z nich v délce tisíců znaků, takže radisté by potřebovali denní přísun milionů náhodně uspořádaných písmen. To je obrovský úkol.

Kdysi se kryptografové domnívali, že lze generovat náhodné klíče prostě tím, že se naslepo ťuká na psacím stroji. Kdykoli se to však zkoušelo, měly písařky tendenci střídat při psaní levou a pravou ruku víceméně pravidelně. To je možná rychlý způsob vytvoření klíče, avšak výsledná řada má určitou strukturu a není náhodná. Pokud písařka udeří na klávesu D, jež se nachází v levé části klávesnice, pak bude další znak pravděpodobně z její pravé části. Má-li být jednorázová tabulková šifra opravdu náhodná, pak zhruba v polovině případů musí za znakem z levé části klávesnice následovat další znak z této poloviny.

Kryptografové brzy zjistili, že vytvořit skutečně náhodný klíč vyžaduje hodně času, úsilí a peněz. Nejlepší náhodné klíče vznikají využitím přírodních procesů, například radioaktivity, o níž víme, že její charakter je skutečně náhodný. Kryptograf může vzít kus radioaktivního materiálu a sledovat jeho emisi pomocí Geigerova počítače. Okamžiky, kdy je emise radioaktivních paprsků častější, se budou střídat s okamžiky menší aktivity. Délka pauz mezi emisemi je nepředvídatelná a náhodná. Ke Geigerovu počítači bychom mohli připojit displej, na němž by se dokolečka zobrazovala stálou a velkou rychlostí abeceda, až by se zobrazení ve chvíli průchodu paprsku zastavilo. Písmeno na displeji by se pak použilo jako jedno z písmen náhodného klíče. Displej by se poté znovu rozběhl a zastavil zas ve chvíli, kdy by došlo k další emisi. Do klíče by se přidalo další písmeno a tak stále dokola. Takové uspořádání by sice zaručovalo opravdovou náhodnost klíče, pro každodenní použití je však příliš nepraktické.

I když dokážeme vyrobit dostatek náhodných klíčů, zbývá druhý problém: jejich distribuce. Představte si bitevní situaci, v níž pracuje komunikační síť se stovkami operátorů. Každý z nich musí mít identickou kopii sešitu se šiframi. Nové sešity je třeba vydat všem současně. A při jejich použití je třeba zaručit, aby nikdo nevypadlz rytmu, aby všichni pracovali vždy s touž tabulkou. Kdyby k takovému způsobu šifrování mělo opravdu dojít, zaplnilo by se bojiště poslíčky a úředníky. A

co horšího, jakmile by jedna sada klíčů padla do rukou nepříteli, celý komunikační systém by byl vyzrazen.

Možná je lákavé odstranit tyto problémy a používat jeden klíč opakované, to však patří k nejtěžším kryptografickým hříchům. Opakovaná aplikace jednorázové tabulky umožní nepřátelskému kryptoanalytikovi rozluštit zprávy poměrně snadno. Technika, která umožňuje rozlomit šifru prostřednictvím dvou šifrových textů zašifrovaných pomocí téže jednorázové tabulky, je vysvětlena v dodatku G, nyní postačí říci, že takové použití jednorázové tabulkové šifry je nekorektní. Odesilatel a příjemce musí použít pro každou zprávu nový klíč.

Jednorázová tabulková šifra je vhodná tam, kde se vyžaduje extrémně vysoké utajení a kde nevadí mimořádně vysoké náklady spojené s výrobou a distribucí klíčů. Touto šifrou je například *zabezpečena*, horká linka spojující prezidenty Ruska a USA.

Praktické nedostatky této teoreticky bezchybné koncepce vedly k tomu, že Mauborgneova myšlenka nebyla nikdy využita přímo v boji. Namísto toho se po první světové válce, s plným vědomím všech jejích kryptografických nezdarů, dál hledal praktický systém, který by bylo možné využít v budoucím konfliktu. Kryptografům netrvalo dlouho a dosáhli nového zlomu, jenž umožnil zabezpečit utajenou komunikaci v bojových podmínkách. Pro zdokonalení šifer byli tentokrát nuceni odložit tužku a papír a namísto toho využít k utajení zpráv nejnovějších technologických vymožeností.

Vývoj šifrovacích strojů - od šifrovacích disků k Enigmě

Nejstarším šifrovacím strojem je šifrovací disk, vynalezený v 15. století italským architektem Leonem Albertim, jedním z otců polyalfabetické šifry. Alberti vzal dva měděné kotouče, jeden o něco větší než druhý, a po jejich obvodu napsal písmena abecedy. Pak umístil menší kotouč na větší, uchytil je na společnou osu a získal tak pomůcku podobnou té, jež je na obrázku 31. Kotouči šlo otáčet nezávisle na sobě, takže abecedy mohly zaujímat různé vzájemné

Obrázek 31: Šifrovací disk Konfederace používaný během americké občanské války.

po zice a pomůcka mohla sloužit pro šifrování jednoduchou Caesaro-vou šifrou. Například pro šifru s posunutím o jeden znak stačilo natočit vnější A proti vnitřnímu B - vnější disk zobrazuje otevřenou abecedu, vnitřní abecedu šifrovou. Každé písmeno otevřeného textu lze nalézt na vnějším disku, odpovídající písmeno šifrového textu se nachází naproti němu na vnitřním disku. Zprávu s Caesarovým posunutím o pět písmen vytvoříme tak, že natočíme vnější A proti vnitřnímu F.

Jde o velmi jednoduché zařízení, usnadňuje však šifrování, a proto přetrvalo po pět století. Verze z obrázku 31 se používala v americké občanské válce. Na obrázku 32 je Code-o-Graph, šifrovací disk používaný hrdinou jednoho z prvních amerických rozhlasových seriálů *kapitánem Půlnoc*. Posluchači mohli získat svůj vlastní Code-o--Graph od sponzora pořadu, společnosti Ovaltine, když zaslali etiketu některého z jeho výrobků. Čas od času končilo vysílání tajnou zprávou od kapitána Půlnoc, kterou si věrní posluchači mohli pomocí svého disku rozšifrovat.

Šifrovací disk je jedním z mnoha možných šifrovacích zařízení, tzv. *scramblerů, jež* zpracovávají otevřený text znak po znaku a převádějí jej na něco jiného, Dosud popsaný způsob jejich činnosti je jed-

Obrázek 32: Code-o-Graph kapitána Půlnoc.
Převádí písmena otevřeného textu (vnější disk) na čísla (vnitřní disk), nikoli na písmena.

noduchý a výsledná šifra poměrně snadná k rozluštění, avšak disk lze použít i komplikovanějším způsobem. Jeho vynálezce Alberti doporučoval změnit nastavení disku v rámci téže zprávy, což v důsledku znamená, že namísto monoalfabetické šifry vzniká polyalfabetic-ká. Představme si například, že by Alberti chtěl pomocí svého disku zašifrovat slovo goodbye a použil k tomu klíčové slovo LEON. Začal by nastavením disku podle prvního písmene klíče, takže proti vnějšímu A by nastavil vnitřní L. Pak by zašifroval první písmeno zprávy, tedy g, a to tak, že by jej vyhledal na vnějším disku a přečetl odpovídající písmeno na disku vnitřním - to je R. Před zašifrováním dalšího znaku zprávy by změnil nastavení disku podle druhého písmene klíče a proti vnějšímu A by tentokrát nastavil vnitřní E. Pak by zašifroval písmeno o a dostal by S. Šifrovací proces by pokračoval nastavením disku podle klíčového písmene 0, pak N, pak znovu L a tak dále. Alberti by vlastně zašifroval zprávu Vigeněrovou šifrou, kde by jeho vlastní křestní jméno posloužilo jako klíč. Šifrovací disk zrychluje práci a v porovnání s Vigenerovym čtvercem zmenšuje pravděpodobnost chyb.

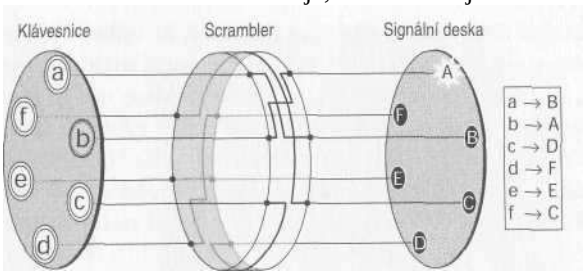
Při tomto použití šifrovacího disku je důležité, že během šifrování se mění jeho nastavení. Tato dodatečná komplikace ztěžuje prolomení šifry, neznemožňuje jej však, protože nejde o nic jiného než o mechanizovanou verzi Vigenerovy šifry, kterou vyluštili Bab-bage a Kasiski. Pět set let po Albertim se však myšlenka šifrovacího disku dočkala návratu v podstatně zdokonalené podobě a vedla ke vzniku nových šifer, o řád náročnějších na rozluštění než jakýkoli starší systém.

Německý *vynálezce* Arthur Scherbius spolu se svým přítelem Richardem Ritterem založil roku 1918 firmu Scherbius & Ritter, jež se zabývala technickými inovacemi na širokém poli od turbín po vyhřívané polštáře. Scherbius odpovídal za výzkum a vývoj a stále hledal nové možnosti uplatnění. Jedním z jeho oblíbených

projektů byla náhrada zastaralých šifrovacích systémů z první světové války, založených na tužce a papíru, něčím dokonalejším, co by využívalo moderní technologie. Díky znalostem, jež získal studiem elektrotechnického inženýrství v Hannoveru a Mnichově, vyvinul šifrovací zařízení, které bylo v podstatě elektrifikovanou variantou Albertiho šifrovacího disku. Pod názvem Enigma vstoupil Scherbiův systém do historie kryptografie jako její nejtěžší noční můra.

Scherbiova Enigma je tvořena mnoha důmyslnými součástmi, jež dohromady tvoří působivý a složitý stroj. Pokud jej však rozložíme na části, je princip fungování celku zcela zřejmý. Základní podoba Scherbiova vynálezu se skládá ze tří vzájemně propojených částí. První z nich je klávesnice pro zadávání otevřeného textu, druhou částí je šifrovací jednotka pro převod každého písmene otevřeného textu na odpovídající písmeno šifrového textu a třetí částí je signální deska tvořená lampičkami, které umožňují zobrazit znak šifrového textu. Na obrázku 33 je znázorněno schéma stroje, pro jednoduchost omezeného na šest písmen abecedy. Máli se zašifrovat písmeno otevřeného textu, stiskne operátor příslušnou klávesu, tím se odešle elektrický signál přes šifrovací jednotku a na druhé straně se na signální desce indikuje příslušný znak šifrového textu.

Klíčovou částí stroje je scrambler, tlustý gumový kotouč protkaný dráty. Vedení přicházející z klávesnice vstupuje do scrambleru na šesti místech, uvnitř se různě otáčí a přehýbá a na šesti místech zas vystupuje ven. Vnitřní zapojení scrambleru určuje, jak budou zašif-



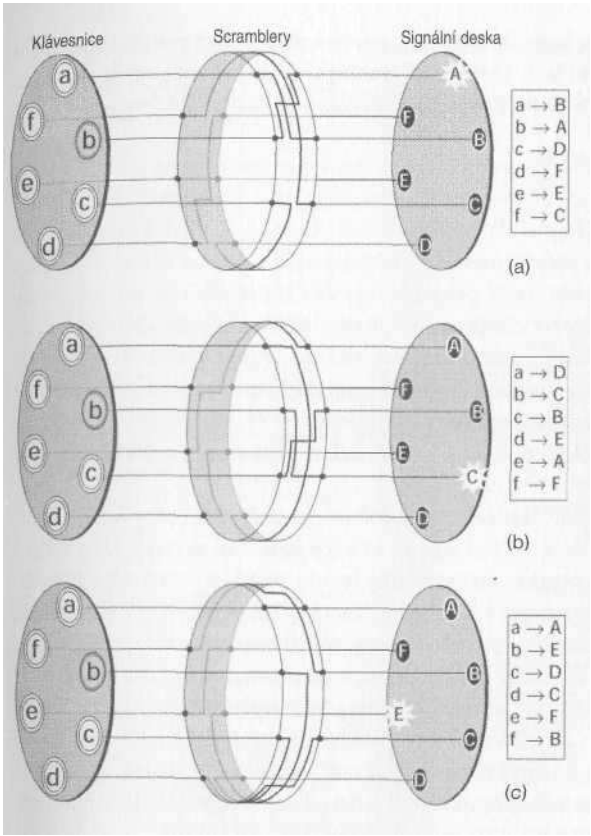
Obrázek 33: Zjednodušená verze stroje Enigma pracující s abecedou tvořenou jen šesti písmeny. Nejdůležitější částí stroje je scrambler. Napíšeme-li na klávesnici b, prochází scramblerem elektrický proud, sleduje vnitřní vedení a na výstupu rozsvítí žárovku A. Stručné řečeno, **b** se zašifruje jako A. Seznam vpravo ukazuje, jak bude zašifrováno každé z šesti písmen abecedy.

rovány znaky otevřené abecedy. Například na obrázku 33 toto zapojení určuje, že:

Napíšeme-li a, rozsvítí se B, takže a je šifrováno jako B. Napíšeme-li b, rozsvítí se A, takže b je šifrováno jako A . Napíšeme-li c, rozsvítí se D, takže c je šifrováno jako D. Napíšeme-li d, rozsvítí se F, takže d je šifrováno jako F. Napíšeme-li e, rozsvítí se E, takže e je šifrováno jako E. Napíšeme-li f, rozsvítí se C, takže f je šifrováno jako C.

Zpráva café se tedy zašifruje jako DBCE. V tomto základním uspořádání scrambler prostě definuje šifrovou abecedu a stroj funguje jako monoalfabetická substituční šifra.

Podstata toho, co Scherbius vymyslel, však spočívá v tom, že disk se po zašifrování každého písmene automaticky pootočí o jednu šestinu otáčky (u reálného stroje pracujícího s úplnou abecedou pak o jednu šestadvacetinu). Obrázek 34a) ukazuje stejné uspořádání jako obrázek 33: stiskneme-li klávesu b, rozsvítí se žárovka A. Tentokrát se však po napsání písmene a rozsvícení žárovky disk otočí o jednu šestinu otáčky do polohy znázorněné na obrázku 34b). Napíšeme-li teď b znovu, rozsvítí se jiné písmeno, konkrétně C. Poté se disk znovu pootočí, jak je vidět na 34c). Tentokrát klávesa b rozsvítí žárovku E. Napíšeme-li b šestkrát po sobě, dostaneme šifrový text ACEBDC. Jinými slovy, šifrová abeceda se po zašifrování každého písmene mění. V tomto rotačním uspořádání definuje scrambler šest šifrových abeced, stroj Lze použít pro šifrování polyalfabetickou šifrou.



Obrázek 34:

Po napsání a zašifrování každého písmene se scrarabler pootočí o jednu pozici a tím se způsob šifrování změní. Na obrázku (a) šifruje scrambler **b** jako A, nová poloha scrambleru na obrázku (b) však

vede k tomu, že **b** se zašifruje jako C. Na obrázku (c), po pootočení o další krok, šifruje scrambler **b** jako E. Po zašifrování dalších čtyř písmen a tedy po čtyřech dalších pootočeních bude scrambler zpět v původní pozici.

Rotace scrambleru je klíčovým prvkem Scherbiovy konstrukce. Stroj v tomto uspořádání však má očividnou slabinu. Napíšeme-li b šestkrát po sobě, scrambler se vrátí do původní polohy. Další opakování písmene b povede k tomu, že se šifrovací schéma bude stále opakovat. Kryptografové se obecně vzato snaží takovému opakování vyhnout, protože vede k pravidelnosti a vnáší do šifrového textu strukturu - příznak slabé šifry. Tomu lze čelit zavedením druhého scramblerového disku.

Na obrázku 35 je schématický náčrtek šifrovacího stroje se dvěma scramblery. Protože je obtížné zakreslit skutečnou třírozměrnou strukturu vnitřního propojení, obrázek 35 se omezuje na dvourozměrné zjednodušení. Vždy po zašifrování jednoho písmene se první scrambler pootočí o jednu pozici. Druhý scramblerový disk je povětšinu času nehybný. Pootočí se teprve tehdy, když první scrambler dokončí celou otáčku. Dosáhne se toho například tak, že na prvním scrambleru je zub, který pohne druhým scramblerem jen jednou za

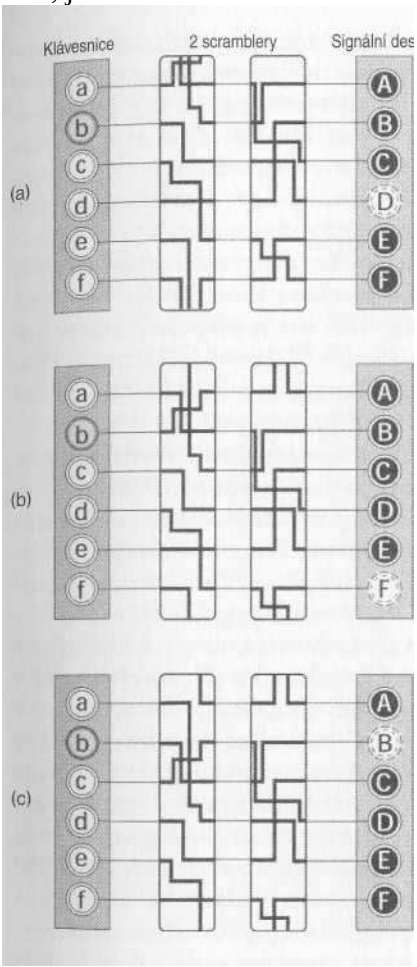
celý oběh.

Na obrázku 35a) je první scrambler v poloze, kdy se právě chystá pohnout druhým. Napíšeme-li a zašifrujeme písmeno, mechanismus se přestaví do polohy znázorněné obrázkem 35b). První scrambler se pohnul o jedno místo, druhý rovněž o jedno místo. Napíšeme-li a zašifrujeme další písmeno, první scrambler se opět pohne o jedno místo, druhý zůstane nehybný - až do té doby, dokud první scrambler nedokončí celou otáčku, což bude po zašifrování dalších pěti písmen. Uspořádání je podobné tachometru v autě: kotouč udávající počet kilometrů se otáčí poměrně rychle, teprve když dokončí celou otočku, pohne o jeden dílek kotoučem udávajícím desítky kilometrů.

Výhoda přidání druhého scrambleru spočívá v tom, že se schéma šifrování po dokončení úplné otáčky prvního scrambleru nezačne opakovat. K opakování sice dojde, ale později - teprve poté, co úplnou otáčku dokončí i druhý. Jedna otáčka druhého scrambleru představuje šest otáček prvního, tedy zašifrování 6 x 6 = 36 písmen. Jinými slovy, k dispozici je 36 různých nastavení scrambleru neboli 36 různých šifrových abeced. V případě úplné abecedy tvořené 26 písmeny jde o 26 x 26 = 676 různých šifrových abeced. Kombinováním scrambleru (jimž se také říká rotory) lze tedy sestavit šifrovací stroj, který neustále přechází od jedné šifrové abecedy k jiné. Operátor napíše písmeno a to se v závislosti na nastavení scrambleru zašifruje podle jedné ze stovek šifrových abeced. Pak se uspořádání scrambleru změní, takže další písmeno se šifruje podle jiné

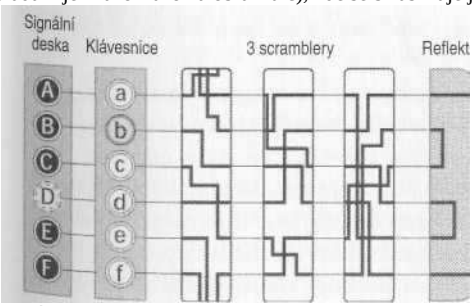
abecedy. To vše se navíc odehrává velmi rychle a přesně, díky automatickému pohybu scrambleru a rychlosti elektrického proudu.

Než si detailně vysvětlíme, jak se měl dle Scherbia jeho šifrovací stroj používat, je nezbytné popsat ještě dva další prvky Enigmy, zobrazené na obrázku 36. Za prvé, standardní Scherbiův šifrovací stroj byl pro zvýšení složitosti vybaven ještě třetím scramblerem - to znamená, že disponoval počtem 26 x 26 x 26 = 17 576 navzájem odlišných nastavení. Za druhé, Scherbius přidal ještě *reflektor*. Tato součást je podobná scrambleru - aspoň do té míry, že jde rovněž o gumový kotouč s vnitřním zapojením vodičů. Na rozdíl od scrambleru se však neotáčí, vodiče do něj vstupují touž stranou, jakou zas



Obrázek 35: Po přidání druhého scrambleru se schéma šifrování opakuje až po zadání 36 písmen.

Pak se oba scramblery vrátí do svých výchozích pozic. Pro zjednodušení jsou scramblery znázorněny jen dvourozměrně. Namísto rotace se zapojení posouvá o jednu pozici směrem dolů. Pokud na schématu část zapojení opustí scrambler nahoře nebo dole, pak se v dalším kroku objeví na jeho opačném konci. Na obrázku a) se b zašifruje jako D. Po zašifrování se první scrambler pootočí o jednu pozici a posune tímto pootočením o jednu pozici i druhý scrambler - to se stává jen tehdy, dokončil-li právě první scrambler celou otáčku. Nové uspořádání je znázorněno na obrázku b), kde se b zašifruje jako F. Po zašifrování se první scrambler pootočí o jednu pozici, ale druhý tentokrát zůstane nehybný. Nové uspořádání je znázorněno na obrázku c), kde se b zašifruje jako B.



Obrázek 36: Scherbiova konstrukce Enigmy obsahovala třetí scrambler a reflektor, jenž posílá signál zpět přes scramblery. Napíšeme-li v tomto konkrétním zapojení klávesnicí b, rozsvítí se žárovka D na signální desce, jež je zde zakreslena hned vedle klávesnice.vystupují. Je-li zařazen reflektor, funguje Enigma následujícím způsobem: operátor napíše písmeno, čímž se vyšle elektrický signál přes tři scramblery. Reflektor obdrží signál a pošle jej přes tyto tři scram-blery zpět, avšak *zcela,* odlišnou cestou. Například při zapojení dle obrázku 36 je tomu tak, že stisk klávesy s písmenem b vyšle signál přes tři scramblery do reflektoru, odkud se opět přes tři scramblery vrátí a rozsvítí žárovku s písmenem D. Ve skutečnosti signál neprochází znovu klávesnicí, jak by se mohlo zdát ze schématu, avšak je směřován rovnou do signální desky se žárovkami. Na první pohled vypadá reflektor jako zbytečný doplněk, neboť jeho charakter je statický a nezvyšuje již počet šifrových abeced. Smysl reflektoru a jeho výhody vyjdou najevo teprve tehdy, jestliže si popíšeme, jak se stroj konkrétně používal k šifrování a dešifrování zpráv.

Před zahájením šifrování musí operátor otáčením nastavit scramblery do předepsané výchozí pozice. Existuje 17 576 možných uspořádání, a proto 17 576 výchozích pozic. Počátečním nastavením scramblerů je dáno, jak se zpráva zašifruje. Enigmu si můžeme představit jako obecný šifrovací systém, v němž počáteční nastavení určuje konkrétní detaily šifrování - jinými slovy, počáteční nastavení odpovídá klíči. Vše je předepsáno kódovou knihou, která určuje konkrétní klíč pro každý den zvlášť. Kniha je k dispozici všem členům komunikační sítě. Distribuce kódových knih je pracná a časově náročná, ale protože potřebujeme jen jeden klíč denně, stačí každé čtyři týdny rozeslat sadu 28 klíčů. Kdyby se namísto toho používala jednorázová tabulková šifra, byl by potřeba pro každou zprávu nový klíč a distribuce klíčů by byla mnohem náročnější. Jakmile jsou scramblery nastaveny podle denního klíče, může odesilatel začít šifrovat. Napíše na klávesnici první písmeno zprávy, podívá se, která žárovka se rozsvítila, a zapíše si první písmeno šifrového textu. První scrambler se

automaticky pootočí. Operátor napíše další písmeno a tak dále. Jakmile tímto způsobem vytvoří celý šifrový text, předá jej radistovi k odvysílání.

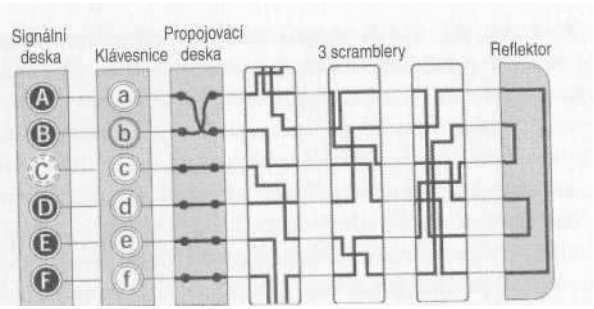
K dešifrování zprávy musí příjemce mít svou vlastní Enigmu a kódovou knihu. Nastaví stroj podle denního klíče, začne psát šifrový text písmeno po písmenu a na signální desce čte otevřený text. Jinými slovy, odesilatel píše otevřený text a získává šifrový, příjemce píše šifrový text a získává otevřený. Šifrování a dešifrování jsou vzájemně zrcadlové postupy. Tak snadno lze dešifrovat právě díky reflektoru. Z obrázku 36 je patrné, že když napíšeme b a sledujeme

vodiče, dostaneme D. Když naopak napíšeme d, dostaneme B. Stroj šifruje písmeno otevřeného textu na písmeno šifrového textu, a pokud se jeho nastavení nezmění, převede rovněž toto písmeno šifrového textu zpět na odpovídající písmeno textu otevřeného.

Je zřejmé, že klíč - včetně kódové knihy, která klíče obsahuje -nesmí padnout do rukou nepřítele. Může se docela dobře stát, že nepřítel ukořistí přístroj, ale bez znalosti výchozího nastavení nemůže zachycenou zprávu nijak snadno dešifrovat. Bez znalosti klíče mu nezbývá nic jiného než vyzkoušet všech 17 576 výchozích nastavení scramblerů. Kryptoanalytik by musel postupovat tak, že natočí rotory ukořistěné Enigmy do jednoho z možných nastavení, zkusí zadat úsek šifrového textu a sleduje, zda generovaný otevřený text dává smysl. Pokud ne, je třeba změnit výchozí nastavení a učinit nový pokus. Pokud by jeden takový pokus trval minutu a pracovalo by se nepřetržitě, pak by se všechna nastavení vyzkoušela asi za dva týdny. To je rozumná úroveň bezpečnosti; kdyby však nepřítel rozdělil práci mezi tucet lidí, mohl by mít výsledek téhož dne. Scherbi-us se proto rozhodl, že zlepší bezpečnost svého vynálezu tím, že zvýší množství počátečních nastavení a tedy počet klíčů.

Scherbius by mohl posílit bezpečnost zařazením dalších scramblerů (každý další by zvýšil počet klíčů šestadvacetkrát), ale tím by se také zvětšily rozměry stroje. Namísto toho zařadil dva jiné prvky. Jednak zkonstruoval scramblery jako vyměnitelné. První kotouč bylo tedy například možné zařadit na třetí pozici a třetí zas na první. Uspořádáním scramblerů je dáno schéma šifrování. Tři scramblery lze uspořádat šesti různými způsoby, takže toto zdokonalení zvyšuje počet klíčů - a počátečních nastavení - na šestinásobek.

Druhou novinkou bylo zařazení *propojovací desky* mezi klávesnici a první scrambler. Pomocí kabelů na propojovací desce lze vzájemně prohodit některá písmena, než vstoupí do prvního scramblerů. Když například spojí operátor kabelem zdířky a a b, pak b zadané z klávesnice sleduje přes scramblery cestu, kterou by jinak sledovalo a, a naopak. Enigma byla vybavena šesti kabely, takže její operátor mohl prohodit šest párů písmen, zatímco zbylých čtrnáct písmen zůstalo nepropojeno a neprohozeno. Prohození písmen je součástí nastavení stroje a je třeba jej specifikovat v kódové knize. Na obrázku 37 je znázorněno zapojení stroje s propojovací deskou. Schéma používá abecedu tvořenou jen šesti písmeny, úměrně tomu jsme prohodili jen jeden pár písmen, zde a a

b. 

Obrázek 37: Propojovací deska se nachází mezi klávesnicí a prvním scramblerem. Když do ní zapojíme kabel, prohodíme vzájemně jednu dvojici písmen; na tomto obrázku je prohozeno a a b. To má za následek, že b se šifruje pomocí cesty, kterou by se bez použití propojovací desky vydalo a, a naopak. U reálného stroje s abecedou tvořenou 26 písmeny měl operátor k dispozici kabely pro záměnu šesti párů písmen.

Součástí Scherbiovy konstrukce je ještě jeden prvek - tzv. *prstenec.* Zatím zde o něm nebyla řeč. Má sice určitý vliv na šifrování, je však nejméně důležitou částí stroje a pro účely tohoto výkladu jsem se rozhodl jej vynechat. (Čtenáři, kteří se chtějí poučit o přesné úloze prstence, se mohou obrátit k některé knize ze seznamu doporučené literatury, například *Seizing the Enigma* od Davida Kahna. V tomto seznamu najdete rovněž adresy dvou webových stránek obsahujících výborné emulátory Enigmy. Můžete si na nich vyzkoušet práci s počítačovou simulací tohoto šifrovacího

stroje.)

Teď, když známe všechny hlavní součásti Scherbiovy Enigmy, můžeme vypočítat množství klíčů, a to tak, že vynásobíme počet možných nastavení propojovací desky počtem možných nastavení scramblerů. Následující seznam ukazuje, jak jednotlivé nastavitelné prvky stroje ovlivňují množství klíčů.

Nastavení scramblerů. Každý ze 3 scramblerů může být nastaven do jedné z 26 výchozích pozic. Proto je k dispozici 26 x 26 x 26 nastavení: 17 576

Uspořádání scramblerů. Tři scramblery (označíme je jako 1, 2 a 3) lze uspořádat šesti způsoby: 123,132,213,231,312,321.

6

propojovací deska. Počet způsobů prohození šesti párů písmen z celkového počtu 26 je obrovský: 100 391 791 500

Celkem. Počet klíčuje dán součinem tří výše uvedených čísel: 17 576 x 6 x 100 391 791 500, což je přibližně

10 000 000 000 000 000.

Když se odesilatel a příjemce dohodnou na zapojení propojovací desky, na pořadí scramblerů a na počátečním nastavení každého z nich - čímž je dán klíč - mohou snadno šifrovat a dešifrovat zprávy. Nepřítel, který nezná klíč, by však musel vyzkoušet každý z 10 000 000 000 000 000 možných klíčů, pokud by chtěl rozluštit šifrový text. Vytrvalý kryptoanalytik, jenž by vyzkoušel jedno nastavení

za minutu, by potřeboval k prověření všech možností dobu delší než *známý* věk vesmíru. (Ve skutečnosti je počet možných klíčů ještě vyšší a čas potřebný k prolomení bezpečnosti Enigmy ještě delší - to je dáno tím, že jsme ignorovali účinek výše zmíněného prstence.)

Vzhledem k tomu, že zdaleka největší vliv na počet klíčů má propojovací deska, můžete si položit otázku, proč se Scherbius namáhal se scramblery. Propojovací deska sama o sobě by však mnoho šifrovací práce nezastala, neboť produkuje jen monoalfabetickousubstituční šifru, v níž se otevřená a šifrová abeceda liší ve dvanácti písmenech. Problém propojovací desky spočívá v tom, že během šifrování se její nastavení nemění, takže sama o sobě by produkovala šifrový text, jenž by se dal rozluštit pomocí frekvenční analýzy. Scramblery přispívají k celkovému počtu klíčů jen málo, ale jejich nastavení se neustále mění, takže výsledný šifrový text nelze frekvenční analýzou rozluštit. Díky kombinaci scramblerů s propojovací deskou Scherbius svůj stroj proti frekvenční analýze ochránil a zároveň jej vybavil nesmírným množstvím možných klíčů.

První patent získal Scherbius roku 1918. Šifrovací stroj měl podobu kompaktní skříňky o rozměrech pouhých 34 x 28 x 15 cm, vážil však solidních 12 kg. Na obrázku 39 je Enigma s otevřeným víkem, připravená k použití. Je na něm dobře patrná klávesnice, kterou se zapisuje otevřený text, a nad ní signální deska, kde se zobrazuje generovaný šifrový text. Pod klávesnicí je propojovací deska. Na ní lze vidět více než šest párů kabelů, protože tento konkrétní přístroj je mírnou modifikací standardního modelu, jejž jsme až dosud popisovali. Na obrázku 40 je Enigma, z níž byl odmontován kryt, aby bylo vidět více součástí přístroje, především pak tři scramblery.

Scherbius věřil, že Enigma je nezdolatelná a že tato její vlastnost vytvoří velkou poptávku po přístroji. Zkusil nabízet svůj šifrovací stroj jak obchodní komunitě, tak vojenským kruhům, přičemž pro každou z těchto skupin vytvořil speciální variantu přístroje. Nabízel například základní verzi pro obchodní použití, zatímco pro ministerstvo zahraničí vytvořil luxusní diplomatickou verzi s tiskárnou namísto signální desky. Cena jednoho přístroje činila asi 20 000 liber v dnešních cenách.

Vysoká cena přístroje však potenciální kupce odrazovala. Podnikatelé namítali, že si bezpečnost komunikací za tuto cenu nemohou dovolit, Scherbius naopak věřil, že si nemohou dovolit obejít se bez ní. Upozorňoval, že klíčová informace vyzrazená obchodnímu soupeři může stát celé jmění, avšak jen málo podnikatelů mu naslouchalo. Německé vojenské kruhy se do nákupu nového šifrovacího stroje také nehrnuly, neboť si nebyly vědomy toho, jakou Škodu jim během první světové války způsobily nedokonalé šifry. Němci například věřili tomu, že Zimmermannův telegram byl ukraden v Mexiku americkými špiony, takže obviňovali mexické úřady. Tou dobou stále ještě nevěděli, že telegram byl ve skutečnosti zachycen a dešifrován Brity a že krach Zimmermannova plánu byl ve skutečnosti pro-nrou německé kryptografie.

Scherbius nebyl se svou narůstající frustrací sám. Další tři vynálezci ve třech různých zemích nezávisle na sobě a téměř současně

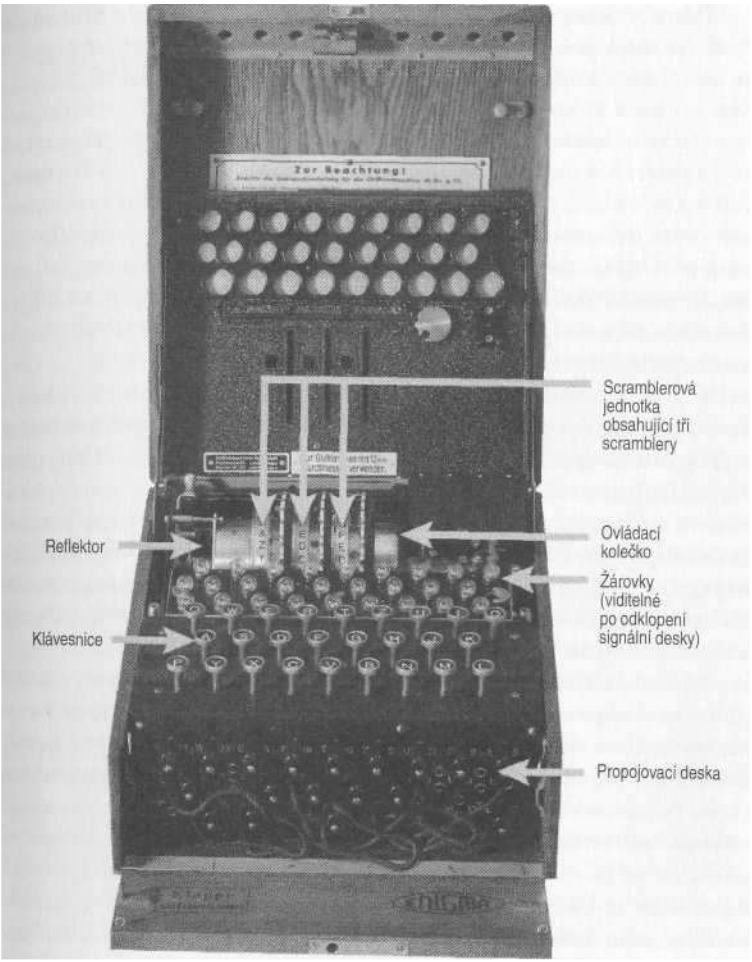
Přišli na myšlenku postavit šifrovací stroj s otočnými scramblery
V Nizozemsku získal roku 1919 Alexander Koch patent č. 10 700 ale
svůj nápad na šifrovací stroj s rotory se mu nepodařilo proměnit
v obchodní úspěch a roku 1927 patentová práva prodal. Arvid

Damm ve Švédsku získal podobný patent, ale do své smrti v roce1927 také nedokázal nalézt odbyt. Americký vynálezce Edward He-bern hluboce věřil ve svůj vynález, tzv. Bezdrátovou sfingu, jeho prohra však byla ze všech největší.

V polovině 20. let 20. století začal Hebern stavět továrnu nákladem 380 000 dolarů. K jeho smůle se však právě v tomto období začala nálada americké společnosti měnit od paranoidního podezírání směrem k otevřenosti. V předchozím desetiletí, jako dozvuk první světové války, ustavila vláda americkou černou komnatu, vysoce efektivní šifrové oddělení s týmem dvaceti kryptoanalytiků, v jejichž čele stál bohémský a skvělý Herbert Yardley. Ten později napsal, že „černá komnata, zamčená, ukrytá a střežená, vidí a slyší všechno. Utajení může být sebelepší, okna sebedokonaleji zastřená, přesto její pronikavý zrak dohlédne do tajných konferenčních sálů ve Washingtonu, v Tokiu, Londýně, Paříži, Ženevě či v Římě. Její jemný sluch zachytí i sebetišší zašeptání v hlavních městech celého svě-ta". Americká černá komnata rozluštila během desetiletí své existence 45 000 kryptogramů, avšak v době, kdy Hebern stavěl továrnu, se stal prezidentem Herbert Hoover, který se pokusil zahájit novou éru mezinárodních vztahů. Černou komnatu rozpustil a jeho ministr zahraničí Henry Stimson prohlásil, že „gentleman nečte cizí dopisy". Stát, který věří, že není správné číst cizí dopisy, časem začne věřit i tomu, že jeho korespondenci také nikdo nečte, takže nevidí důvod pro pořízení kvalitních šifrovacích strojů. Hebern prodal jen dvanáct přístrojů, celkem asi za 1 200 dolarů, a roku 1926 byl nespokojenými akcionáři pohnán k soudu a podle kalifornského obchodního práva shledán vinným.

Naproti tomu německé vojenské kruhy zažily - naštěstí pro Scher-bia - šok, v jehož důsledku docenily hodnotu Enigmy, a to díky dvěma britským dokumentům. Prvním z nich byla *Světová krize* Winsto-na Churchilla, publikovaná roku 1923, v níž se dramaticky popisuje, jak Britové získali cenný německý kryptografický materiál:

„Počátkem září 1914 ztroskotal v Baltském moři německý lehký křižník *Magdeburg*. O několik hodin později vylovili Rusové tělo utonulého německého poddůstojníka, který ke svým prsům, rukama ztuhlýma smrtelnou křečí, stále ještě tiskl šifrovací a signální knihy německého námořnictva spolu s mapami Severního moře a Helgolandského zálivu s detailně vyznačenými čtvercovými souřadnicemi. 6. září mne navštívil ruský námořní atašé. Obdržel depeši z Petrohradu, v níž se tato událost



Obrázek 40: Enigma s otevřeným vnitřním víkem, takže jsou vidět tři scramblery.

popisovala a kde se také uvádělo, že díky získaným dokumentům dokázala ruská admiralita dešifrovat přinejmenším části německé námořní komunikace. Rusové byli toho názoru, že Británie jako přední námořní velmoc by měla těmito mapami a dokumenty disponovat. Pokud vyšleme loď, ruští důstojníci nám je předají."

/Takto získaný materiál umožnil kryptoanalytikům z Kanceláře č. 40 rutinně dešifrovat německé depeše. Téměř o deset let později se tak Němci konečně dověděli o selhání své komunikační bezpečnosti. Téhož roku (1923) publikovalo britské královské námořnictvo oficiální historii první světové války, kde se znovu připomínalo, že odposlech a dešifrování německé komunikace byly pro Dohodu velkou výhodou. Tyto úspěchy britské rozvědky představovaly zároveň ostré odsouzení činnosti těch, kteří odpovídali v Německu za utajení. Oni sami museli

připustit a napsat do vlastní zprávy, že „německé námořní velení, jehož rádiovou komunikaci Angličané odposlouchávali a dešifrovali, hrálo proti britskému velení takříkajíc s odkrytými kartami".

Němci prozkoumali možnosti, jak se napříště vyhnout takovému kryptografickému fiasku, a došli k závěru, že nejlepším řešením je Enigma. Scherbius zahájil velkovýrobu roku 1925, již o rok později se Enigma *začala,* používat v armádě a nakonec i ve státní správě a ve státem řízených organizacích, jako například na železnici. Tyto Enigmy se lišily od několika málo přístrojů, jež Scherbius dříve prodal komerčnímu sektoru, protože vnitřní zapojení scramble-rů bylo jiné. Uživatelé komerčních přístrojů tudíž neměli přístup k vládní a vojenské komunikaci.

Během dalších dvaceti let koupila německá armáda přes 30 000 přístrojů Enigma. Scherbiův vynález jí poskytl nejdokonalejší šifrovací systém na světě, takže na začátku druhé světové války disponovali Němci naprosto bezprecedentní úrovní bezpečnosti komunikací. Po nějakou dobu se *zdálo,* že Enigma sehraje důležitou roli ve vítězství nacistů, nakonec se však významně podílela na Hitlerově pádu. Scherbius nežil dost dlouho, aby na vlastní oči viděl úspěch a porážku svého šifrovacího systému. Roku 1929 se mu vymklo z rukou jeho koňské spřežení, narazil s vozem do zdi a 13. května zemřel na vnitřní zranění.

4

Boj s Enigmou

Po první světové válce pokračovali britští kryptoanalytici v Kanceláři č. 40 v luštění německých komunikací. Roku 1926 *začali* zachycovat depeše, jež je zcela zmátly. To *začala,* pracovat Enigma. Jak počet těchto přístrojů rostl, schopnost Kanceláře č. 40 získávat informace rapidně poklesla. Američané a Francouzi se také snažili bojovat s novou šifrou, ale jejich snaha byla marná, a tak se brzy vzdali naděje. Německo nyní mělo nejbezpečnější komunikace na světě.

Rychlost, s níž se spojenečtí kryptoanalytici vzdali naděje na prolomení šifry Enigmy, ostře kontrastovala s jejich vytrvalostí v době první světové války. Tváří v tvář představě porážky pracovali tehdy dnem i nocí, aby německé šifry rozluštili. Zdá se, že obavy byly hlavní hnací silou jejich práce a že tíseň patří ke klíčovým faktorům úspěšné kryptoanalýzy. Stejně tak poháněly obavy a tíseň francouzské kryptoanalytiky, když na konci 19. století čelili vzrůstající moci Německa. Po první světové válce se však Spojenci nebáli nikoho. Německo bylo porážkou ochromeno, Spojenci byli v dominantní pozici, a proto jejich kryptoanalytické nasazení ochablo. Na straně Spojenců poklesl počet kryptoanalytiků i jejich kvalita.

Existoval však jeden stát, jenž si nemohl dovolit odpočívat na vavřínech: Polsko. Po první světové válce obnovili Poláci svou nezávislost, obávali se však všeho, co ji mohlo ohrozit. Východně od nich se rozkládalo Rusko, dychtivé šířit svůj komunismus, na západ od Polska leželo Německo, odhodlané získat nazpět území, jež muselo Polsku po válce postoupit. Země vtisknutá mezi dva nepřátele nutně potřebovala rozvědku a její informace. Poláci založili nové šifrové oddělení,

které nazvali Biuro Szyfrow. Jestliže někdy platí, že nutnost je matkou invence, pak je rovněž možné, že ohrožení je matkou kryptoanalýzy. Příkladem dovednosti Biura Szyfrow je úspěch tohoto oddělení během rusko-polské války v letech 1919-1920. Jen v samotném srpnu 1920, když sovětská vojska stála před Varšavou, dešifrovalo Biuro 400 nepřátelských depeší. Stejně úspěšně mo-nitorovali Poláci i německé komunikace - až do roku 1926, kdy také narazili na Enigmu.

Za dešifrování německých komunikací odpovídal kapitán Mak-symilian Ciezki, oddaný vlastenec původem z města Szamotuly, centra polského nacionalismu. Ciezki měl k dispozici komerční verzi Enigmy, z níž byly patrné všechny principy Scherbiova vynálezu. Komerční verze se však bohužel od vojenské varianty výrazně lišila co do vnitřního zapojení scramblerů. Bez znalosti zapojení vojenské verze neměl Ciezki naději dešifrovat zprávy německé armády. Byl z toho tak zoufalý, že dokonce najal jasnovidce v urputné snaze vydobýt ze zašifrovaných zpráv nějaký význam. Není žádným překvapením, že to nepomohlo -jasnovidec nedosáhl takového průlomu, jaký Biuro Szyfrow potřebovalo. S prvními kroky směřujícími k prolomení Enigmy překvapivě pomohl neloajální Němec Hans-Thilo Schmidt.

Narodil se v Berlíně roku 1888 jako druhý syn váženého profesora a jeho aristokratické manželky. Schmidt se rozhodl pro armádní kariéru a bojoval v první světové válce. Nebyl však shledán dost užitečným, aby mohl v armádě zůstat i po drastickém snížení stavů, k němuž došlo v důsledku versaillské smlouvy. Pokusil se tedy prosadit se jako podnikatel, ale svou továrnu na mýdlo musel zavřít kvůli poválečné depresi a hyperinflaci. Schmidt se ocitl i se svou rodinou bez prostředků.

Zatímco byl Hans-Thilo Schmidt takto pokořen, jeho starší bratr Rudolf slavil úspěchy. Rudolf rovněž bojoval ve válce a zůstal v armádě i po jejím konci. Ve 20. letech prošel sérií povýšení a nakonec se stal náčelníkem štábu spojovacích jednotek. Odpovídal za bezpečnost a utajení komunikací a byl to právě on, kdo schválil nasazení přístrojů Enigma.

Po krachu svého podnikání musel Hans-Thilo požádat bratra o pomoc. Rudolf mu opatřil práci v berlínské Chiffrierstelle - úřadu, jenž odpovídal za správu německých šifrovaných komunikací. Šlo o velitelské centrum sítě přístrojů Enigma, o přísně tajné zařízení pracující s vysoce citlivými informacemi. Když se Hans-Thilo přestěhoval do Berlína, zanechal svou rodinu v Bavorsku, kde byly nižší životní náklady. Žil sám v nákladném Berlíně, zbídačelý a osamělý, plný závisti vůči úspěšnému bratrovi a zášti k zemi, která odmítla jeho služby. Výsledek byl nevyhnutelný. Prodat tajné informace o Enigmě cizí zemi znamenalo vydělat peníze a zároveň se

pomstít, poškodit bezpečnost Německa a podlomit organizaci řízenou vlastním bratrem.

8. listopadu 1931 se Schmidt dostavil do hotelu Grand v belgickém Verviers na schůzku s francouzským tajným agentem, jehož krycí jméno znělo Rex. Za odměnu 10 000 marek (asi 20 000 liber v dnešních cenách) umožnil Schmidt Rexovi ofotografovat dva dokumenty: *Gebrauchsanweisungfiir die Cbiffriermaschine Enigma* a *Schlús-selanleitung fiir die Chiffriermascbine*

Enigma. Šlo o návody k použití Enigmy, a přestože neobsahovaly žádné výslovné údaje o vnitřním zapojení scramblerů, dalo se z jejich informací toto zapojení odvodit.

Kvůli Schmidtově zradě mohli nyní Spojenci sestrojit přesnou repliku německé vojenské Enigmy. To však k dešifrování zpráv nestačilo. Síla šifry nespočívá v utajení přístroje, ale v utajení jeho počátečního nastavení. Chce-li kryptoanalytik dešifrovat zachycenou zprávu, musí nejprve zjistit, který z milionů miliard klíčů použít. Německé memorandum to shrnulo slovy: „Při posuzování bezpečnosti šifrovacího systému vycházíme z předpokladu, že nepřítel má přístroj k dispozici."

Francouzská tajná služba byla v dobré výchozí pozici, protože mela Schmidta jako informátora a disponovala dokumenty, z nichž vyplývalo vnitřní zapojení vojenské Enigmy. Francouzští kryptoana-lytici však nebyli na patřičné úrovni. Zdálo se, že nechtějí a nedove-dou využít nově získaných poznatků. Po první světové válce trpěli přehnanou sebedůvěrou a ztrátou motivace. Francouzské Bureau du chiffre se dokonce ani nenamáhalo postavit repliku vojenské Enigmy, neboť bylo přesvědčeno, že další krok, tedy nalezení klíče nezbytného k dešifrování konkrétní zprávy, je tak jako tak nemožný.

O deset let dříve podepsali Francouzi smlouvu o vojenské spolupráci s Polskem. Poláci vyjádřili zájem o vše, co souviselo s Eni-gmou, takže v souladu s deset let starou smlouvou Francouzi prostě předali fotokopie Schmidtových dokumentů svým spojencům a přehodili beznadějný úkol rozluštit Enigmu na Biuro Szyfrow. Jeho specialisté pochopili, že dokumenty představují jen začátek, na rozdíl od Francouzů je však poháněl strach z německé invaze. Poláci přesvědčili sami sebe, že k nalezení klíče pro Enigmu určitě nějaká cesta vede. Byli si jisti, že ji najdou, věnují-li úkolu dost úsilí, vynalézavosti a duševních kapacit.

Ze Schmidtových dokumentů vyplývalo nejen vnitřní zapojení scramblerů, ale listiny obsahovaly také detailní popis, jak vypadají německé kódové knihy. Operátoři Enigmy obdrželi každý měsíc novou kódovou knihu, která udávala klíč pro konkrétní den. Pro první den měsíce mohla kódová kniha specifikovat například následující *denníklíč:*

(1) *Nastavení propojovací desky:* A/L-P/R-T/D-B/W-K/F-O/Y
(2) *Uspořádání scramblerů:* 2-3-1
(3) *Orientace scramblerů:* Q -C -W

Uspořádání a orientace scramblerů se dohromady nazývají nastavení scramblerů. Aby operátor Enigmy nastavil tento denní klíč, postupoval tímto způsobem:

(1) *Nastavení propojovací desky:* Prohoďte písmena A a L tím, že je spojíte na propojovací desce kabelem, pak stejným způsobem prohoďte P a R,T a D, B a W, K a F, 0 a Y.

(2) *Uspořádání scramblerů:* Umístěte druhý scrambler do první pozice ve stroji, třetí scrambler do druhé pozice a konečně první scrambler do třetí pozice.

(3) *Orientace scramblerů:* Na vnějším okraji každého scramblerů je vyryta abeceda, což vám umožní nastavit požadovanou orientaci scramblerů. V tomto případě otáčejte prvním scramblerem tak dlouho, až je orientován písmenem Q nahoru, pak otáčejte druhým, až je nahoře písmeno C, a nakonec třetím

scramblerem, až je nahoře W.

Jednou z metod šifrového provozu je šifrovat všechny zprávy odeslané daného dne příslušným denním klíčem. To znamená, že po celý den nastavují na začátku každé zprávy všichni operátoři svou Enigmu podle téhož klíče. Kdykoli se pak má odeslat zpráva, je třeba ji napřed přepsat do Enigmy, přitom zaznamenat šifrový text a ten nakonec odevzdat radistovi k odvysílání. Radista na straně příjemce zaznamená příchozí zprávu, předá ji operátorovi Enigmy, který ji zapíše do přístroje nastaveného na stejný denní klíč a přečte původní zprávu.

Takový postup je přiměřeně bezpečný, oslabuje jej však to, že se denně šifrují stovky zpráv týmž denním klíčem. Obecně lze říci, že pokud se pro větší množství materiálu použije stejný klíč, usnadní se tím práce nepřátelským kryptoanalytikům. Když se vrátíme například k monoalfabetickým šifrám, je zřejmé, že z několika stran textu lze sestavit frekvenční analýzu snáze než z pouhých několika vět.

Němci proto jako chytré dodatečné opatření zavedli pravidlo, že denním klíčem se šifruje takzvaný *klíč zprávy.* Ten má stejné zapojení propojovací desky a stejné uspořádání scramblerů jako denní klíč, liší se však od něj orientací scramblerů. Nová orientace scramblerů není v kódové knize, takže je nezbytné, aby ji odesilatel zaslal příjemci bezpečnou cestou. Němci proto postupovali následovně: odesilatel nejprve nastaví svůj přístroj podle denního klíče, jehož součástí je orientace scramblerů - řekněme QCW. Poté náhodně vybere novou orientaci scramblerů pro denní klíč, řekněme PGH. Poté zašifruje PGH podle denního klíče. Klíč zprávy se do Enigmy zapíše dvakrát, aby se vyloučil překlep či jiná chyba. Odesilatel tedy zašifruje PGHPGH například jako KIVBJE. Povšimněte si, že PGH se pokaždé zašifruje jinak (jednou jako KIV, podruhé jako BJE), protože scramblery se otáčejí a mění tím režim šifrování. Odesilatel pak změní nastavení scramblerů na PG H a zašifruje vlastní zprávu podle tohoto klíče zprávy. Na straně příjemce je Enigma nastavena na denní klíč, tedy QCW. Příjemce zapíše prvních šest písmen zprávy a čte "GHPGH. Nastaví tedy své scramblery na PGH a dešifruje vlastní text zprávy.

V podstatě jde o to, že se odesilatel a příjemce dohodnou na hlavním klíči, který však neužívají pro šifrování zpráv, ale jen pro šif-rování unikátního klíče každé zprávy. Kdyby Němci tento systém nepoužívali, pak by se celý denní provoz - patrně tisíce zpráv obsahujících miliony písmen - šifrovaly týmž klíčem. Pokud se však denní klíč používá jen k přenosu klíčů zpráv, pak se jím šifruje jen malé množství textu. Při 1 000 zprávách denně to je pouhých 6 000 písmen. A protože klíč zprávy se vybírá náhodně a šifruje se jím jen jedna zpráva, používá se také k zašifrování malého množství textu -zpravidla několika stovek znaků.

Na první pohled vypadá takový systém neproniknutelně, ale polští kryptoanalytici se nedali zastrašit. Byli připraveni prozkoumat každou cestičku, aby našli slabinu Enigmy a nedostatky systému, který *využívá,* denní klíč spolu s klíčem zprávy. V čele boje s Enig-mou stáli kryptoanalytici nového typu. Po staletí se mělo za to, že nejlepšími kryptoanalytiky jsou odborníci na strukturu jazyka, Enigma však přinutila Poláky, aby přehodnotili svou personální politiku. Jelikož se jednalo o mechanickou šifru, Biuro Szyfrow došlo k názoru, že lepší šanci by mohly mít vědecky orientované mozky. Biuro uspořádalo kurs kryptografie, na

nějž pozvalo dvacet matematiků, kteří napřed museli odpřísáhnout mlčenlivost. Všichni byli z poznaňské univerzity. Přestože to nebyla nejuznávanější akademická instituce v zemi, měla jinou výhodu. Ležela na západě země, v oblasti, jež do roku 1918 patřila Německu. Všichni zúčastnění matematici hovořili plynně německy.

Tři kursisté z dvaceti prokázali talent luštit šifry a Biuro je zaměstnalo. Nejnadanějším matematikem byl Marian Rejewski, plachý třiadvacetiletý mladík s brýlemi, který studoval statistiku a chtěl pracovat v pojišťovnictví. Na univerzitě měl dobré výsledky, ale teprve Biuro Szyfrow se pro něj stalo tím pravým působištěm. Během zácviku nejprve rozluštil řadu tradičních šifer a teprve poté se zaměřil na nezměrnou výzvu, již představovala Enigma. Pracoval *zcela*, sám a veškerou svou energii soustředil na záludnosti Scherbiova stroje. Pokoušel se analyzovat z matematického hlediska všechny aspekty činnosti Enigmy, testovat účinky scramblerů a propojovací desky. Jeho práce však kromě logiky vyžadovala také inspiraci, jak je to nezbytné v celé matematice. Jiný válečný kryptoanalytik to vyjádřil slovy, že pro tvořivé luštění šifer je třeba „denně obcovat se zlými duchy, aby člověk dokázal podat výkon v duchovním jiu-jitsu".

Rejewského strategie útoku na Enigmu vycházela ze skutečnosti, že opakování je nepřítelem bezpečnosti: opakování vede k zákonitostem, jež pak mohou kryptoanalytici luštit. Nejnápadnějším pakováním byl v případě Enigmy klíč zprávy, zašifrovaný vždy dvakrát na začátku každé zprávy. Pokud operátor zvolil klíč U LJ, pak jej musel zašifrovat dvakrát, U L J U L J převedl na PEFNWZ a tuto sekvenci odeslal na počátku vlastní zprávy. Němci trvali na opakování, aby se vyhnuli chybám způsobeným překlepem nebo rádiovou interferencí. Nepředvídali však, že tak mohou ohrozit bezpečnost komunikace.

Rejewski každý den dostal nový balík zachycených zpráv. Všechny začínaly šesti písmeny opakovaného třípísmenného klíče zprávy, všechny byly zašifrovány podle téhož dohodnutého denního klíče. Tak například mohl obdržet čtyři zprávy, které začínaly následujícími zašifrovanými klíči zprávy:

	1.	2.	3.	4.	5.	6
První zpráva	L	O	K	R	G	M
Druhá zpráva	M	V	T	X	Z	E
Třetí zpráva	J	K	T	M	P	E
Čtvrtá zpráva	D	V	Y	P	Z	X

V každé z těchto zpráv vzniklo první a čtvrté písmeno zašifrováním téhož písmene, a to prvního písmene klíče zprávy. Také druhé a páté písmeno jsou zašifrováním téhož písmene, a to druhého písmene klíče zprávy. I třetí a šesté písmeno jsou zašifrováním téhož písmene, a to třetího písmene klíče zprávy. Například v první zprávě jsou La R zašifrováním téhož písmene, prvního písmene klíče zprávy. Stejné písmeno je zašifrováno různě, poprvé jako L a potom jako R, z toho důvodu, že se mezi dvěma šifrováními první scrambler Enigmy posunul o tři kroky a změnil tak celkový způsob šifrování.

Skutečnost, že L a R jsou zašifrováním téhož písmene, umožnila Rejewskému vyvodit drobná omezení týkající se počátečního nastavení přístroje. Počáteční neznámé nastavení scramblerů zašifrovalo první písmeno denního klíče, který je

také neznámý, jako L. Další nastavení scramblerů, tři kroky od původního nastavení, které je stále neznámé, zašifrovalo týž znak jako R.

Takové vymezení se může zdát mlhavé, protože je plné neznámých, ale přinejmenším to dokazuje, že písmena L a R jsou těsně spojena původním nastavením přístroje Enigma, denním klíčem. ^ každou další zachycenou novou zprávou lze identifikovat další vztahy mezi prvním a čtvrtým písmenem opakovaného klíče zprávy. Všechny tyto vztahy jsou odrazem počátečního nastavení Enigmy.Například druhá zpráva (viz výše) nám říká, že písmena M a X jsou v určitém vztahu, třetí řádek napovídá, že stejná závislost existuje mezi J a M, a čtvrtá zpráva ukazuje, že totéž existuje i mezi D a P. Re-jewski shrnul tyto vztahy tak, že je uspořádal do tabulky. Pro čtyři zprávy, která zatím máme, odráží tabulka vztahy mezi (L, R), (M, X), (J,M) a(D, P):

1. písmeno ABCDEFGHIJKLMNOPQRSTUVWXYZ 4. písmeno P M R X

Když dostal Rejewski během jediného dne dostatek *zpráv,* mohl sestavit úplnou abecedu vztahů. Kompletní množinu závislostí představuje následující tabulka:

1. písmeno ABCDEFGHIJKLMNOPQRSTUVWXYZ 4. písmeno FQHPLWOGBMVRXUYCZITNJEASDK

Rejewski neznal denní klíč ani neměl představu, jaký klíč zprávy operátor zvolil, ale věděl, že výsledkem je tato tabulka vztahů. Kdyby byl denní klíč jiný, potom by také tabulka vztahů byla naprosto jiná. Následovala otázka, zda existuje nějaký způsob, jak z této tabulky stanovit denní klíč. Rejewski začal hledat v tabulce zákonitosti - struktury, které mohly denní klíč naznačit. Nakonec se zaměřil na jeden konkrétní typ takové zákonitosti, v níž figurovaly řetězce písmen. Například ve výše uvedené tabulce je A v horní řadě spojeno s F v dolní řadě. Když nyní vyhledáme F v horní řadě, ukáže se, že F je spojeno s W. Podíváme se na W v horní řadě. Zjistíme, že W je spojeno s A, u kterého jsme začali. Řetězec se uzavřel.

Se zbývajícími písmeny abecedy mohl Rejewski vytvořit více řetězců. Sestavil jejich strukturu a v každém řetězci zaznamenal počet spojení:

A → F → W → A	3 spojení
B → Q → Z → K → V → E → L → R → I → B	9 spojení
C → H → G → O → Y → D → P → C	7 spojení
J → M → X → S → T → N → U → J	7 spojení

Dosud jsme pouze uvažovali o spojeních mezi prvním a čtvrtým písmenem šestipísmenného opakovaného klíče. Rejewski však pracoval i se vztahy mezi druhým a pátým písmenem a třetím a šestým písmenem. Vždy se snažil sestavit strukturu řetězců včetně počtu spojení.

Rejewski si povšiml, že se řetězce každý den mění. Někdy sestavil hodně krátkých řetězců, jindy pouze pár dlouhých. A samozřejmě se také měnila uvnitř řetězců jednotlivá písmena. Charakter řetězců byl jasně dán nastavením denního klíče, který vznikal důsledkem nastavení propojovací desky, uspořádání scramblerů a jejich orientace. Otázkou zůstávalo, jak z těchto řetězců určit denní

klíč. Který z 10 000 000 000 000 000 možných denních klíčuje spojen s konkrétní strukturou řetězce? Počet možností byl jednoduše příliš velký.

V tomto bodě pronikl Rejewski do podstaty problému. Přestože na podobu řetězců mělo vliv jak nastavení propojovací desky, tak scramblerů, jejich působení mohlo být do určité míry rozdílné. Zvláště jedna vlastnost řetězce byla zcela závislá na nastavení scramblerů, avšak neměla nic společného s nastavením propojovací desky: byla to *délka řetězce*. Ukážeme si to na příkladu, v němž denní klíč vyžaduje, aby písmena S a G byla vzájemně prohozena jako součást nastavení propojovací desky. Pokud tuto součást denního klíče změníme tím, že odstraníme kabel, který spojuje S a G, a použijeme jej místo toho k výměně například T a K, potom se řetězce změní následujícím způsobem:

A → F → W → A	3 spojení
B → Q → Z → T → V → E → L → R → I → B	9 spojení
C → H → S → O → Y → D → P → C	7 spojení
J → M → X → G → K → N → U → J	7 spojení

Některá písmena v řetězci se změnila, ale počet spojení v každém řetězci rozhodně zůstal konstantní. Rejewski identifikoval tu vlastnost řetězce, která byla výhradně důsledkem nastavení scramblerů.

Celkový počet nastavení scramblerů je dán jako počet uspořádání (6) vynásobený počtem možných orientací (17 576), což dává číslo 105 456. Takže místo toho, aby se trápil, který z 10 000 000 000 000 000 denních klíčů odpovídá určité sadě řetězců, mohl se Rejewski soustředit na mnohem jednodušší problém: Které z 105 456 nastavení scramblerů odpovídá pozorovanému počtu spojení v rámci sady řetězců? Toto číslo je stále velké, ale zhruba sto miliardkrát menší než celkový počet možných denních klíčů. Jinými slovy, náročnost úkolu poklesla o řád sta miliard. Takový úkol je již pravděpodobně řešitelný.

Rejewski postupoval následujícím způsobem: díky špionáži Hans-Thilo Schmidta měl k dispozici repliku přístroje Enigma. Jehotým se dal do namáhavé práce: prozkoušel všech 105 456 nastavení scramblerů a katalogizoval délky řetězců, jež byly každým nastavením generovány. Dokončit katalog zabralo celý rok, ale jakmile Biu-ro nashromáždilo všechna data, Rejewski mohl konečně začít dešifrovat Enigmu.

Každý den se podíval na zašifrované klíče zprávy, tedy na prvních šest písmen každé zachycené zprávy, a tuto informaci použil k vybudování své tabulky vztahů. To mu umožnilo najít jednotlivé řetězce a v každém z nich určit počet spojení. Například analýza prvního a čtvrtého písmene by mohla vyústit ve čtyři řetězce se 3,9,7 a 7 spojeními. Analýza druhého a pátého písmene by mohla také vést ke čtyřem řetězcům - se 2, 3, 9 a 12 spojeními. Analýza třetího a šestého písmene by mohla vést k pěti řetězcům s 5, 5, 5, 3 a 8 spojeními. Rejewski stále ještě neměl ponětí o denním klíči, ale věděl, že z něj vyplývají tři sady řetězců s následujícím počtem řetězců a spojení:

4 řetězce z 1. a 4. písmene se	3, 9, 7 a 7 spojeními
4 řetězce z 2. a 5. písmene se	2, 3, 9 a 12 spojeními

5 řetězců z 3. a 6. písmene s 5, 5, 5, 3 a 8 spojeními

Rejewski nyní mohl nahlédnout do svého katalogu, který obsahoval každé nastavení scramblerů indexované podle druhu generovaných řetězců. Když našel položku v katalogu, jež obsahovala správný počet řetězců s odpovídajícím počtem spojení, znal nastavení scramblerů pro daný denní klíč. Řetězce byly jakoby otisky prstů - důkaz, který odhalil původní uspořádání a orientaci scramblerů. Rejewski pracoval jako detektiv, který na místě zločinu sejme otisk prstu a potom použije databázi, aby našel odpovídajícího podezřelého.

Když Rejewski identifikoval scramblerovou část denního klíče, musel ještě odhalit nastavení propojovací desky. Ačkoli zde bylo kolem sta miliard možností, šlo o poměrně jednoduchý úkol. Rejewski začal nastavením scramblerů ve své replice Enigmy podle zjištěné scramblerové části denního klíče. Potom odstranil všechny kabely z propojovací desky, aby neměla na šifrování žádný vliv. Nakonec vzal část zachycené zprávy a naťukal ji do přístroje. Výsledkem byla převážně jakási hatmatilka, protože správná kabeláž propojovací desky byla zatím neznámá. Poměrně často se však objevily mlhavě rozeznatelné věty jako třeba plijedtedobelrina - pravděpodobně to mohlo znamenat „přijeďte do Berlína". Pokud byl tento předpoklad

správný, potom to znamenalo, že písmena R a L jsou spojena a vyměněna kabely propojovací desky, zatímco A, I, E, B a N nikoli. Analýzou dalších vět pak bylo možné určit další písmena, jež je třeba vzájemně prohodit pomocí propojovací desky. Když se takto podařilo určit nastavení propojovací desky při známém nastavení scramblerů, měl Rejewski k dispozici úplný denní klíč a mohl tedy rozšifrovat jakoukoliv zprávu zaslanou toho dne.

Rejewski si velmi zjednodušil úkol nalézt denní klíč tím, že oddělil problém nastavení scramblerů od problému nastavení propojovací desky. Každý z nich byl sám o sobě řešitelný. Původně jsme odhadli, že prověřit každý možný klíč k Enigmě by zabralo delší dobu, než je celkové stáří vesmíru. Rejewski však strávil sestavováním svého katalogu délek řetězců pouhý rok. Pak již mohl najít denní klíč téhož dne, kdy jej nepřítel začal používat. A jakmile měl denní klíč, disponoval stejnou informací jako zamýšlený příjemce, a tak mohl zprávu snadno dešifrovat.

Po Rejewského průlomu se německá komunikace stala průhlednou. Polsko sice ve válce s Německem nebylo, ale přesto mu hrozila invaze, takže úleva po přemožení Enigmy byla obrovská. Pokud niohli Poláci zjistit, co měli němečtí generálové za lubem, pak měli naději, že se dokážou ubránit. Osud polského národa závisel na Re-jewském a on svou zemi nezklamal. Rejewského útok na Enigmu je J[e]dním ze skutečně skvělých výkonů krypto analýzy. Bohužel jsemmusel jeho práci shrnout na několika stránkách, proto jsem vynechal některé technické detaily a všechny slepé uličky. Enigma je komplikovaný šifrovací přístroj a její rozlomení vyžadovalo obrovský intelektuální výkon. Toto zjednodušení by vás nemělo svést k mylným závěrům a podcenit to, co Rejewski dokázal.

Polský úspěch v prolomení Enigmy byl dán třemi faktory: strachem, matematikou a špionáží. Beze strachu z invaze by Poláky odradila zdánlivá

nezranitelnost šifry. Bez matematiky by Rejewski nebyl schopen analyzovat řetězce. A bez Schmidta, kódovým jménem „Asche", a jeho dokumentů by nebylo známo vnitřní zapojení scramblerů a kryptoanalýza by nemohla ani začít. Rejewski se nezdráhal vyjádřit svůj dík Schmidtovi: Jeho dokumenty byly jako nebeská mana, všechny dveře byly rázem otevřeny."

Poláci úspěšné používali Rejewského techniku po několik let. Když Hermann Góring navštívil v roce 1934 Varšavu, neměl ani ponětí, že jeho komunikace je zachycována a dešifrována. Když on a další němečtí hodnostáři pokládali věnec k hrobu Neznámého vojína v blízkosti kanceláří Biura Szyfrow, Rejewski se na ně mohl dívat z okna a spokojeně myslet na to, že dovede číst jejich nejtajnější komunikaci.

Dokonce i když Němci učinili malou změnu ve způsobu vysílání zpráv, Rejewski situaci zvládl. Jeho starý katalog délek řetězců byl po této změně k ničemu. Než by jej dával znovu dohromady, sestavil jeho mechanickou verzi, která automaticky vyhledávala správná nastavení scramblerů. Rejewského vynález byl adaptací Enigmy, která byla schopná rychle prověřit každé ze 17 576 nastavení, dokud nenarazila na to správné. Protože existovalo šest možných uspořádání scramblerů, bylo nutné mít šest Rejewského přístrojů pracujících paralelně. Každý z nich představoval jedno z šesti možných uspořádání. Dohromady tvořily jednotku, která byla asi metr vysoká a dovedla najít denní klíč zhruba během dvou hodin. Říkalo se jim *bomby* - jméno mohlo narážet na hlasitý tikot, který vydávaly, když prověřovaly nastavení scramblerů. Další verze říká, že Rejewski dostal nápad postavit tyto přístroje, když v kavárně jedl „bombu", zmrzlinu ve tvaru polokoule. Bomby účinně mechanizovaly proces dešifrování. Byla to přirozená odpověď na Enigmu, jež byla mechanizací šifrování.

Po velkou část 30. let 20. století pracoval Rejewski se svými kolegy neúnavně na odhalování klíčů k Enigmě. Měsíc po měsíci se tým musel vypořádávat se stresem a napětím kryptoanalýzy, opravovat

mechanické poruchy bomb, zvládat nekončící přísun zašifrovaných odposlechů. Jejich životy začaly být ovládány pronásledováním denních klíčů, té rozhodující informace, která odhalí smysl

zašifrovaných zpráv. Polští kryptoanalytici však nevěděli, že velká část jejich práce je zbytečná. Šéf Biura major Gwido Langer v té době už vlastnil denní klíče Enigmy, ukrýval je však schované ve svém stole.

Langer prostřednictvím Francouzů získával informace od Schmidta. Aktivity německého špiona neskončily v roce 1931 dodáním dvou dokumentů o fungování Enigmy, ale pokračovaly po dalších sedm let. Schmidt se setkal s francouzským agentem Rexem asi dvacetkrát, často na odlehlých horských chatách, kde bylo zaručeno jejich soukromí. Na každém setkání Schmidt předal jednu nebo více kódových knih, z nichž každá obsahovala měsíční dávku denních klíčů. Byly to právě ty kódové

knihy, jež byly distribuovány všem německých operátorům Enigmy a které obsahovaly všechny informace potřebné k zašifrování a dešifrování zpráv. Celkem Schmidt dodal kódové knihy, které obsahovaly denní klíče na 38 měsíců. Klíče by Rejewskému ušetřily obrovské množství času a námahy, nebylo by třeba konstruovat bomby a bylo by možné uvolnit pracovní sílu pro jiné sekce Biura. Pozoruhodně prohnaný Langer se však rozhodl Rejewskému neprozradit, že má klíče k dispozici. Tím, že Rejewského připravil o snadno získané klíče, jej Langer připravoval na nevyhnutelný okamžik, kdy už klíče nebudou k dispozici. Věděl, že když vypukne válka, nebude již Schmidt moci pokračovat v tajných schůzkách a Rejewski bude muset být soběstačný. Langer si myslel, že by měl Rejewski trénovat své dovednosti ještě v době míru jako přípravu na události, které je čekají.

Rejewski nakonec narazil na meze svých možností. V prosinci 1938 němečtí kryptografové zvýšili bezpečnost Enigmy. Všichni operátoři dostali dva nové scramblery, takže jejich uspořádání mohlo být tvořeno jakýmikoli třemi z pěti možných scramblerů. Předtím byly k dispozici pouze tři scramblery (označené 1, 2 a 3), ze kterých se mohlo vybírat, a tedy pouze šest způsobů jejich uspořádání, nyní však navíc přibyly dva scramblery (označené 4 a 5), počet uspořádání tedy vzrostl na 60, jak vidíme v tabulce 10. Prvním úkolem Re-jewského bylo nalézt vnitřní zapojení dvou nových scramblerů. Horší však bylo, že také musel postavit desetkrát více bomb, aby mohl i nadále testovat všechna možná uspořádání scramblerů. Nákladyna vybudování takové baterie bomb byly patnáctinásobkem ročního rozpočtu na vybavení celého Biura. Následující měsíc se situace dále zhoršila, protože Němci zvýšili počet kabelů propojovací desky z šesti na deset. Místo dvanácti písmen, která se měnila před vstupem do scramblerů, se jich nyní měnilo dvacet. Počet možných klíčů vzrostl na 159 000 000 000 000 000 000.

V roce 1938 dosáhly dovednosti Poláků v odposlechu a dešifrování svého vrcholu, začátkem roku 1939 však nové scramblery a přidané kabely zarazily tok špionážních informací. Rejewski, který v předchozích letech posouval hranice možností kryptoanalýzy, byl dočasně poražen. Dokázal, že Enigma není nerozlomitelná šifra, ale bez prostředků nutných k prověření každého nastavení scramblerů nemohl najít denní klíč a dešifrování nebylo možné. V takových bez-nadějných podmínkách by mohl být Langer v pokušení předat klíče, které získal od Schmidta, ale už je neměl. Právě před zavedením nových scramblerů Schmidt zrušil kontakty s agentem Rexem. Po sedm let mu dodával klíče, které nebyly nezbytné. Když však nyní Poláci klíče opravdu potřebovali, už nebyly k dispozici.

Nová nezranitelnost Enigmy byla zdrcujícím úderem pro Polsko, protože Enigma nebyla pouze prostředkem komunikace, ale také klíčovou součástí Hitlerovy strategie tzv. *hlitzkriegu.* Koncept této bleskové války zahrnoval rychlý, intenzivní, koordinovaný útok, což znamenalo, že velké tankové divize musely komunikovat mezi sebou navzájem stejně jako s pěchotou a dělostřelectvem.

Kromě toho měly být pozemní síly podporovány hloubkovými bombardéry *Štuka*, což vyžadovalo účinnou a rychlou komunikaci mezi frontou

Uspořádání tří scramblerů	Uspořádání se dvěma přidanými scramblery									
123	1	1	1	1	1	1	1	1	1	1
	24	25	34	35	42	43	45	52	53	
132	1	2	2	2	2	2	2	2	2	2
	54	14	15	34	35	41	43	45	51	
213	2	2	3	3	3	3	3	3	3	3
	53	54	14	15	24	25	41	42	45	
231	3	3	3	4	4	4	4	4	4	4
	51	52	54	12	13	15	21	23	25	
312	4	4	4	4	4	4	5	5	5	5
	31	32	35	51	S2	53	12	13	14	
321	5	5	5	5	5	5	5	5	5	5
	21	23	24	31	32	34	41	42	43	

Tabulka 10: Uspořádání pěti scramblerů

a letišti v zázemí. Heslem blitzkriegu byla „rychlost útoku díky rychlosti komunikace". Pokud Poláci nemohli přijít Enigmě na kloub, neměli naději, že by zastavili prudký německý útok, který byl očividně záležitostí pouhých několika měsíců. Němci už okupovali Sudety a 27. dubna 1939 odvolali pakt o neútočení s Polskem. Hitlerova protipolská rétorika byla čím dál tím ostřejší. Langer se rozhodl, že pokud dojde k invazi do Polska, pak jeho kryptografický průlom, který byl do té doby držen v tajnosti před Spojenci, nesmí být ztracen. Jestliže Polsko nemohlo mít užitek z Rejewského práce, potom Weli mít možnost ji vyzkoušet a pokračovat v ní Spojenci. Langer uvažoval, že Británie a Francie, země daleko bohatší než Polsko, by •nožná dokázaly plně využít princip bomb.30. června major Langer zatelegrafoval svým francouzským a britským protějškům a pozval je do Varšavy, aby prodiskutovali některé naléhavé záležitosti týkající se Enigmy. 24. června vedoucí francouzští a britští kryptoanalytici dorazili do ústředí Biura, aniž by věděli, co je čeká. Langer je uvedl do místnosti, ve které stál objekt pokrytý černou látkou. Látku stáhl a dramaticky tak odhalil jednu z Re-jewského bomb. Jeho publikum užaslo, když slyšelo, jak Rejewski po léta luštil Enigmu. Poláci byli o deset let popředu před kýmkoli jiným na světě. Zvláště Francouzi žasli, protože práce Poláků byla založena na výsledcích francouzské špionáže. Francouzi předali informaci od Schmidta Polákům, protože se domnívali, že nemá žádnou hodnotu, ale Poláci dokázali, že tomu tak není.

Jako překvapení na závěr Langer nabídl Britům a Francouzům dvě náhradní repliky Enigmy a detailní plány bomb, které pak byly převezeny v diplomatických zavazadlech do Paříže. Odtamtud byl 16. srpna jeden z přístrojů Enigma poslán do Londýna. Přes kanál La Manche jej ve svých zavazadlech propašoval dramatik Sacha Gui-try a jeho žena, herečka Yvonne Printempsová, aby případní němečtí špioni pozorující přístav nepojali podezření. O dva dny později, 1. září 1939, Hitler vpadl do Polska a začala válka.

Husa, která nikdy nezaštěbetala

Po třináct let se Britové a Francouzi domnívali, že šifra Enigma je nerozlomitelná, ale nyní vysvitla naděje. Polský objev dokázal, že šifra Enigma není beze slabin, což pozvedlo morálku spojeneckých kryptoanalytiků. Polský postup byl zastaven zavedením nových scramblerů a zvýšením počtu propojovacích kabelů, zůstalo však nesporné, že Enigmu už není třeba považovat za dokonalou šifru.

Polský průlom také dokázal Spojencům význam působení matematiků v roli kryptoanalytiků. Britská Kancelář č. 40 byla vždy ovládána lingvisty a klasickými filology, nyní však nastala intenzivní snaha doplnit pracovníky o matematiky a přírodovědce. Vědci byli přijímáni především na základě známostí („old-boy network"). Kmenoví zaměstnanci Kanceláře č. 40 kontaktovali své bývalé kolegy z Oxfordu a Cambridge. Existovala i síť „starých kamarádek" („old-girl network"), která získávala absolventky z míst jako Newn-ham College a Girton College v Cambridgi.

Noví pracovníci nemířili do Kanceláře č. 40 v Londýně, ale místo toho šli do Bletchley Park v Buckinghamshire, sídla tzv. Government Code and Cypher School (GC&CS), nově vytvořené organizace, která postupně přebírala úlohu Kanceláře č. 40. Bletchley Park mohl poskytnout prostor daleko více pracovníkům, což bylo důležité, protože hned po začátku války se očekávala záplava šifrovaných odposlechů. Během první světové války Německo odvysílalo dva miliony slov za měsíc, ale předpokládalo se, že větší rozšíření rádia v druhé světové válce může vést k přenášení až dvou milionů slov denně.

Ve středu Bletchley Parku stálo rozlehlé venkovské sídlo z viktoriánských dob postavené v pseudogotickém stylu finančníkem sirem Herbertem Leonem. Zámeček s knihovnou, jídelnou a zdobeným tanečním sálem se stal sídlem velení celé operace Bletchley. Velitel Alastair Denniston, ředitel GC&CS, měl v přízemí kancelář s výhledem do zahrady, který mu však brzy zkazila výstavba velkého množství nových budov. Tyto provizorní dřevěné stavby byly sídlem různých kryptoanalytických aktivit. Například budova č. 6 se specializovala na luštění komunikací německé armády. Pak předala dešifrované texty do budovy č. 3, kde pracovníci zpravodajské služby texty překládali a snažili se získané informace využít. Budova č. 8 se specializovala na námořní Enigmu, její zaměstnanci rozšifrované zprávy posílali do budovy č. 4, kde se sbíraly a překládaly zpravodajské informace. Původně bylo v Bletchley Parku pouze dvě stě zaměstnanců, za pět let však zámeček a provizorní stavby hostily sedm tisíc mužů a žen.

Během podzimu 1939 se vědci a matematici v Bletchley naučili bojovat proti záludnostem šifry Enigmy a rychle si osvojili techniku Poláků. Bletchley měl více pracovníků a zdrojů než polské Biuro Szyfrow, byl tedy schopen zvládnout zvýšení počtu scramblerů a fakt, že složitost Enigmy vzrostla na desetinásobek. Každých

čtyřiadvacet hodin se pro britské kryptoanalytiky opakovala stejná rutina. O půlnoci přešli němečtí operátoři Enigmy na nový denní klíč. Od tohoto okamžiku už bylo lhostejné, co v Bletchley dokázali předchozího dne - začínalo se znovu. Kryptoanalytici museli začít identifikovat nový denní klíč. To mohlo zabrat několik hodin, ale jakmile objevili nastavení Enigmy pro tento den, pracovníci Bletchley mohli začít dešifrovat nashromážděné německé zprávy a odhalovat informace, které byly v jejich boji s nacisty neocenitelné.

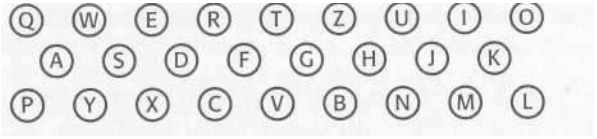
Překvapení je klíčovým nástrojem každého vojenského velitele. Jakmile se v Bletchley podařilo rozluštit Enigmu, německé plány byly rázem čitelné a Britové věděli, co zamýšlí německé vrchní velení. Když se Britové dozvěděli o místě hrozícího útoku, mohli vyslat posily nebo provést úhybný manévr. Jestliže se Spojencům podařilo zachytit a dešifrovat rozhovor Němců o vlastních slabinách, mohli tím směrem zaměřit ofenzívu. Dešifrovací práce v Bletchley byly válečnou aktivitou s nejvyšším stupněm důležitosti. Když například Německo napadlo Dánsko a Norsko v dubnu roku 1940, Bletchley poskytl detailní obrázek německých operací. Během bitvy o Británii dovedli kryptoanalytici předem varovat před bombardováním včetně časových a místních údajů. Kromě toho ještě dodávali informace o stavu *Luftwaffe*, například o počtu zničených letadel a o rychlosti, s jakou byly nahrazeny. Bletchley všechny tyto informace posílal do ústředí MI6, které je dále předávalo válečnému kabinetu, ministerstvu letectví a admiralitě.

Mezi ovlivňováním průběhu války si kryptoanalytici tu a tam našli čas na odpočinek. Podle Malcolma Muggeridge, který sloužil

•$_{n}$é službě a navštívil Bletchley, patřil k oblíbeným kratochvílím asák, zjednodušená verze softbalu:

Každý den po obědě, když bylo počasí příznivé, hráli kryptoanalytici pasáka na trávníku před zámečkem, přičemž se chovali napůl vážně, jak se lidé z univerzitních kruhů chovají, kdykoli se *zabývají* činnostmi, jež by mohly být pokládány za lehkovážné nebo bezvýznamné v porovnání s jejich hlavními aktivitami. Stávalo se tedy, že o nějaké herní situaci diskutovali se stejným zápalem, s nímž by se patrně věnovali otázkám, zda mají lidé svobodnou vůli anebo jak vznikl svět."

Jakmile kryptoanalytici z Bletchley zvládli polské postupy, začali hledat vlastní cesty k nalezení klíče Enigmy. Například využili faktu že němečtí operátoři Enigmy občas volili snadné klíče. Pro každou zprávu měl operátor vybrat odlišný klíč zprávy, tři náhodná písmena. Ale v žáru bitvy, než aby přepracovaní operátoři namáhali svou představivost a vybrali náhodný klíč, zvolili někdy raději tři písmena následující za sebou na klávesnici Enigmy (viz obrázek 46), jako třeba QWE nebo BNM. Těmto snadným klíčům zprávy se v Bletchley začalo říkat *cilky* (angl. *cillies).* Jinou *cilkou* bylo opakované používání některých klíčů zprávy, možná iniciál operátorovy přítelkyně - jedny takové iniciály C. I. L. mohly stát u



původu tohoto

kých filologů, šachových velmistrů a křížovkářů v rámci každé budovy. Na první pohled neřešitelný problém koloval tak dlouho, dokud se nedostal k někomu, kdo dostal ten správný nápad vedoucí k ieho vyřešení, nebo k někomu, kdo ho byl schopen vyřešit alespoň částečně a pak jej poslal zase dál. Gordon Welchman, který velel budově č. 6, popsal svůj tým jako „smečku loveckých psů, kteří se snaží zachytit stopu". V Bletchley se odehrálo mnoho velkých kryp-toanalytických průlomů a zabralo by několik knih popsat každý jednotlivý přínos. Ale jedna osobnost zasluhuje být přece popsána podrobněji - Alan Turing, který rozpoznal největší slabinu Enigmy a nemilosrdně jí využil. Díky Turingovi se podařilo luštit šifru Enigma dokonce za nejsložitějších okolností.

Alan Turing byl počat na podzim roku 1911 v Chatrapuru, ve městě blízko Madrasu v jižní Indii, kde byl jeho otec Julius Turing úředníkem. Julius a jeho žena Ethel se rozhodli, že se jejich syn má narodit v Británii, a proto se vrátili do Londýna, kde se Alan 23. června 1912 narodil. Jeho otec se brzy poté vrátil do Indie a matka jej následovala pouze o patnáct měsíců později. Alana zanechala v péči chův a přátel, dokud nebyl dost velký, aby mohl chodit do internátní školy.

V roce 1926 ve věku 14 let se Turing stal žákem Sherborne Scho-ol v Dorsetu. V první den jeho školní docházky se konala generální stávka, ale Turing se rozhodl školu nezameškat, a tak jel bez dopro**Obrázek 46:** Rozložení klávesnice Enigmy.

termínu. Než přistoupili kryptoanalytici ke zdlouhavému luštění Enigmy běžnou obtížnou cestou, stalo se jejich zvykem napřed vyzkoušet cilky. Jejich tušení se někdy vyplatilo.

Cilky nebyly slabou stránkou Enigmy, ale její obsluhy. Bezpečnost Enigmy snížila také jiná lidská chyba, tentokrát na vyšší úrovni. Ti, kteří byli zodpovědní za sestavení knih kódů, se museli rozhodnout, které scramblery budou konkrétního dne použity a ve které pozici. Snažili se dosáhnout toho, aby nastavení scramblerů bylo nepředvídatelné, takže rozhodli, že žádný scrambler nesmí zůstat ve stejné pozici dva dny po sobě. Označíme-li scramblery čísly 1, 2, 3, 4 a 5, pak bude první den uspořádání například 134, druhý den bude přípustné uspořádání 215, ale ne 214, protože scrambler číslo 4 nesmí zůstat ve stejné pozici dva dny po sobě. To může vypadat jako rozumná strategie, protože scramblery neustále mění pozici, ale uplatnění takového pravidla vlastně ulehčuje kryptoanaly-tikům život. Vyloučení některých možností znamená, že ti, kdo sestavovali knihy kódů, zmenšili o polovinu počet možných uspořádání. Kryptoanalytici z Bletchley si to uvědomili a snažili se toho co nejvíce využít. Jakmile určili uspořádání scramblerů pro jeden den, mohli okamžitě vyloučit polovinu uspořádání pro den následující, tudíž jejich pracovní zatížení bylo zmenšeno o polovinu.

Podobně tomu bylo s pravidlem, že nastavení propojovací desky nesmějí zahrnovat výměnu mezi písmenem a jeho sousedem, což znamenalo, že S smí být

zaměněno za jakékoliv písmeno kromě R a T. Existoval názor, že je dobré se takovým očividným výměnám záměrně vyhýbat, ale zavedení tohoto pravidla rovněž drasticky snížilo počet možných klíčů.

Hledání nové kryptoanalytické zkratky bylo nezbytné, protože přístroj Enigma se během války stále vyvíjel. Kryptoanalytici byli neustále nuceni inovovat, znovu navrhovat a dolaďovat bomby a hledat úplně nové strategie. Částečnou příčinou jejich úspěchu byla bizarní sestava matematiků, přírodovědců, lingvistů, klasic- vodu na kole 100 km ze Southamptonu do Sherborne, což byl výkon, o němž pak psali v místních novinách. Během prvního roku ve škole získal pověst nesmělého, neohrabaného chlapce, jehož jediné schopnosti se projevily v oblasti přírodních věd. Cílem Sherborne bylo z chlapců udělat vyrovnané muže, způsobilé k vládnutí impériu, ale Turing tyto ambice nesdílel a cítil se ve škole nešťastný.

Jeho jediným skutečným přítelem ve škole byl Christopher Mor-com, který se rovněž zajímal o přírodní vědy. Společně diskutovali o posledních vědeckých novinkách a prováděli vlastní pokusy. Jejich přátelství zažehlo Turingovu intelektuální zvědavost, ale - což je důležitější - mělo pro něj také hluboké emocionální následky. An-drew Hodges, Turingův životopisec, napsal: „Byla to první láska... Patřil k ní pocit podlehnutí a zjitřené pozornosti, jako když jiskřivé barvy vybuchují na černobílém pozadí." Jejich přátelství trvalo čtyři roky, ale Morcom si zřejmě nebyl vědom hloubky citu, který k němu Turing choval. Během jejich posledního roku na Sherborne Turing navždy ztratil možnost říci mu o svých citech. Ve čtvrtek 13. února 1930 Christopher Morcom náhle zemřel na tuberkulózu.

Turing byl zničen ztrátou jediné osoby, kterou kdy miloval. Jeho způsobem, jak se vyrovnat s Morcomovou smrtí, bylo soustředit se na vědecké studium a jít ze všech sil ve stopách talentovaného přítele. Morcom, který se zdál být z obou chlapců nadanější, již získal stipendium do Cambridge. Turing byl přesvědčen, že je také jeho povinností získat místo v Cambridgi a učinit objevy, které by jinak určitě učinil jeho přítel. Požádal Christopherovu matku o fotografii, a když ji dostal, matce odepsal: „Dívá se na mne z mého stolu a povzbuzuje mě k tvrdé práci."

Roku 1931 byl Turing přijat na King's College v Cambridgi. Vstoupil tam v době, kdy probíhala intenzivní debata o povaze matematiky a logiky, a Turing tak měl na dosah ruky její hlavní účastníky, k nimž patřil Bertrand Russell, Alfred North Whitehead a Ludwig Wittgenstein. V centru polemiky byl problém nerozhod-nutelnosti, kontroverzní pojem vyvinutý logikem Kurtem Gódelem. Dříve se předpokládalo, že - alespoň teoreticky - lze nalézt odpověď na všechny matematické otázky. Ale Godel dokázal, že existuje jisté množství otázek, jež stojí mimo dosah logického důkazu, takzvané nerozhodnutelné otázky. Matematici byli traumatizováni novinkou, že matematika není všemocná disciplína, za kterou ji vždy považovali. Chtěli zachránit svůj obor, a tak hledali způsob, jak identifiko$_t$ ošemetná tvrzení tak, aby nebyla nerozhodnutelná. Právě tento '1 inspif°^{va}l Turinga k napsání jeho nejvlivnější matematické stati *On Computable Numbers* (O vyčíslitelnosti), publikované roku 1937. V divadelní hře o Turingově životě

Prolomení kódu, kterou napsal Hugh Whitemore, se jedna postava ptá Turinga na význam jeho práce Odpoví: ‚Je to o tom, co je správné a co špatné. V podstatě to je odborný článek o matematické logice, ale také o tom, jak těžko se odlišuje správné od špatného. Lidé - většina lidí - si myslí, že v matematice vždy víme, co je pravda a co omyl. Tak to není. Už ne."

Ve snaze identifikovat nerozhodnutelné otázky popisuje Turingův článek pomyslný stroj, který byl sestrojen, aby prováděl matematické operace nebo algoritmy. Jinými slovy, takový stroj by dovedl provést pevně stanovený, předepsaný sled kroků, jež by například vynásobily dvě čísla. Turing předpokládal, že by se čísla k vynásobení vložila do stroje prostřednictvím papírové pásky podobné děrné pásce, pomocí níž se vkládala melodie do mechanického piána. Výsledek násobení by se pak zapsal na jinou pásku. Turing si představoval celou řadu takzvaných Turingových strojů, každý speciálně vytvořený k řešení určitého úkolu jako dělení, umocnění nebo rozklad na činitele. Potom učinil radikální krok.

Vymyslel si stroj, jehož vnitřní chod by se dal měnit tak, aby mohl vykonávat všechny funkce všech představitelných Turingových strojů. Tato změna by se realizovala vkládáním dalších pásek, které by proměnily univerzální stroj ve stroj na dělení, stroj na násobení nebo na jiný typ stroje. Turing toto hypotetické zařízení nazval *univerzální Turingův stroj*, protože by byl schopen odpovědět na jakoukoli otázku, kterou si jen dokáže logik vymyslet. Naneštěstí se ukázalo, že není vždy v silách logiky zodpovědět otázku o rozhod-nutelnosti jakéhokoli výroku, a tak ani univerzální Turingův stroj nebyl schopen rozhodnout, zda je nebo není daný výrok pravdivý.

Matematici, kteří četli Turingovu stať, byli zklamáni, že Gódelo-va příšera nebyla zdolána, ale jako cenu útěchy jim Turing předal detailní plán moderního programovatelného počítače. Turing znal Babbagovu práci, univerzální Turingův stroj lze chápat jako reinkarnaci jeho *Difference Engine No. 2*. Turing však šel mnohem dále [a] položil programování solidní teoretický základ, který nás dodnes ohromuje svým potenciálem. Nezapomeňme, že se vše udalo ve tři-[c]atých letech 20. století, kdy neexistovala technologie, která by Tu-Hnguv stroj mohla zhmotnit. Jemu to však nevadilo. Toužil po uzná-ní ze strany matematické komunity, která jeho článku zatleskala jako jednomu z nejdůležitějších objevů století. Turingovi bylo teprve dvacet šest let.

Pro Turinga to bylo obzvláště šťastné a úspěšné období. Ve třicátých letech udělal vědeckou kariéru a stal se členem King's College, sídla světové intelektuální elity. Vedl život ortodoxního cambridgeského učitele - dával přednost čisté matematice a triviálním aktivitám. Roku 1938 si zašel na film *Sněhurka a sedm trpaslíků*, obsahující památnou scénu, v níž zlá královna ponoří jablko do jedu. Jeho kolegové pak často slýchali hrůzný zpěv: „Vlož jablko do lektvaru, dej mu sílu smrti, zmaru."

Turing si své roky v Cambridgi užil. Nejen že dosáhl akademického úspěchu, ale nalézal se v tolerantním a motivujícím prostředí. Homosexualita byla na univerzitě do značné míry tolerována, což

znamenalo, že měl volnost navazovat vztahy, aniž by se musel strachovat, kdo by to mohl odhalit a co by tomu řekli ostatní kolegové. Přestože neměl vážný dlouhodobý vztah, zdálo se, že je se svým životem spokojený. Potom se v roce 1939 Turingova akademická kariéra prudce přerušila. Government Code and Cypher School jej pozvala, aby se stal kryptoanalytikem v Bletchley. 4. září 1939, den poté, co Neville Chamberlain vyhlásil válku Německu, se Turing přestěhoval z cambridgeské idyly do hostince Crown Inn ve vesnici

Shenley Brook End.

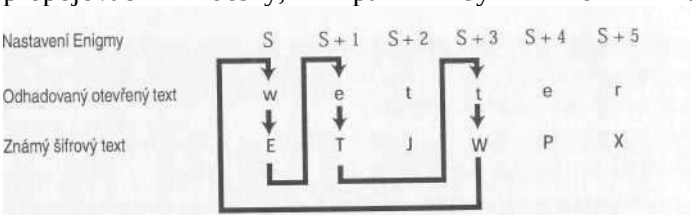
Každý den jel na kole S km ze Shenley Brook End do Bletchley Park a tam částečně pobýval v jednotlivých budovách, kde se podílel na rutinní práci při rozlamování kódů, a částečně se pohyboval ve výzkumném středisku, bývalém skladišti jablek, hrušek a švestek sira Herberta Leona. Tam kryptoanalytici diskutovali o aktuálních problémech nebo společně probírali, jak se vypořádat s problémy, které mohou nastat v budoucnosti. Turing se soustředil na to, co se může stát, kdyby Němci změnili svůj systém výměny klíčů zprávy. Počáteční úspěchy Bletchley vycházely z práce Rejewského, který využil faktu, že operátoři Enigmy šifrovali každý klíč zprávy dvakrát (pokud byl klíč zprávy například YGB, potom operátor zašifroval YGBYGB). Toto opakování mělo zajistit, že příjemce neudělá chybu, ale zároveň vytvořilo trhlinu v bezpečnosti Enigmy. Britští kryptoanalytici odhadovali, že nepotrvá dlouho, než si Němci všimnou, že opakování klíče šifru Enigmu ohrožuje. Pak by patrně operátorům Enigmy řekli, aby opakování klíče zanechali, čímž by aktuální techniky používané v Bletchley přestaly fungovat. Bylo na Turingovi, jak *nalézt* alternativní způsob útoku na Enigmu - způsob, který by nespoléhal na opakování klíče zprávy.

Jak týdny plynuly, Turing si uvědomil, že se v Bletchley shromáždila rozsáhlá knihovna rozšifrovaných zpráv, a všiml si, že mnoho z nich mělo pevnou strukturu. Došel k názoru, že studiem starých rozšifrovaných zpráv by mohl někdy předpovědět část obsahu ne-rozšifrované zprávy, pokud by vyšel z doby odeslání a zdroje zprávy. Zkušenosti například ukazovaly, že Němci denně posílali krátce po šesté hodině pravidelné zprávy o počasí. Takže šifrovaná zpráva zachycená v 6.05 téměř jistě obsahovala slovo wetter, což německy znamená „počasí". Přísný protokol používaný v armádě znamenal, že takové zprávy byly stylově velmi sešněrované, takže Turing si mohl být jist, že v zašifrované zprávě slovo wetter skutečně nalezne. Díky pevné struktuře zpráv se dalo téměř s určitostí říci, že prvních šest písmen určitého zašifrovaného textu odpovídá v původní zprávě písmenům wetter. Když lze část otevřeného textu takto propojit s

částí šifrového textu, říkají kryptoanalytici takové vazbě „tahák" (angl. crib).

Turing si byl jist, že by mohl pomocí taháků rozluštit Enigmu. Kdyby měl zašifrovaný text a věděl, že určitý jeho úsek, řekněme ETJWPX, představuje wetter, pak by stál před úkolem nalézt takové nastavení Enigmy, které by změnilo wetter na ETJWPX. Jednoduchý, ale nepraktický způsob, jak to udělat, by bylo vzít přístroj Enigma, vyťukat wetter a podívat se, zda se ukáže správný šifrový text. Pokud ne, potom by kryptoanalytik změnil nastavení přístroje prohozením kabelů na propojovací desce, prohozením nebo změnou orientace scramblerů a pak by znovu vyťukal wetter. Pokud by se opět neobjevilo správné znění šifrového textu, kryptoanalytik by změnil nastavení znovu - a znovu a znovu, dokud by nenalezl to správné řešení. Jediný problém s touto metodou pokusů a omylů je skutečnost, že existuje 159 000 000 000 000 000 000 možných nastavení, jež je třeba ověřit, takže nalezení toho jediného uspořádání, které by změnilo wetter na ETJWPX, je zdánlivě nemožným úkolem.

Aby Turing problém zjednodušil, pokusil se napodobit Rejewského strategii. Chtěl oddělit problém nastavení scramblerů (pozice jednotlivých scramblerů a jejich konkrétní orientace) od problému zapojení propojovací desky. Kdyby přišel na to, jak využít taháky nezávisle na zapojení propojovací desky, pak by mohl ověřit všech-



Obrázek 48: Jeden z Turingových taháků, který znázorňuje smyčku.

ny možné kombinace scramblerů, jichž bylo 1 054 560 (60 uspořádání x 17 576 orientací). To už bylo schůdné. Po nalezení správného nastavení scramblerů by mohl odvodit zapojení propojovací desky. Nakonec se rozhodl pro konkrétní typ taháků obsahující vnitřní smyčky podobné řetězcům, s nimiž pracoval Rejewski. Řetězce spojovaly písmena uvnitř opakovaného klíče zprávy. Turingovy smyčky však neměly co dělat s klíčem zprávy, neboť Turing ve své práci vycházel z předpokladu, že Němci brzy přestanou opakované klíče zpráv vysílat. Turingovy smyčky místo toho spojovaly písmena původního a zašifrovaného textu. Například tahák na obrázku 48 obsahuje smyčku. Nezapomeňte, že taháky jsou založeny pouze na odhadech - ale pokud předpokládáme, že tahák je správný, můžeme spojit písmena w~*E, e—>T, t-+W jako část smyčky. Přestože neznáme nastavení Enigmy, můžeme první nastavení, ať již je jakékoli, označit jako S. Víme, že v tomto prvním nastavení je w zašifrováno jako E. Po tomto zašifrování se první

scrambler posune o jedno místo na nastavení S + 1 a písmeno e je zašifrováno jako T. Scrambler se pootočí o další pozici a zašifruje písmeno, které není součástí smyčky, takže toto šifrování budeme ignorovat. Scrambler se posune o další místo a my znovu dosáhneme písmene, které je součástí smyčky. V nastavení S + 3 je písmeno t zašifrováno jako W. Úhrnem tedy víme:

V nastavení S Enigma zašifruje w jako E.

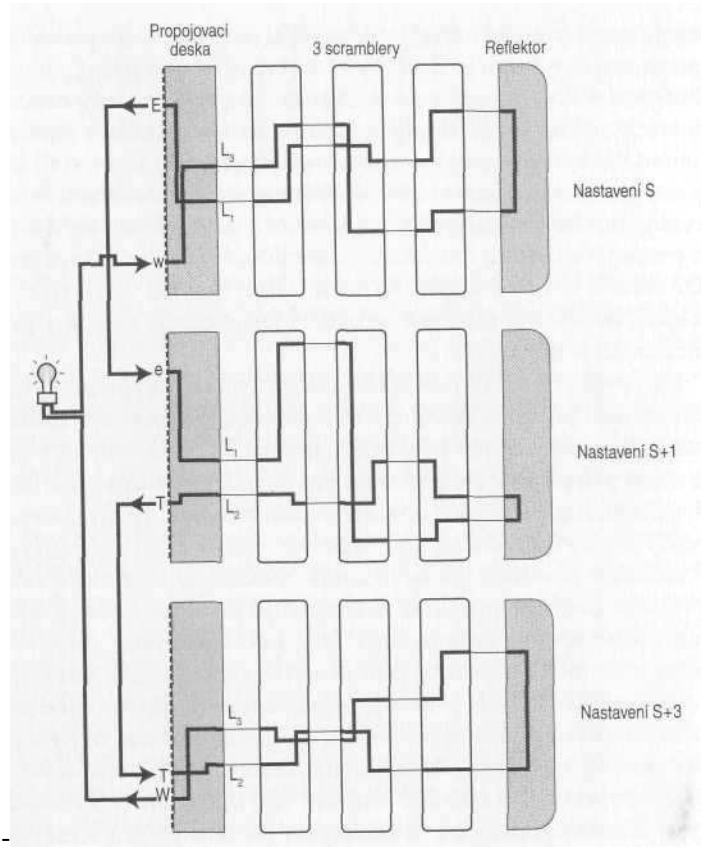
V nastavení S + 1 Enigma zašifruje e jako T.

V nastavení S + 3 Enigma zašifruje t jako W.

Zatím to vypadá jen jako zajímavá šifrovací struktura, ale Turing pečlivě sledoval důsledky vztahů uvnitř smyčky a pochopil, že získal klíčovou zkratku, kterou potřeboval k rozlomení Enigmy. Namísto toho, aby pracoval s jedním přístrojem Enigma na testování každého nastavení, začal si Turing pohrávat s myšlenkou na tři oddělené stroje, z nichž každý by se *zabýval* rozšifrováním jednoho ele-jnentu smyčky. První přístroj by zkusil zašifrovat w jako E, druhý by zašifroval e do T a třetí t do W. Tyto tři přístroje by byly nastaveny identicky až na to, že druhý z nich by měl scramblery nastaveny o jeden krok dále oproti prvnímu (nastavení S + 1) a třetí o tři kroky oproti prvnímu (nastavení S + 3). Turing si pak představil horečně pracujícího kryptoanalytika nepřetržitě měnícího zapojení kabelů na propojovací desce i nastavení scramblerů, aby dosáhl správného zašifrování. Všechny změny by musel dělat vždy na všech třech přístrojích najednou, přičemž by musel respektovat popsaný posun v nastavení scramblerů.

Na první pohled to není žádný velký úspěch. Kryptoanalytici by stále museli prověřit všech 159 000 000 000 000 000 000 možných nastavení, a aby to bylo ještě horší, museli by totéž provést zároveň na třech přístrojích, ne pouze na jednom. Další stupeň Turingova nápadu však mění situaci a velmi ji zjednodušuje. Turinga napadlo spojit Enigmy mezi sebou tak, že povede vodiče mezi vstupy a výstupy každého přístroje, jak to ukazuje obrázek 49. Smyčka v taháku se vlastně nahradí smyčkou elektrického obvodu. Podle Turingových představ měly Enigmy stále měnit svá nastavení, jak je to popsáno výše, avšak proud by jimi protékal pouze tehdy, když by nastavení na všech třech přístrojích byla správná. Kdyby do obvodu přidal žárovku, proud by ji rozsvítil a signalizoval tak, že bylo nalezeno správné nastavení. Prozatím by všechny tři přístroje stále ještě musely prověřit 159 000 000 000 000 000 000 možných nastavení, aby se žárovka rozsvítila. Avšak teprve po této přípravě měl přijít Turingův závěrečný logický skok, jenž úlohu rázem zjednodušil o řád sta miliard.

Turing zkonstruoval elektrický obvod tak, aby anuloval vliv propojovací desky, takže umožnil ignorovat miliardy jejích možných nastavení. Obrázek 49 ukazuje, že do první Enigmy vstupuje elektrický proud do scramblerů a vystupuje na neznámém písmenu, které nazveme l_r Proud potom teče přes propojovací desku, která transformuje l_x na E. Písmeno E je spojeno vodičem s písmenem e v druhé Enigmě, kde se v další propojovací desce převede zpět na L_t. Jinými slovy, dvě propojovací desky se navzájem vynulují. Proud, Který vystupuje ze scramblerů druhé Enigmy, vstupuje do její propojovací desky na písmenu 1_2 a tam se převede na T. To je spojeno vodičem s písmenem t ve třetí Enigmě, a jak proud prochází její



Obrázek 49: Smyčka v taháku může být analogická elektrické smyčce. Tři přístroje Enigmy jsou nastaveny identicky až na to, že drahý přístroj má scramblery nastaveny o jeden krok dopředu oproti prvnímu přístroji (nastavení S + 1) a třetí nastavení je posunuto o tři kroky oproti prvnímu (nastavení S + 3). Výstup z každé Enigmy je poté napojen na vstup další Enigmy. Tři sady scramblerů se pak otáčejí společně až do okamžiku, kdy je obvod uzavřen a světlo se rozsvítí. V tu chvíli se dosáhne hledaného nastavení. V diagramu nahoře je obvod uzavřen, takže odpovídá správnému nastavení.

pro-pojovací deskou, převede se zpět na l_2. Propojovací desky se v celém obvodu navzájem vynulují, a proto je Turing mohl zcela ignorovat. Jediné, co teď potřeboval, bylo spojit výstup první sady scramblerů L_1 se vstupem druhé sady scramblerů (také LJ a tak dále. Turing

neznal hodnotu písmena L_{l3} takže musel propojit všech 26 výstupů nrvní sady scramblerů se všemi odpovídajícími vstupy druhé sady scramblerů a tak dále. Nakonec dostal 26 elektrických obvodů, $_z$ nichž každý měl žárovku, která signalizovala uzavření obvodu. Tři sady scramblerů by tedy jednoduše prověřily každou ze 17 576 orientací, druhá sada scramblerů by byla vždy o krok napřed před první a třetí sada scramblerů by byla o dva

kroky napřed před druhou sadou. Až by se nalezla správná orientace scramblerů, jeden z obvodů by se uzavřel a rozsvítil svou žárovku. Kdyby scramblery změnily orientaci každou vteřinu, daly by se všechny možnosti prověřit za pět hodin.

Zůstaly pouze dva problémy. Za prvé, mohlo by se stát, že by přístroje běžely se špatným uspořádáním scramblerů, protože Enigma používala, jak víme, vždy tři z pěti možných scramblerů uspořádané zcela libovolně, což dává šedesát možných nastavení. Pokud se tedy prověří všech 17 576 orientací a žárovka se nerozsvítí, je třeba vyzkoušet další z šedesáti možných uspořádání scramblerů. Jinou možnost představuje paralelně spustit šedesát sad po třech Enig-mách.

Druhý problém spočíval v tom, jak stanovit zapojení kabelů na propojovací desce, jakmile bylo známo uspořádání a orientace scramblerů. To je poměrně jednoduché. Kryptoanalytik nastaví na Enigmě správným způsobem scramblery, zapíše šifrový text a podívá se na výsledek. Pokud dostane tewwer místo wetter, pak je jasné, že kabely musí být zapojeny tak, aby zaměnily w a t. Vložení další části zašifrovaného textu odhalí další prohozená písmena.

Kombinace taháků, smyček a elektricky spojených přístrojů vyústila v pozoruhodné kryptografické dílo, jež mohl realizovat pouze Turing díky svým jedinečným znalostem matematických strojů. Jeho úvahy o imaginárních Turingových strojích byly reakcí na tajuplnou otázku matematické nerozhodnutelnosti, ale tento čistě akademický výzkum jej vybavil způsobem uvažování, které je nezbytné k návrhu praktického přístroje schopného vyřešit velmi reálné problémy.

Bletchley získal 100 000 liber nezbytných na realizaci Turingových myšlenek ve fungující zařízení, kterým se říkalo bomby, protože jejich mechanické řešení vzdáleně připomínalo přístroje, s nimiž pracoval Rejewski. Každá z Turingových bomb se měla skládat z dvanácti sad elektricky spojených scramblerů Enigmy, aby se uměla vy-pořádat s daleko delšími smyčkami písmen. Kompletní jednotka měla být kolem dvou metrů vysoká, dva metry dlouhá a metr široká. Turing dokončil svůj návrh na začátku roku 1940, výroba byla zadána společnosti British Tabulating Machinery v Letchworthu.

Zatímco Turing čekal na dodávku bomb, pokračoval ve své každodenní práci v Bletchley. Zvěst o jeho průlomu se brzy rozšířila mezi dalšími vedoucími kryptoanalytiky, kteří ho začali uznávat jako špičkového odborníka. Podle jeho kolegy Petera Hiltona: „Alan Turing byl evidentně génius, ale přístupný génius. Vždy byl ochoten vynaložit čas a námahu, aby vysvětlil své myšlenky; nebyl úzkým specialistou, takže jeho všestranné myšlení zahrnovalo rozlehlou oblast exaktních věd."

Vše, co se týkalo Government Code and Cypher School, bylo ovšem přísně tajné, takže nikdo mimo Bletchley si nebyl vědom Tu-ringova pozoruhodného výkonu. Například jeho rodiče ani netušili, že Alan pracuje jako kryptoanalytik, natož aby věděli, že je v této práci nejlepší v Británii. Jednou své matce řekl, zeje zapojen do určité formy vojenského výzkumu, ale dále to nerozváděl. Turingova matka bylajen poněkud rozladěna, že syna jeho pracovní postavení nepřiměje k serióznějšímu účesu. Bletchley sice byl vojenským zařízením, vojáci však uznali, že stojí za to tolerovat zanedbanost a ex-centričnost přítomných „profesůrků". Turing se málokdy obtěžoval oholit, nehty míval zanesené špínou, šaty zmačkané. Zda vojáci také vědomě tolerovali jeho homosexualitu, není známo. Jack Good, veterán z Bletchley, to komentoval slovy: „Naštěstí nahoře nevěděli, že Turing je homosexuál. Jinak bychom také mohli prohrát válku."

Jeho první prototyp bomby, pojmenovaný Victory, dorazil do Bletchley 14. března 1940. Přístroj byl hned uveden do provozu, ale první výsledky byly méně než uspokojující. Přístroj se ukázal být daleko pomalejší, než se předpokládalo, nalezení klíče trvalo týden. Soustředěným úsilím se Turingův tým snažil zvýšit jeho výkonnost. O několik týdnů později již dokončili nový návrh. Další čtyři měsíce zabrala výroba této vylepšené bomby. Mezitím se kryptoanalytici museli vypořádat s katastrofou, kterou předpokládali. Dne 1. května 1940 změnili Němci svůj protokol výměny klíčů. Přestali opakovat klíč zprávy, a proto se dramaticky snížil počet úspěšných rozšifrování Enigmy. Informační vakuum trvalo do 8. srpna, kdy dorazila nová bomba. Byla pokřtěna *Agnus Del* nebo krátce *Agnes.* Tento přístroj měl naplnit Turingova očekávání.

Během následujících osmnácti měsíců bylo uvedeno do provozu dalších patnáct bomb. Využívaly nápovědy z taháků, ověřovaly nastavení scramblerů a odhalovaly klíče, přičemž klapaly jako milion pletacích jehlic. Když šlo všechno dobře, bomba mohla nalézt klíč Enigmy za hodinu. Jakmile se podařilo pro konkrétní zprávu určit nastavení scramblerů a zapojení propojovací desky, tedy její klíč zprávy, bylo už jednoduché odvodit denní klíč a dešifrovat všechny ostatní zprávy zaslané téhož dne.

Přestože bomby představovaly rozhodující průlom v kryptografii, dešifrování se nestalo pouhou formalitou. Bylo třeba překonat mnoho překážek, než bomby mohly vůbec začít hledat klíč. Aby bomba mohla pracovat, potřebuje nejprve taháky, které hledali kryptoanalytici a předávali je operátorům bomb. Nebylo však zaručeno, že analytici uhodli správný význam zašifrovaného textu. Dokonce i když měli správný tahák, mohl být na špatném místě - kryptoanalytici mohli uhodnout, že zašifrovaná zpráva obsahuje určitou větu, ale přiřadili ji nesprávnému úseku šifrového textu. Existoval však trik sloužící k ověření, zda je tahák ve správné pozici.

V následujícím příkladu je kryptoanalytik přesvědčen, že je otevřený text správný, ale není si jist, zda jej propojil se správnými písmeny v zašifrovaném textu.

Odhadovaný otevřený text	wetternul	1	sechs	

Známý šifrový text IPRENLWKMJJSXCPLEJWQ

Jednou z vlastností přístroje Enigma byla jeho neschopnost zašifrovat písmeno na sebe sama, což byl důsledek existence reflektoru. Písmeno a nemohlo být zašifrováno jako A, písmeno b nemohlo být nikdy zašifrováno jako B a tak dále. Tahák uvedený výše tedy není umístěn správně, protože první e ve slově wetter nemůže odpovídat písmenu E v šifrovém textu. Abychom nalezli správnou pozici, zkusíme posunout otevřený a šifrový text vůči sobě, dokud se nedostaneme do polohy, kdy není ani jedno písmeno spárováno samo se sebou. Pokud posuneme otevřený text o jedno místo doleva, stále to nesedí, protože tentokrát první s v sechs odpovídá S v šifrovém textu. Pokud však posuneme otevřený text o jedno místo doprava, zmizí nekorektní párování. Tento tahák je tudíž pravděpodobně na správném místě a lze jej použít jako základ pro rozšifrovaní pomocí bomby:Odhadovaný wetternul 1 sechs
otevřený text

Známý šifrový text IPRENLWKMJJSXCPLEJWQ

Zpravodajské informace shromážděné v Bletchley byly k dispozici pouze nejvyššímu vojenskému velení a vybraným členům válečného kabinetu. Winston Churchill si byl plně vědom důležitosti práce v Bletchley a 6. září 1941 kryptoanalytiky navštívil. Při setkání byl překvapen podivnou směsicí lidí, kteří mu poskytovali tak hodnotné informace; vedle matematiků a lingvistů tam byl také specialista na porcelán, kurátor pražského muzea, mistr Británie v šachu a četní experti na bridž. Churchill řekl siru Stewartu Menziesovi, šéfovi Secret Intelligence Service: „Řekl jsem vám, abyste obrátili každý kámen, ale nečekal jsem, že to vezmete tak doslova." I přes tento komentář měl velkou slabost pro nesourodý tým. Nazval je „husou, která snáší zlatá vejce a nikdy nezaštěbetá".

Návštěva měla pozvednout morálku kryptoanalytiků a ukázat jim, že jejich práce je oceňována na nejvyšších místech. Díky ní také Tu-ring a jeho kolegové získali odvahu, aby s Churchillem navázali osobní kontakt, když se blížila krize. Aby Turing co nejvíce využil kapacitu bomb, potřeboval více zaměstnanců, jeho požadavek však zamítl nový ředitel Bletchley Edward Travis, který se obával, že nemůže odůvodnit další zvyšování stavů. Kryptoanalytici proto 21. října porušili subordinaci, ignorovali Travise a napsali přímo Churchillovi:

„Vážený pane premiére,

před několika týdny jste nás poctil návštěvou. Věříme, že považujete naši práci za důležitou. Měl jste možnost vidět, že - převážně díky energii a prozíravosti velitele Travise - jsme byli vybaveni „bombami" pro rozlomení německých kódů Enigma. Myslíme si však, že byste měl vědět, že tato práce vázne a že v některých případech není vykonávána vůbec, především proto, že nemáme dostatečný počet zaměstnanců pro obsluhu strojů. Obracíme se přímo na Vás z toho důvodu, že jsme

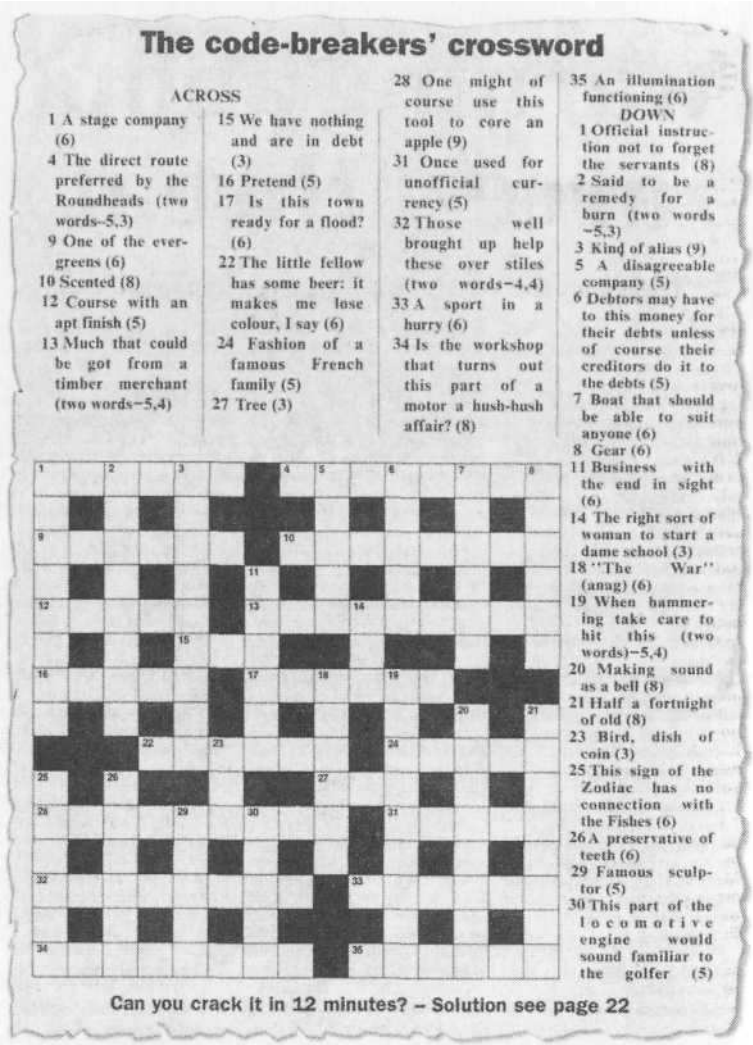
po měsíce dělali vše, co jsme mohli, běžnými úředními cestami a ztrácíme naději na brzké zlepšení bez Vaší intervence... Jsme, sire, Vašimi poslušnými služebníky, A. M. Turing W. G. Welchman C. H. O'D. Alexander P. S. Milner-Barry."

Churchill neváhal s odpovědí. Ihned se obrátil přípisem na svého personálního šéfa:

K OKAMŽITÉMU VYŘÍZENÍ

„Zajistěte, aby dostali vše, co chtějí, s nejvyšší možnou prioritou, a ohlaste mi, že se tak stalo."

Napříště už neexistovaly žádné překážky v přijímání pracovníků nebo v dodávkách materiálu. Koncem roku 1942 bylo v provozu 49 bomb. V Gayhurst Manor severně od Bletchley bylo zřízeno nové pracoviště vybavené bombami. Jako součást náboru zadala Government Code and Cypher School inzerát do *Daily Telegrapk.* Vyhlásila v něm anonymní soutěž pro čtenáře. Úkolem bylo vyluštit přiloženou křížovku (obrázek 51) v čase pod 12 minut. Vycházelo se z názoru, že experti na křížovky mohou být také dobrými kryptoana-lytiky a že by mohli vhodně doplnit vědecké mozky v Bletchley -o čemž samozřejmě v novinách nic nebylo. Odpovědělo 25 čtenářů, které pak pozvali do Fleet Street na test. Pět z nich dokončilo křížovku ve stanoveném čase, dalšímu chybělo pouze jedno slovo.O několik týdnů později se všech šest zúčastnilo pohovoru vedeného vojenskou rozvědkou a nakonec byli skutečně přijati jako kryp-toanalytici do Bletchley Parku.



The code-breakers' crossword

ACROSS

1 A stage company (6)
4 The direct route preferred by the Roundheads (two words–5,3)
9 One of the evergreens (6)
10 Scented (8)
12 Course with an apt finish (5)
13 Much that could be got from a timber merchant (two words–5,4)
15 We have nothing and are in debt (3)
16 Pretend (5)
17 Is this town ready for a flood? (6)
22 The little fellow has some beer: it makes me lose colour, I say (6)
24 Fashion of a famous French family (5)
27 Tree (3)
28 One might of course use this tool to core an apple (9)
31 Once used for unofficial currency (5)
32 Those well brought up help these over stiles (two words–4,4)
33 A sport in a hurry (6)
34 Is the workshop that turns out this part of a motor a hush-hush affair? (8)
35 An illumination functioning (6)

DOWN

1 Official instruction not to forget the servants (8)
2 Said to be a remedy for a burn (two words –5,3)
3 Kind of alias (9)
5 A disagreeable company (5)
6 Debtors may have to this money for their debts unless of course their creditors do it to the debts (5)
7 Boat that should be able to suit anyone (6)
8 Gear (6)
11 Business with the end in sight (6)
14 The right sort of woman to start a dame school (3)
18 "The War" (anag) (6)
19 When hammering take care to hit this (two words)–5,4)
20 Making sound as a bell (8)
21 Half a fortnight of old (8)
23 Bird, dish of coin (3)
25 This sign of the Zodiac has no connection with the Fishes (6)
26 A preservative of teeth (6)
29 Famous sculptor (5)
30 This part of the locomotive engine would sound familiar to the golfer (5)

Can you crack it in 12 minutes? – Solution see page 22

Obrázek 51: Křížovka v *Daily Telegraph* použitá jako test pro nábor nových kryptoanalyti-ků (řešení je v dodatku H).

Jak unést knihu kódů

Až dosud jsme si provoz Enigmy popisovali jako jeden obrovský komunikační systém, ale ve skutečnosti šlo o několik oddělených sítí. Například německá armáda v severní Africe měla svou síť, její operátoři Enigmy používali kódové knihy odlišné od těch, jež byly určeny pro Evropu. Pokud se v Bletchley podařilo určit denní klíč pro severní Afriku, bylo možné dešifrovat všechny německé zprávy posílané toho dne ze severní Afriky, ale pro rozluštění zpráv odesílaných v Evropě to nic neznamenalo. Rovněž Luftwaffe měla vlastní komunikační síť, pro

dešifrování její komunikace bylo třeba najít její denní klíč.

Některé sítě byly na rozluštění těžší než jiné. Síť Kriegsmarine byla ze všech nejtěžší, protože německé námořnictvo používalo dokonalejší verzi přístroje Enigma. Operátoři námořní Enigmy měli na výběr z osmi scramblerů, nikoli pouze z pěti, což znamenalo, že existovalo téměř šestkrát více uspořádání scramblerů a tedy téměř šestkrát více klíčů, které museli v Bletchley prověřit. Další odlišnost námořní Enigmy se týkala reflektoru sloužícího k posílání signálů zpět přes scramblery. Ve standardní Enigmě byl reflektor vždy upevněn s určitou orientací, v námořní Enigmě s ním však šlo otáčet a nastavit jej do kterékoli z 26 orientací. Počet možných klíčů se tak dále zvýšil na 26násobek.

Kryptoanalýza námořní Enigmy byla těžší i kvůli operátorům námořnictva, kteří byli pečliví a neposílali stereotypní zprávy, čímž ochuzovali Bletchley o taháky. Kriegsmarine také zavedla bezpečnější systém výběru a vysílání klíčů zprávy. Více scramblerů, pohyblivý reflektor, nestereotypní zprávy a nový systém výměny klíčů zprávy -to vše přispělo k tomu, že německá námořní komunikace byla neproniknutelná.

Neúspěch Bletchley v úsilí rozluštit námořní Enigmu vedl k tomu, že Kriegsmarine postupně získávala převahu v bitvě o Atlantik. Admirál Karl Donitz vyvinul velmi efektivní dvoustupňovou strategii vedení námořní války, která začala tím, že se jeho ponorky rozptýlily a hledaly v Atlantiku spojenecké konvoje. Jakmile jedna z nich zahlédla cíl, zahájila další stadium strategie - přivolala na scénu další ponorku. Útok začal až tehdy, když se shromáždilo více ponorek. Měla-li tato strategie koordinovaného útoku uspět, bylo nezbytné, aby Kriegsmarine měla přístup k bezpečné komunikaci.Námořní Enigma takovou komunikaci poskytovala, a proto měly útoky ponorek devastující účinek na spojenecké loďstvo, jež zásobovalo Británii tolik potřebnými potravinami a výzbrojí.

Dokud komunikace ponorek zůstávala neprostupná, neměli Spojenci představu o rozmístění ponorek a nemohli plánovat bezpečné trasy pro konvoje. Zdálo se, že jedinou strategií Admirality, jak zjistit polohu německých ponorek, je poznačit si místa potopených britských lodí. Mezi červnem 1940 a červnem 1941 ztratili Spojenci v průměru 50 lodí měsíčně a byli vystaveni nebezpečí, že nebudou schopni stavět dostatečně rychle nové lodě. Kromě toho také docházelo k děsivým ztrátám na životech - během války zahynulo na 50 000 spojeneckých námořníků. Pokud by se nepodařilo tyto ztráty výrazně omezit, byla Británie v nebezpečí, že prohraje bitvu o Atlantik, což by vedlo i k prohře celé války. Churchill později píše: „Uprostřed přívalu násilných událostí dominovala všemu jediná obava. Bitvy lze vyhrát nebo prohrát, akce mohou být úspěšné nebo nezdařené, území mohou být dobyta nebo opuštěna, avšak klíč k naší síle pokračovat ve válce nebo dokonce udržet národ naživu spočíval v ovládnutí zaoceánských tras a ve volnému přístupu do našich přístavů."

Polská zkušenost a případ Hans-Thilo Schmidta naučily Bletch-ley Park, že pokud při rozlomení šifry selže intelektuální úsilí, potom je nezbytné se spoléhat na špionáž, infiltraci a krádeže, aby se podařilo získat nepřátelské klíče. Občas Bletchley dosáhl pokroku proti námořní Enigmě díky chytrému triku RAF. Britská

letadla položila miny na dohodnutá místa a tím vyprovokovala německá plavidla k vyslání varovné zprávy dalším plavidlům. Tato varování zašifrovaná Enigmou obsahovala odkaz na mapu, Britové však věděli předem, o jaké souřadnice jde, takže je bylo možné použít jako tahák. Jinými slovy, v Bletchley předem věděli, že určitá část šifrového textu představuje určitou sadu souřadnic. Kladení min kvůli získání taháku, známé jako „zahradničení", vyžadovalo, aby RAF létala na speciální mise, což se nedalo dělat systematicky. V Bletchley museli najít jiný způsob.

Alternativní strategie rozluštění námořní Enigmy vycházela z krádeže klíčů. Jeden z nejsmělejších plánů krádeže klíčů vymyslel lan Fleming, pozdější tvůrce Jamese Bonda, během války pracovník námořní rozvědky. Navrhl fingovanou havárii ukořistěného německého bombardéru v kanálu La Manche poblíž německé lodi. Jeho

lán předpokládal, že se němečtí námořníci přiblíží k letadlu, aby achránili své kamarády, načež se posádka letadla, britští piloti převlečení za Němce, nalodí na německou loď a zmocní se jejich knih kódů. Tyto německé knihy kódů obsahovaly informace nezbytné pro určení šifrovacího klíče, a protože lodě byly často vzdáleny od základny na dlouhé období, kniha kódů by byla platná nejméně měsíc. V Bletchley by tedy mohli dešifrovat námořní Enigmu po celý

měsíc

Po schválení Flemingova plánu, známého jako Operace bezohlednost, začala britská rozvědka připravovat bombardér *Heinkel* na fingovanou havárii a shromažďovat posádku letadla z německy mluvících Angličanů. Plán byl načasován na počátek měsíce, aby se získaly čerstvé knihy kódů. Fleming jel do Doveru dohlížet na celou operaci, ale naneštěstí tam nebyla poblíž žádná německá loď, takže plán bylo třeba odložit na neurčito. O čtyři dny později zaznamenal Frank Birch, který vedl námořní sekci v Bletchley, reakci Turinga a jeho kolegy Petera Twinna: „Turing a Twinn ke mně přišli jako hrobníci, které někdo ošidil o pěkné tělo, rozhořčení zrušením Operace bezohlednost."

Později byla Operace bezohlednost zcela zrušena, ale německé námořní knihy kódů se nakonec podařilo ukořistit díky sérii odvážných přepadení meteorologických lodí a ponorek. Tyto takzvané „córky" dodaly do Bletchley dokumenty nezbytné k dešifrování kódu. Když se podařilo námořní Enigmu rozluštit, v Bletchley mohli přesně určovat polohu ponorek a válka o Atlantik se začala vyvíjet ve prospěch Spojenců. Konvoje mohly být odkloněny, aby se nesetkaly s ponorkami, a britské torpédoborce mohly dokonce zahájit protiponorkovou ofenzivu.

Zásadní význam mělo, aby německé velení nikdy nepojalo podezření, že Spojenci „córli" knihy kódů pro Enigmu. Kdyby Němci zjistili, že jejich bezpečnost byla ohrožena, vylepšili by Enigmu a Bletchley by byl zase na začátku. Stejně jako v případě Zimmer-mannovy telegrafní epizody i nyní Britové podnikli různá bezpečnostní opatření jako třeba potopení německého plavidla po krádeži jeho knih kódů. To přesvědčilo admirála Dónitze, že šifrový materiál není v britských rukou, ale v bezpečí na dně moře.

Další opatření se týkala využití získaných zpravodajských informací. Mohlo se stát, že díky dešifrování sice zjistili Britové polohu mnoha ponorek, ale nebylo by moudré je všechny napadnout, protože náhlé nevysvětlitelné zvýšení britských úspěchů by Němce varovalo, že jejich komunikace již není bezpečná. Proto Spojenci umožnili některým ponorkám uniknout a další napadli pouze tehdy, když nejdříve vyslali výzvědné letadlo a odůvodnili tak přiblížení torpédoborce o několik hodin později. Jindy Spojenci vysílali falešné zprávy popisující pozorování ponorek, jimiž zdůvodnili následný útok.

Navzdory snaze potlačit všechny náznaky toho, že Enigma byla rozluštěna, mezi německými bezpečnostními experty někdy vzbudily britské akce přece jen obavy. Při jedné příležitosti v Bletchley rozšifrovali zprávu udávající přesnou pozici skupiny německých tankerů a zásobovacích lodí, celkem devíti plavidel. Admiralita se rozhodla, aby nevzbudila podezření, nepotopit všechny lodě. Proto informovala své torpédoborce o přesné poloze pouhých sedmi lodí, což umožnilo lodím *Gedania* a *Gonzenbeim* uniknout. Sedm lodí bylo skutečně potopeno, ale torpédoborce Královského námořnictva náhodou narazily i na zbylé dvě lodi, které měly ušetřit, a také je potopily. Torpédoborce nevěděly o Enigmě ani o politice nevzbuzování podezření - pouze se domnívaly, že dělají svou práci. Admirál Kurt Fricke v Berlíně podnítil vyšetřování tohoto a podobných útoků ve snaze prověřit možnost, že Britové rozlomili Enigmu. Vyšetřování došlo k závěru, že početné ztráty byly způsobeny buď náhodou, nebo britským špionem, který infiltroval Kriegsmarine. Rozluštění Enigmy se považovalo za nemožné a nepředstavitelné.

Anonymní kryptoanalytici

Kromě toho, že Bletchley Park rozlomil německou šifru Enigma, uspěl také v dešifrování italských a japonských zpráv. Zpravodajské informace, které vyplynuly z těchto tří zdrojů, dostaly kódové jméno Ultra. Díky nim získali Spojenci výhodu na všech bojištích. V severní Africe pomohla Ultra zničit německé zásobovací linky a informovala Spojence o stavu sil generála Rommela, díky čemuž Osmá armáda odrazila německou ofenzivu. Ultra také varovala před německou invazí do Řecka, což umožnilo britským silám se stáhnout bez těžkých ztrát. Nešlo jen o Řecko; Ultra poskytovala přesné zprávy o situaci nepřítele v celém Středomoří. To bylo obzvlášť důležité ve chvíli, kdy se Spojenci v roce 1943 vyloďovali v Itálii a na Sicílii.

V roce 1944 Ultra sehrála důležitou roli při spojenecké invazi na evropský kontinent. V měsících předcházejících dni D poskytovaly zprávy dešifrované v Bletchley detailní obrázek o rozložení německých vojsk podél francouzského pobřeží. Sir Harry Hinsley, oficiální historik britské rozvědky během války, napsal:

‚Jak se informace ze zdroje Ultra hromadily, došlo k několika nepříjemným překvapením. Konkrétně v druhé polovině května se ukázalo - po předchozích znepokojivých náznacích, že Němci došli k závěru, že oblast mezi Le Havrem a Cherbourgem je pravděpodobným a možná dokonce hlavním cílem invaze - že Němci vyslali posily do Normandie a na Cherbourgský poloostrov. Díky včasné informaci však Spojenci modifikovali plány vylodění na pláži Utah. Zůstává neoddiskutovatelným faktem, že ve chvíli, kdy vyslané vojsko vyrazilo, byl náš

odhad počtu, identity a rozmístění nepřátelských divizí na západě - v celkovém počtu padesáti osmi divizí - přesný ve všech položkách operačního významu kromě dvou."

Během války kryptoanalytici v Bletchley věděli, že jejich práce má velký význam, a Churchillova návštěva Bletchley tento názor potvrdila. Nikdy se však nedověděli žádné podrobnosti strategického charakteru, nikdo jim neřekl, k čemu a jak se jejich informace používají. Nikdo jim například neřekl o dni D, tedy datu vylodění spojenců v Normandii. Náhodou se stalo, že navečer před vyloděním si kryptoanalytici naplánovali taneční večírek. To znepokojovalo velitele Travise, ředitele Bletchley a jedinou osobu široko daleko, která byla zasvěcena do plánu pro den D. Nemohl říct tanečnímu výboru budovy č. 6, aby večírek zrušil, protože by to byla jasná narážka, že na obzoru je důležitá ofenzíva, což by se dalo klasifikovat jako porušení utajení. Večírek byl proto povolen. Náhodou došlo k tomu, že špatné počasí odsunulo vylodění o dvacet čtyři hodin, takže kryptoanalytici měli čas vzpamatovat se z následků veselého večera. V den vylodění francouzský odboj zničil pozemní komunikační linky a přinutil tak Němce komunikovat pouze rádiem, což dalo Bletchley příležitost zachytit a rozšifrovat ještě více zpráv. V tomto klíčovém bodu války tak Bletchley poskytovala ještě detailnější obrázek německých válečných operací než dříve.

Stuart Milner-Barry, jeden z kryptoanalytiků z budovy č. 6, na-P[sa]l: „Myslím, že od starověku - pokud vůbec někdy - se nevedla Jiná válka, v níž by jedna strana měla plně k dispozici informacez druhé strany." Americká zpráva dochází k podobnému závěru: „Ultra vytvořila podmínky, jež změnily rozhodovací proces vojenských a politických špiček. Znát svého nepřítele je velice uklidňující pocit. Roste nepostřehnutelně, ale trvale, pokud pravidelně a podrobně pozorujete jeho myšlenky, způsoby, zvyky a činy. Znalosti tohoto typu umožňují méně improvizovat, plánovat s větší jistotou, bez rizika a rozhodněji."

Existuje kontroverzní tvrzení, že výkony z Bletchley byly rozhodujícím faktorem spojeneckého vítězství. Jisté je, že válku významně zkrátily. Dobře je to vidět, když analyzujeme bitvu o Atlantik a zvažujeme, jak by probíhala, kdyby nebyla k dispozici Ultra. Především by došlo k tomu, že silné německé ponorkové loďstvo by potopilo více spojeneckých lodí. Tím by bylo ohroženo spojení s Amerikou, Spojenci by museli predisponovat lidské zdroje na stavbu nových lodí. Historikové odhadli, že by to pozdrželo spojenecké plány o několik měsíců, což by znamenalo odsunutí invaze ze dne D přinejmenším na následující rok. Podle sira Harryho Hinsleye „válka by skončila v roce 1948 místo v roce 1945, kdyby Government Code and Cypher School nebyla schopna číst šifru Enigma a nepo-skytovala zpravodajské informace Ultra".

Během tohoto prodlení by v Evropě došlo k mnoha dalším ztrátám. Hitler by byl schopen lépe využít střely V-l a V-2 a působit tak škody v jižní Anglii. Historik David Kahn shrnuje význam rozluštění Enigmy: „Zachránilo životy. Nejen spojenecké a ruské životy, ale díky zkrácení války také životy německé, italské a japonské. Někteří lidé, kteří válku přežili, by nebyli naživu, kdyby k rozluštění nedošlo. Za to svět vděčí kryptoanalytikům; to je klíčová lidská hodnota jejich

triumfu."

Po válce zůstaly úspěchy Bletchley důkladně hlídaným tajemstvím. Po úspěšném luštění zpráv během války chtěla Británie pokračovat ve svých výzvědných aktivitách a nebyla ochotna prozradit své schopnosti. Británie získala tisíce přístrojů Enigma, které rozmístila ve svých bývalých koloniích, kde věřili, že šifra je tak bezpečná, jak se zdála Němcům. Britové neudělali nic pro to, aby je vyvedli z omylu, a v následujících letech běžně dešifrovali jejich tajnou komunikaci.

Mezitím byla Government Code and Cypher School v Bletchley Parku zavřena. Tisíce mužů a žen, kteří přispěli k vytvoření Ultra, se rozešli. Bomby byly rozebrány a každý útržek papíru, který se vztahoval k válečným dešifrovacím aktivitám, byl buď zamčen do trezoru nebo spálen. Britské dešifrovací aktivity převzalo nově vzniklé ústředí Government Communication Headquaters (GCHQ) v Londýně, které se v roce 1952 přemístilo do Cheltenhamu. Přestože někteří z kryptoanalytiků přešli ďo GCHQ, většina z nich se vrátila ďo svých civilních životů se závazkem mlčenlivosti, takže svou klíčovou roli ve spojeneckém válečném úsilí nemohli odhalit. Zatímco vojáci, kteří bojovali v konvenčních bitvách, se směli pochlubit svými hrdinskými činy, kryptoanalytici, kteří sváděli intelektuální bitvy s nemenším významem, museli čelit zahanbení, že na otázky o svých válečných aktivitách nemohli oďpovědět jinak než vyhýbavě. Gor-don Welchman vypráví, jak jeden z mladých kryptoanalytiků, který s ním pracoval v budově č. 6, dostal kousavý ďopis od svého bývalého ředitele školy, který jej obviňoval, že je hanbou školy, protože nebyl na frontě. Derek Taunt, který také pracoval v budově č. 6, shrnuje pravý přínos svých kolegů: „No, možná jsme zrovna nebyli s králem Jindrou na den svatého Kryšpína, ale šunky jsme si taky neváleli a nemusíme se vůbec cítit špatně, že jsme byli tam, kďe jsme byli.*"

Po třech desetiletích mlčení nakonec ticho kolem Bletchley Parku v 70. letech 20. století skončilo. Kapitán F. W. Winterbotham, který byl zodpovědný za distribuci informací Ultra, začal naléhat na britskou vládu s argumentem, že země Commonwealthu přestaly používat šifru Enigma a že již není co získat skrýváním faktu, že Británie ji rozlomila. Tajné služby neochotně souhlasily a povolily mu napsat knihu o činnosti Bletchley Parku. Winterbothamova kniha *The Ultra Secret* vydaná v létě 1974 se stala signálem, že bývalí pracovníci Bletchley mohou přinejmenším mluvit o svých válečných aktivitách. Gordon Welchman pocítil velikou úlevu: „Po válce jsem se vyhýbal diskusím o válečných událostech ze strachu, že bych mohl vycházet z informací Ultra a ne z veřejně dostupných zdrojů. Cítil jsem, že tento obrat událostí mě zbavil závazku mlčenlivosti."

Ti, kteří tolik přispěli k válečnému úsilí, mohli nyní obdržet zasloužené uznání. Snad nejpozoruhodnějším důsledkem Winterbo-thamovy knihy bylo to, že si Rejewski uvědomil obrovský důsledek svého předválečného luštění Enigmy. Po německé invazi do Polska Rejewski utekl do Francie, a když byla i Francie obsazena, prchl do

*Narážka na jednu z klíčových scén ze hry *Jindřich V.* od Williama Shakespeara.

Británie. Zdálo by se přirozené, že by se stal součástí britského úsilí o rozluštění Enigmy, ale místo toho byl poslán řešit méně důležité šifry do malé zpravodajské jednotky v Boxmooru u Hemel Hemp-steadu. Není jasné, proč byl tak brilantní mozek vyloučen z Bletch-ley Parku, kvůli tomu však Rejewski nevěděl vůbec nic o aktivitách Government Code and Cypher School. Až do vydání Winterbotha-movy knihy neměl ani tušení, že jeho myšlenky poskytly základ pro rutinní dešifrování Enigmy během války.

Pro někoho vyšly Winterbothamovy knihy příliš pozdě. Mnoho let po smrti Alastaira Dennistona, prvního ředitele Bletchley, obdržela jeho dcera dopis od jednoho z jeho kolegů: „Váš otec byl velký muž, jemuž budou všichni anglicky mluvící lidé dlužni ještě dlouhou dobu, ne-li navždy. Je smutné, že tak málo lidí vědělo přesně, co udělal."

Alan Turing byl dalším kryptoanalytikem, který nežil tak dlouho, aby se dočkal jakéhokoliv veřejného uznání. Místo toho, aby byl vychvalován jako hrdina, byl pronásledován pro svou homosexualitu. Roku 1952, když hlásil vloupání na policii, naivně prozradil, že měl homosexuální vztah. Policie usoudila, že nemá jinou možnost než jej zatknout a obvinit ze „spáchání nemravnosti podle oddílu 11 dodatku Trestního zákona z roku 1885". V denících se objevila zpráva o provinění a soudním stíhání, Turing byl veřejně pokořen.

Turingovo tajemství tak bylo odhaleno, jeho sexuální orientace se stala veřejně známou. Britská vláda zrušila jeho bezpečnostní prověření. Nesměl již pracovat na výzkumných projektech týkajících se rozvoje počítačů. Soud mu nařídil navštěvovat psychiatra a podstoupit hormonální léčení, jehož důsledkem byla impotence a obezita. Turing upadl do depresivních stavů. 7. června 1954 si do ložnice odnesl sklenici kyanidového roztoku a jablko. Před dvaceti lety si prozpěvoval: „Vlož jablko do lektvaru, dej mu sílu smrti, zmaru." Nyní byl připraven uposlechnout. Ponořil jablko do kyanidu a několikrát si kousl. Ve věku pouhých dvaačtyřiceti let jeden ze skutečných géniů kryptoanalýzy spáchal sebevraždu.

5

Jazyková bariéra

Zatímco britští kryptoanalytici luštili německou šifru Enigma a ovlivňovali tak průběh války v Evropě, jejich američtí kolegové měli stejně významný vliv na události v Pacifiku, protože rozluštili japonskou strojovou šifru označenou kódovým názvem Purpur. V červnu roku 1942 Američané například rozluštili zprávu, v níž byl v hrubých rysech načrtnut japonský plán přivábit americké námořní síly k Aleutským ostrovům předstíráním útoku. To by umožnilo japonskému námořnictvu dosáhnout jeho skutečného cíle - Mid-wayských ostrovů. Přestože americké lodě nejprve upadly do léčky a opustily Midway, příliš se nevzdálily. Když američtí kryptoanalytici zachytili a rozluštili japonský příkaz k útoku na Midwayské ostrovy, lodě byly schopny se pohotově vrátit a bránit ostrov v jedné z nejdůležitějších bitev války v Pacifiku. Podle admirála Chestera Nimitze americké vítězství u Midway „bylo ve své podstatě vítězstvím výzvědných služeb.

Sami Japonci, kteří se pokoušeli překvapit, byli nakonec překvapeni".

Téměř o rok později američtí kryptoanalytici identifikovali zprávu, která zachycovala plán cesty admirála Isoruko Yamamoto, velitele japonského loďstva, na severní Salamounovy ostrovy. Nimitz rozhodl vyslat stíhačky, aby zkřížily Yamamotovu trasu a sestřelily jeho stroj. Yamamoto, proslulý svou chorobnou přesností, se přiblížil ke svému cíli přesně v 8.00, jak to stálo v zachyceném časovém rozvrhu. Tam na něj čekalo 18 amerických bojových letounů P-38, kterým se podařilo zabít jednu z nejvlivnějších postav japonského vrchního velení.

Přestože byly japonské a německé šifry Purpur a Enigma nakonec rozlomeny, poskytly zpočátku stoprocentní bezpečnost a pro americké a britské kryptoanalytiky představovaly velkou výzvu. Kdyby byly šifrovací přístroje užívány správně - tedy bez opakování klíčů zprávy (message keys), bez cilek (cillies), bez omezení v nastavení propojovací desky a scramblerů, bez stereotypních zpráv,ze kterých se staly taháky - je docela dobře možné, že by je nikdo nerozlomil.

Opravdová síla a potenciál šifrovacích přístrojů byly demonstrovány přístrojem Typex (někdy též Type X), šifrovacím strojem používaným britskou armádou a letectvem, a strojem SIGABA (neboli M-143-C), který vlastnily americké vojenské síly. Oba tyto přístroje byly složitější než Enigma a oba byly používány správně, a proto zůstaly nepřekonány po celou válku. Spojenečtí kryptografové spoléhali na to, že komplikované elektromechanické šifrovací přístroje zaručí bezpečnou komunikaci. Nicméně komplikované šifrovací přístroje nejsou jediným způsobem, jak posílat bezpečné zprávy. Jedna z nejbezpečnějších forem šifrování, která se používala během druhé světové války, byla také jednou z nejjednodušších.

Během války v Tichomoří si američtí velitelé začali uvědomovat, že šifrovací stroje jako SIGABA mají jeden zásadní nedostatek. Přestože elektromechanické šifrování poskytovalo poměrně vysokou úroveň bezpečnosti, bylo bolestně pomalé. Zprávy bylo nutno vyťukat do stroje písmeno po písmeni, také výsledek bylo nezbytné zapsat stejným způsobem a nakonec musel být hotový zašifrovaný text odeslán radistou. Radista příjemce musel zašifrovanou zprávu předat expertovi na šifry, který pečlivě vybral správný klíč, naťukal zašifrovaný text do šifrovacího přístroje a dešifroval jej opět písmeno po písmeni. Čas a prostor, požadovaný pro tuto delikátní operaci, byl sice k dispozici na velitelství nebo na palubě lodi, ale šifrování pomocí přístrojů nebylo praktické pro nebezpečnější a exponovanější prostředí, jakými byly například tichomořské ostrovy. Jeden válečný zpravodaj popsal potíže s komunikací v žáru boje v džungli: „Když se boje začaly omezovat na malý prostor, všechno se muselo dít ve zlomcích vteřin. Na šifrování a dešifrování nebyl čas. V této chvíli se posledním útočištěm stal slang, čím sprostší, tím lepší." Bohužel pro Američany mnozí japonští vojáci chodili do amerických škol a mluvili plynně anglicky včetně vulgárních výrazů. Hodnotné poznatky o americké strategii a taktice se tak dostávaly do rukou nepřátel.

Jeden z prvních, který reagoval na tento problém, byl Philip Johnston, inženýr z Los Angeles, který byl příliš starý na to, aby mohl bojovat, ale přesto chtěl přispět k porážce nacistů. Na začátku roku 1942 začal formulovat šifrovací systém

inspirovaný svými dětskými zážitky. Johnston, syn protestantského misionáře, vyrůstal

v navažské rezervaci v Arizoně a byl znalcem kultury Navahů. Byl jedním z mála lidí mimo kmen, který dokázal plynně hovořit jejich jazykem, což mu umožňovalo tlumočit rozhovory mezi Navahy a zástupci vlády. Vrcholem jeho dovedností byla návštěva v Bílém domě, kde - jako devítiletý - překládal pro dva Navahy, kteří požadovali po prezidentovi Theodoru Rooseveltovi korektnější zacházení s jejich komunitou. Johnston si byl plně vědom toho, jak je navažský jazyk pro ostatní lidi neproniknutelný, a proto ho napadlo, že by jazyk Kavahů nebo jiných původních obyvatel Ameriky mohl fungovat jako skutečně nerozlomitelný kód. Kdyby každý tichomořský prapor disponoval dvojicí domorodých Američanů - radistů, bezpečná komunikace by byla zaručena.

Johnston se obrátil se svým nápadem na podplukovníka Jamese E. Jonese, velitele pro komunikaci v Camp Elliot poblíž San Diega. Stačilo prohodit pár navažských vět ke zmatenému důstojníkovi a Johnston jej dokázal přesvědčit, že tento nápad stojí za důkladné uvážení. O čtrnáct dní později se vrátil se dvěma Navahy, připravený provést zkušební demonstraci před vyššími důstojníky námořnictva. Navahové byli navzájem izolováni. Jeden z indiánů dostal šest typických zpráv v angličtině, které přeložil do navažštiny a rádiem poslal svému kolegovi. Ten je přeložil zpět do angličtiny, zapsal a předal důstojníkům, kteří je porovnali s originálem. Navaž-ská tichá pošta se ukázala být bez jediné skulinky, proto důstojníci námořnictva schválili pilotní projekt a nařídili, aby neodkladně začal nábor.

Podplukovník Jones a Philip Johnston se museli předtím, než kohokoliv najali, rozhodnout, jestli povedou pilotní studii s Navahy, nebo vyberou jiný kmen. Johnston při své původní ukázce spolupracoval s Navahy, protože s jejich kmenem měl osobní kontakty, ale to z nich nutně nedělalo ideální volbu. Nejdůležitější kritérium výběru byla jednoduše otázka počtu: námořnictvo potřebovalo najít kmen, jenž by byl schopný poskytnout velké množství mužů, kteří by mluvili plynně anglicky a zároveň byli gramotní. Nedostatek vládních investic znamenal, že ve většině *rezervací* byla míra gramotnosti velmi nízká, a proto soustředili pozornost na čtyři největší kmeny: Navahy, Siouxe, Chippewa a Pima-Papago.

Navahové byli největším kmenem, ale zároveň nejméně gramotným, zatímco příslušníci Pima-Papago měli nejvyšší gramotnost, i když jich bylo nejméně. Mezi čtyřmi kmeny bylo těžké vybrat tenpravý, nakonec se však základem rozhodnutí stal jiný důležitý faktor. Oficiální zpráva o Johnstonově nápadu říká:

„Navahové byli jediným kmenem ve Spojených státech, který nebyl in-filtrován během posledních dvaceti let německými studenty. Tito Němci, studující různé kmenové dialekty pod maskou studentů umění, antropologů a podobně, nepochybně získali dobré znalosti všech kmenových dialektů s výjimkou navažského. Proto byli Navahové jediným vhodným kmenem, poskytujícím naprostou bezpečnost pro tento typ požadované práce. Je třeba se také zmínit o faktu, že navažský kmenový dialekt je naprosto nesrozumitelný jiným kmenům a všem ostatním lidem, snad jen s výjimkou 28 Američanů, kteří tento dialekt studovali. Navažština představuje pro nepřítele tajný kód, který je obdivuhodně vhodný pro rychlou a bezpečnou komunikaci."

V době vstupu Ameriky do druhé světové války žili Navahové v drsných podmínkách a *zacházelo* se s nimi jako s podřadnými lidmi. Přesto jejich kmenová

rada podporovala Američany ve válce a vyjádřila jim loajalitu: „Neexistuje čistší koncentrace amerikanis-mu, než jaká je mezi Prvními Američany." Navahové byli tak dychtiví bojovat, že někteří z nich lhali o svém věku nebo se nacpávali trsy banánů a polykali velké množství vody, aby dosáhli požadavku minimální odvodní váhy 55 kg. Stejně tak nebyl žádný problém najít vhodné kandidáty pro navažské mluvčí kódu, což je název funkce, díky níž se později stali známými. Během čtyř měsíců od bombardování Pearl Harboru zahájilo 29 Navahů, někteří teprve patnáctiletí, osmitýdenní kurs v komunikaci u námořnictva.

Než mohl výcvik začít, musely námořní síly překonat problém, jenž se projevil u jediného dalšího kódu, který byl kdy založen na jazyku původních Američanů. Kapitán E. W. Horner z roty D 141. pěšího pluku v severní Francii během první světové války rozkázal, aby bylo osm mužů z kmene Choctaw převeleno do funkce radistů. Jejich jazyku samozřejmě nikdo z nepřátel nerozuměl, a tak Choc-tawové umožňovali bezpečnou komunikaci. Nicméně šifrovací systém měl zásadní vadu, protože jazyk Choctawů neměl ekvivalenty pro moderní vojenské termíny. Proto musely být specifické technické výrazy v depeších přeloženy neurčitým výrazem - s tím rizikem, že je příjemce zprávy bude špatně interpretovat.

Stejný problém se vyskytl s navažským jazykem, ale námořnictvo rozhodlo vytvořit slovník navažských termínů, které by nahradily

jinak nepřeložitelná anglická slova a vyloučily tak jejich dvojznačnost. Účastníci kursu pomáhali sestavovat slovník a zejména pomo-$_{c}${ výrazů z oblasti přírody nahrazovali vojenskou terminologii. Jména ptáků tak byla použita pro letadla a jména ryb pro lodě (viz tabulka 11). Velitelé se stali „válečnými náčelníky", četa „bahenní partou", zákopy byly pojmenovány „jeskynními příbytky" a mino-tnety byly označeny jako „zbraně, které sedí na bobku".

Přestože kompletní slovník obsahoval 274 slov, stále tu zůstával problém, jak přeložit méně předvídatelná slova a jména lidí a míst. Řešením bylo vynalézt zakódovanou fonetickou abecedu pro hláskování složitých slov. Například slovo Pacific by se hláskovalo jako nig, ant, cat, ice, fox, ice, cat" („prase, mravenec, kočka, led, liška, led, kočka" - pozn. překl.), což by se přeložilo do navažštiny jako b1-sod1h, wol-la-chee, raoasi, tkln, ma-e, tkln,moasi. Kompletní navažská abeceda je uvedena v tabulce 12. Za osm týdnů se účastníci kursu naučili celý slovník a abecedu a odstranili tak potřebu knihy kódů, která by mohla padnout nepříteli do rukou. Pro Navahy bylo jednoduché naučit se všechno nazpaměť, protože jejich jazyk neměl tradičně žádnou psanou formu, a tak byli zvyklí učit se zpaměti svým pohádkám a rodinným příběhům. Jak řekl jeden z frekventantů kursu William McCabe: „V navažštině je všechno ukryto v paměti -písně, modlitby, prostě všechno. Tak jsme byli vychováni."

Na konci výcviku byli Navahové podrobeni testu. Odesilatelé přeložili sérii zpráv z angličtiny do navažštiny, poslali je a příjemci, který je přeložil zpět do angličtiny s pomocí naučeného slovníku a v případě potřeby prostřednictvím speciální abecedy. Výsledky byly bezchybné. Aby námořnictvo ověřilo sílu systému, předalo na-

Bojové letadlo	Kolibřík	Da-he-tih-h1

Výzvědné letadlo	Sova	Ne-as-jah
Torpédové letadlo	Vlaštovka	Tas-ch1zz1e
Bombardér	Káně	Jay-sho
Protiponorkový bombardér	Mládě jestřába	G1n1
Bomby	Vejce	A-ye-shi
Obojživelné vozidlo	Žába	Chal
Válečná loď	Velryba	Lo-tso
Torpédoborec	Žralok	Ca-lo
Ponorka	*Železní* ryba	Besh-lo

abulka 11: Navažská kódová slova pro letadla a lodě.

A	Ant (mravenec)	Wol-la-chee	N	Nut (ořech)	Nesh-chee
	Bear (medvěd)	Shush	0	Owl (sova)	Ne-ahs-Jsh
	Cat (kočka)	Moasi	P	Pig (prase)	Bi-sodih

Deer (jelen)	Be	Q	Quiver (toulec)	Ca-yellth
Elk (los)	Dzeh	R	Rabbit (králík)	Gah
Fox (liška)	Ma-e	S	Sheep (ovce)	Dibeh
Goat (koza)	KUzzle	T	Turkey (krůta)	Than-z1e
Horše (kůň)	L1n	U	Ute (Šošon)	No-da-1h
Ice (led)	Tk1n	V	Victor (vítěz)	A-keh-d1-gl1n1
Jackass (osel)	Kele-cho-g1	W	Weasel (lasička)	Gloe-1h
Kid (kůzle)	Kl1zz1e-yazz1	X	Cross (kříž)	Al-an-as-dzoh
Lamb (jehně)	D1beh-yazz1	Y	Yucca (juka)	Tsah-as-z1h
Mouše (myš)	Na-as-tso-si	Z	Zinc (zinek)	Besh-do-gl1z

Tabulka 12: Navažský kód pro abecedu.

hrávku vysílání do zpravodajského oddělení - do jednotky, která rozluštila Purple, nejtěžší japonskou šifru. Po třech týdnech intenzivní kryptoanalýzy byli námořní analytici stále ještě zmateni. Navažský jazyk nazvali „podivnou posloupností hrdelních, nosových a jazykolomných zvuků... nemohli jsme je ani přepsat, natož rozlomit kód". Navažský kód byl ohodnocen jako úspěšný. Dva navažští vojáci John Benally ajohnny Manuelito byli určeni, aby zůstali a cvičili další várku rekrutů, zatímco ostatních 27 navažských mluvčích kódu bylo přiděleno ke čtyřem plukům a posláno do Tichomoří.

Japonské síly zaútočily na Pearl Harbor 7. prosince 1941 a zanedlouho ovládly větší část západního Tichomoří. Japonské jednotky obsadily 10. prosince americkou posádku v Guamu, 13. prosince zabraly Guadalcanal, jeden z ostrovů Šalamounova souostroví, Hong Kong kapituloval 25. prosince a americké jednotky na Filipínách se vzdaly 2. ledna 1942. Následujícího léta chtěli Japonci upevnit svou kontrolu nad Tichomořím zbudováním letiště na Gua-dalcanalu, čímž by vytvořili základnu pro bombardéry, kterými by zničili spojenecké zásobovací trasy a prakticky znemožnili protiútok Spojenců. Admirál Ernest King, velitel amerických námořních operací, považoval za nezbytné zaútočit na ostrov ještě před dokončením letiště. 7. dubna stála První námořní divize v čele invaze na Guadalcanal. Mezi prvními, kdo se vylodili, byli i Navahové, aby se ukázalo, jak se záměr Američanů osvědčí.

Přestože Navahové věřili, že jejich dovednosti budou pro námořnictvo požehnáním, jejich první pokusy vedly ke zmatku. Mnozí

radisté o novém kódu nevěděli a po celém ostrově rozesílali panické zprávy, že Japonci vysílají na amerických frekvencích. Plukovník velící operaci nechal okamžitě zastavit navažskou komunikaci, dokud se nepřesvědčil, že má smysl pokračovat. Jeden z mluvčích kódu vzpomíná, jak se to stalo:

„Plukovník dostal nápad. Řekl, že nás ponechá ve službě pod jednou podmínkou: pokud dokážu být výkonnější než jeho ‚bílý kód' - mechanická věc ve tvaru válce. Oba jsme poslali zprávy, bílým válcem a mým hlasem. Oba jsme obdrželi odpovědi a závodili jsme v tom, kdo rozluští svou odpověď jako první. Zeptal se mě: Jak dlouho ti to bude trvat? Dvě hodiny?' a já odpověděl: ‚Spíše dvě minuty.' Druhý muž ještě stále luštil, když mi potvrdili příjem mé zpáteční zprávy. Trvalo to čtyři a půl minuty. Řekl jsem: ‚Pane plukovníku, kdy vzdáte tu věc s tím válcem?' Nic neřekl. Jenom si zapálil dýmku a odkráčel pryč."

Mluvčí kódu se brzy osvědčili i v boji. Během jedné etapy války na ostrově Saipan obsadil prapor námořníků pozice předtím držené japonskými vojáky, kteří se stáhli. Najednou se ozvala blízko sal-va. Námořníci se dostali pod palbu vlastních amerických jednotek, které nevěděly o jejich postupu. Napadení vojáci volali rádiem a anglicky vysvětlovali své postavení, přesto palba pokračovala, protože útočící americké jednotky je podezřívaly, že zprávy pocházejí od japonských vojáků, kteří se je snaží zmást. Až když námořníci poslali zprávu v navažštině, útočníci pochopili svou chybu a zastavili útok. Navažská zpráva nemohla být zfalšována a vždy se jí dalo věřit.

Reputace mluvčích kódu se brzy rozšířila a koncem roku 1942 žádaly bojové jednotky o dalších 83 mužů. Navahové sloužili ve všech šesti námořních divizích a jejich služby byly někdy využívány dalšími americkými silami.Válka slov brzy proslavila Navahy jako hrdiny. Ostatní vojáci jim často nabízeli, že ponesou jejich rádia a zbraně, a někdy měli i osobní strážce, částečně i pro ochranu proti vlastním spolubojovníkům. Nejméně ve třech případech byli mluvčí kódu chybně považováni za japonské vojáky a zajati Američany. Pustili je až tehdy, když se za ně zaručili kolegové z jejich vlastní jednotky.

Neproniknutelnost navažského kódu byla dána tím, že navažšti-na patří do skupiny jazyků Na-Dene, která není spojena s žádným asijským nebo evropským jazykem. Například navažská slovesa se nečasují jen podle podmětu, ale i předmětu. Zakončení slovesa závisí na tom, do jaké kategorie předmět spadá: jestli je dlouhý (např. dýmka, tužka), tenký a ohebný (např. had, řemen), sypký (např. cukr, sůl), v hromádce (např. seno), mazlavý (bahno, výkaly) a mnoho dalších. Sloveso v sobě zahrnuje i příslovce a odráží také to, zda má mluvčí osobní zkušenost s tím, o čem mluví, nebo zda o tom jen slyšel. V důsledku toho může jediné navažské sloveso odpovídat celé anglické větě a pro cizince je tedy naprosto nemožné rozluštit jeho význam.

Přes svou sílu trpěl navažský kód dvěma význačnými vadami. Za prvé slova, která nebyla ani v původním navažském slovníku, ani v seznamu 274 povolených kódových slov, musela být hláskována za použití speciální abecedy. To bylo časově velmi náročné, a proto padlo rozhodnutí přidat do slovníku dalších 234 obecných slov. Například státy dostaly navažské přezdívky: „Houpavý klobouk" pro Austrálii, „Spoutaný vodou" pro Británii, „Spletené vlasy" pro Čínu, „Železný klobouk" pro Německo, „Plovoucí země" pro Filipíny a „Bolavá ovce" pro Španělsko.

Druhý problém se týkal těch slov, jež bylo nezbytné i přes tato opatření

hláskovat. Pokud by Japoncům došlo, že jde o hláskování,

mohli by si uvědomit, že lze použít frekvenční analýzu k určení, které navažské slovo představuje které písmeno. Brzy by bylo zřejmé, že nejužívanější slovo je d z e h, které znamená los a představuje e, nejužívanější písmeno anglické abecedy. Pouhé hláskování jména ostrova Guadalcanal a čtyřikrát opakování slova wol-la-chee (mravenec) by bylo cennou nápovědou k tomu, které slovo představuje písmeno a. Řešením bylo přidání více slov, která nahrazovala často používaná písmena. Navíc byla zavedena dvě slova jako alternativy ke každému z šesti nejpoužívanějších písmen (e, t, a, o, i, n) a jedno slovo pro dalších šest nejpoužívanějších písmen (s, h, r, d, 1, u). Například písmeno a mohlo být nahrazeno slovem be-la-sana (jablko) nebo tse-n1 hl (sekera). Guadalcanal se potom mohlo hláskovat s pouhým jedním opakováním: klizzie, shi-da, wol-la-chee, lha-cha-eh, be-la-sana, dibeh-yazzie, moasi, tse-n1hl, nesh-chee, tse-nihl, ah-jad (koza, strýc, mravenec, pes, jablko, jehně, kočka, sekera, oříšek, sekera, noha).

S růstem intenzity bojů v Tichomoří a s americkým postupem ze Salamounových ostrovů k Okinawě hráli navažští mluvčí kódu stá-le důležitější roli. Během prvních dnů útoku na Iwo Jima bylo posláno více než 800 navažských zpráv, všechny bezchybně. Podle ge-nerálmajora Howarda Connera „bez Navahů by námořníci nikdy neobsadili Iwo Jimu". Přínos navažských mluvčích kódu je ještě pozoruhodnější, když vezmeme do úvahy, že kvůli splnění své povinnosti museli čelit a vzdorovat svým hluboce zakořeněným obavám, které vyplývaly z jejich spirituálního založení. Navahové věří, že duše mrtvých *chindi* se bude mstít na živých, pokud se nad mrtvým tělem nevykonají předepsané obřady. Válka v Pacifiku byla zvláště krvavá, s těly roztroušenými po bojišti, a přesto mluvčí kódu vždy sebrali odvahu pokračovat bez ohledu na *chindi*, kteří je strašili. V knize *The Navajo Code Talkers* (Navažští mluvčí kódu) od Doris Paulové si jeden z Navahů vzpomíná na příhodu, jež je typická pro jejich odvahu, oddanost a soustředění:

„Když člověk zvedl hlavu jen o nějakých patnáct čísel, v tu ránu bylo po něm, tak byla střelba prudká. A potom někdy nad ránem to zničehonic na chvíli přestalo. Do té doby jsme se nezastavili ani my, ani oni. Jeden Japonec to ticho asi nevydržel, vyskočil, začal řvát a ječet a vrhl se k našemu zákopu s dlouhým samurajským mečem. Naši do něho museli našít pětadvacet kulek, možná čtyřicet, než padnul.

Vedle mě v zákopu byl kámoš a ten Japonec mu mečem podřízl krk, dočista celej. Chvíli ještě zkoušel popadnout dech s podříznutým hrdlem. Ten zvuk byl hroznej, jak zkoušel dýchat. No, umřel, co jinýho. Když Japončík padnul, jeho teplá krev mi polila ruce. Držel jsem v nich mikrofon a volal jsem pak o pomoc, v kódu. Řekli mi pak, že i když to bylo v takový situaci, rozuměli úplně zřetelně každý mý slabice."

Navažských mluvčích kódu bylo celkem dvě stě čtyřicet. Přestože byla oceňována jejich odvaha bojovníků, jejich speciální role v zabezpečování komunikace byla utajena.Vláda jim zakázala mluvit o vlastní práci a jejich výjimečný přínos nebyl zveřejněn. Stejně jako Turing a kryptoanalytikové z Bletchley Park i Navahové byli po desetiletí neznámí. Teprve v roce 1968 byl

navažský kód odtajněn a následujícího roku se mluvčí kódu poprvé od konce války setkali. Ocenění se jim dostalo roku 1982, kdy americká vláda vyhlásila 14. srpen Národním dnem navažských mluvčích kódu. Největší poctou práci Navahů však byla jednoduše skutečnost, že jejich kód je jeden z velmi mála kódů v celé historii, který nebyl nikdy prolomen. Šéf japonské rozvědky generálporučík Seizo Arisue připustil, že

jeho organizace sice dokázala rozluštit kód amerického letectva, avšak s navažským kódem si nikdy neporadila.

Luštění ztracených jazyků a starých písem

Úspěch navažského kódu spočíval do značné míry v tom, že mateřský jazyk jedné osoby je naprosto nesrozumitelný tomu, kdo s ním není obeznámen. Úloha, jíž čelili japonští kryptoanalytici, byla v mnoha směrech podobná té, před níž stáli archeologové, snažící se rozluštit dávno zapomenuté jazyky, které byly někdy zapsané písmem již dlouho nepoužívaným. Úkol archeologů je dokonce ještě náročnější. Zatímco Japonci měli k dispozici souvislý proud navažských slov, jež se mohli pokusit identifikovat, veškerými informacemi, které měli k dispozici archeologové, byly někdy jen malé sbírky hliněných tabulek. Archeologičtí luštitelé kódů navíc často neměli představu o kontextu nebo obsahu starých textů, chyběla jim tedy nápověda, na kterou se vojenští kryptoanalytici mohli spolehnout.

Luštění starých textů vypadá jako téměř beznadějný úkol, přesto se mnoho mužů a žen zasvětilo tomuto svízelnému podniku. Jejich posedlost byla hnána touhou porozumět písemným památkám našich předků, přáním, jehož splnění by nám umožnilo porozumět jejich slovům a zachytit záblesk dávných myšlenek a životů. Touhu po rozlomení dávných šifer asi nejlépe shrnul Maurice Pope, autor *The Story ofDeciphrement* (Příběhu o rozluštění): „Rozluštění je zdaleka nejlákavějším úspěchem, jehož může vědec dosáhnout. Neznámé texty v sobě mají cosi magického, zvláště pokud pocházejí ze vzdálené minulosti. Osobě, jež jejich tajemství vyluští, bezpochyby patří odpovídající sláva."

Rozluštění starých textů není součástí neutuchajícího zápasu mezi kryptografy a kryptoanalytiky. Máme zde totiž luštitelé - archeology - ale žádné kryptografy. Ve většině případů starých textů nejde o záměrný pokus původního písaře zakrýt jeho smysl. Zbytek této kapitoly, jež se zabývá rozborem starodávných písem, je tudíž určitou odbočkou od hlavního tématu knihy. Principy luštění dávných nápisů jsou však v podstatě tytéž jako u konvenční vojenské kryptoanalýzy. Mnozí vojenští kryptoanalytici byli také skutečně Přitahováni výzvou rozluštit starý text - pravděpodobně proto, žerozbor starého písma byl osvěžující změnou oproti vojenské kryp-toanalýze, nabízel totiž čistě intelektuální hádanku, nikoli vojenskou výzvu. Jinými slovy, motivací byla v jejich případě spíše zvědavost než nenávist.

Nejproslulejší a bezpochyby nejromantičtější ze všech takových rozluštění bylo prolomení egyptských hieroglyfů. Hieroglyfy zůstávaly po staletí záhadou a archeologové nemohli dělat více než spekulovat o jejich významu. Přesto byly hieroglyfy díky klasické analytické práci nakonec rozluštěny a od té doby mohou archeologové číst z první ruky zprávy o historii, kultuře a víře starých Egypťanů. Rozluštění hieroglyfů přemostilo tisíciletí mezi námi a civilizací faraónů.

Nejstarší hieroglyfy se datují do roku 3000 př. n. 1. Tato forma zdobné plastiky přetrvala po následujících tři a půl tisíce let. Propracované symboly hieroglyfů byly vhodné pro zdi majestátných chrámů (řecké slovo *bieroglyphia* znamená „posvátná plastika"), byly však příliš složité, než aby se hodily i pro každodenní záznamy. Proto se souběžně s hieroglyfy vyvíjela *bieratika,* běžné písmo, v němž byly hieroglyfy nahrazeny zástupnými znaky, jež se zapisovaly rychleji a snáze. Okolo roku 600 př. n. 1. byla hieratika nahrazena ještě jednodušším písmem známým jako *démotika,]ehoi* název byl odvozen ze stejně znějícího řeckého slova s významem „lidový", který odráží jeho světskou funkci. Hieroglyfy, hieratika a démotika jsou v zásadě stejné písmo - dnes bychom řekli, že jde jen o vzájemně odlišné fonty.

Všechny tři formy písma jsou fonetické, což znamená, že znaky do značné míry představují jednotlivé zvuky, přesně jako písmena v anglické abecedě. Po více než tři tisíce let používali staří Egypťané tyto formy písma ve všech oblastech svého života, stejně jako my používáme dnešní písmo. Potom ke konci 4. století n. 1., během jedné generace, egyptské písmo zmizelo. Poslední datované příklady starého egyptského písma byly nalezeny na ostrově Philae. Chrámový hieroglyfický nápis byl vytesán v roce 394 n. 1. a část textu vyrytá na zeď v démotickém písmu pochází z roku 450 n. 1. Příčinou vymizení egyptského písma bylo rozšíření křesťanství. Církev postavila jeho používání mimo zákon, aby vykořenila jakékoli spojení s egyptskou pohanskou minulostí. Stará písma byla nahrazena koptštinou, písmem skládajícím se z 24 písmen řecké abecedy doplněných o šest znaků z démotiky pro egyptské hlásky, které v řečtině neexistovaly. Převaha koptštiny byla tak výrazná, že schopnost číst hieroglyfy,

démotiku a hieratiku vymizela. Staroegyptština nadále přetrvala jako mluvená řeč, i když se postupně vyvinula v jazyk, který dnes označujeme jako koptštinu. Postupem času - když se v 11. století rozšířila v této oblasti arabština - však koptský jazyk i písmo vymizely. Poslední jazyková vazba se starými egyptskými královskými říšemi padla a znalosti potřebné ke čtení faraónských příběhů byly ztraceny.

Zájem o hieroglyfy se znovu probudil v 17. století, když papež Sixtus V. reorganizoval Řím: dal vystavět novou síť ulic a na každé křižovatce nechal vztyčit obelisk dovezený z Egypta. Učenci se pokoušeli rozluštit smysl hieroglyfů na obeliscích, ale vycházeli z mylného předpokladu: nikdo nebyl připraven přijmout, že hieroglyfy představují fonetické znaky neboli *fonogramy.* Mělo se za to, že starověká civilizace nemohla vyvinout moderní fonetické písmo. Místo toho byli učenci 17. století přesvědčeni, že hieroglyfy byly *piktogramy* - že tyto složité znaky představovaly celé pojmy, a nebyly tedy ničím jiným než primitivním obrázkovým písmem. Tomu běžně věřili i cizinci, kteří navštívili Egypt v době, kdy byly hieroglyfy ještě živým písmem. Diodorus Siculus, řecký historik v 1. století př. n. 1., napsal:

‚Je tomu tak, že podoby egyptských písmen berou na sebe tvary všemožných druhů živých stvoření a okončetin lidského těla a náčiní... Proto jejich písmo nevyjadřuje myšlenku kombinací slabik, jedna s druhou, ale vnější podobností s tím, co kresba kopíruje a co je formou metafory vtisknuto do paměti cvikem... Tak

jestřáb symbolizuje jim všechno, co se děje rychle, protože toto stvoření je nejrychlejším z okřídlených živočichů. A tato idea se přenáší odpovídající metaforou na všechny hbité věci a na ty tvory, ke kterým rychlost patří."

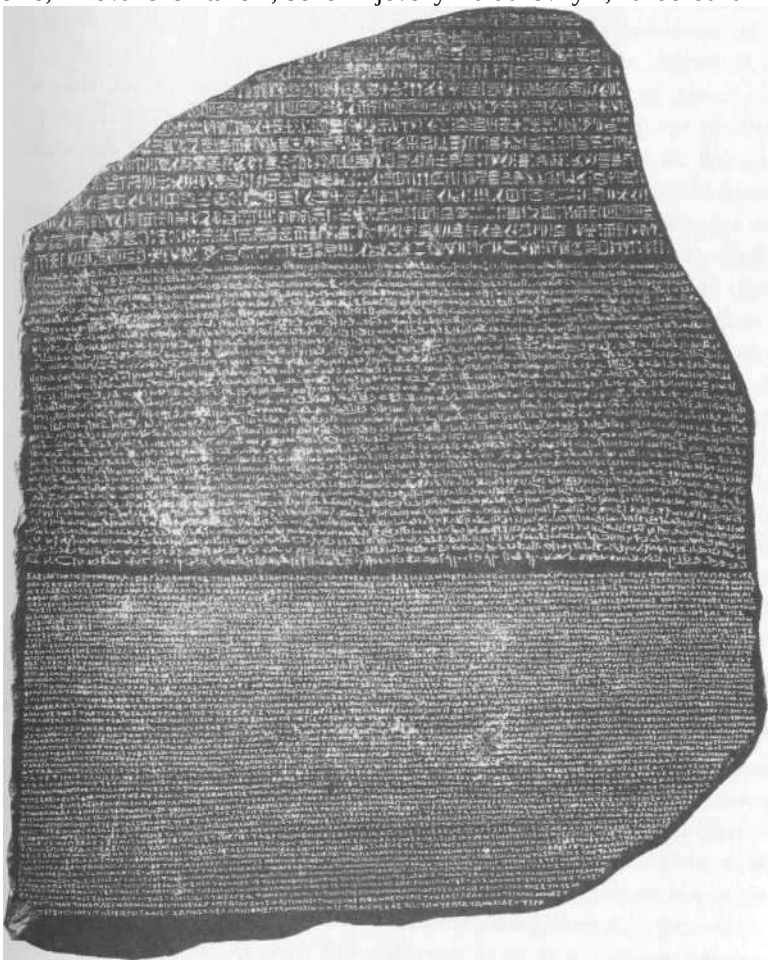
Ve světle takového úsudku možná není tak překvapující, že se učenci 17. století pokoušeli vyluštit hieroglyfy tím, že každý z nich interpretovali jako ucelený pojem. Například v roce 1652 německý jezuitský kněz Athanasius Kircher vydal slovník alegorických výkladů nazvaný *Oedipus aegyptiacus* a použil jej k vytvoření řady bláznivých a kouzelných překladů. Několik hieroglyfů, které, jak nyní víme, představují pouze jméno faraóna Apriese, přeložil Kircher jako: „dobrodiní božského Osirise má se získat pomocí svatých obřadů a řady božstev tak, aby prospěch z Nilu mohl být obdržen". Dnes se Kircherovy překlady zdají směšné, ale jejich dopad na dalšípotenciální luštitele byl obrovský. Kircher byl víc než egyptolog, napsal také knihu o kryptografii, zkonstruoval hudební fontánu, vynalezl magickou lampu (předchůdce kinematografu), spustil se do kráteru Vesuvu a získal tak titul „otec vulkanologie". Tento jezuita byl široce uznáván jako nejrespektovanější učenec své doby, takže jeho myšlenky měly na generace budoucích egyptologů velký vliv.

Půldruhého století po Kircherovi, v létě roku 1798, se památky starého Egypta znovu dostaly do centra pozornosti, když Napoleon Bonaparte vyslal tým historiků, vědců a kreslířů, aby bezprostředně následovali jeho invazní armádu. Tito učenci (neboli „pekinézové", jak jim říkali vojáci) udělali pozoruhodný kus práce při mapování, kreslení, přepisování, měření a zapisování všeho, čeho byli svědky. V roce 1799 narazili na nejslavnější kus kamene v historii archeologie. Francouzští vojáci z Fort Julien jej nalezli ve městě Rosetta v nilské deltě. Vojáci měli za úkol zbořit starou zeď, aby vyčistili cestu pro rozšíření pevnosti. Do zdi byl zabudován kámen, který nesl pozoruhodný soubor nápisů. Stejný text byl na kameni napsán třikrát: v řečtině, démotickým písmem a hieroglyfy. Rosettská deska, což je název, pod nímž se proslavila, se ukázala být ekvivalentem kryptoa-nalytické nápovědy - přesně jako nápovědy, jež pomohly analytikům v Bletchey Parku prolomit Enigmu. Snadno srozumitelná řečtina byla prakticky vzato otevřený text, který bylo možné porovnat s dé-motickou a hieroglyfickou šifrou. Rosettská deska byla potenciální prostředek k rozluštění významu starých egyptských symbolů.

Vědci ihned rozpoznali význam kamene a poslali jej na podrobnější prozkoumání do Národního institutu v Káhiře. Než se však institut mohl pustit do serióznějšího výzkumu, ocitla se francouzská armáda na pokraji porážky postupujícími britskými jednotkami. Francouzi přemístili Rosettskou desku z Káhiry do relativního bezpečí Alexandrie. Ironie osudu však způsobila, že když se Francouzi vzdali, na základě článku XVI Dohody o kapitulaci byly všechny památky v Alexandrii předány Britům, zatímco památky umístěné v Káhiře se mohly vrátit do Francie. Roku 1802 se deska černého čediče, jejíž hodnotu nelze vyčíslit (měří 118 cm na výšku, 77 cm na šířku a její tloušťka je 30 cm, váží tři čtvrtě tuny), vydala na palubě válečné lodi *UEgyptienne* do Portsmouthu a později téhož roku byla umístěna v Britském muzeu v Londýně, kde se nachází dodnes.

Překlad řeckého textu brzy odhalil, že Rosettská deska obsahuje nařízení

všeobecného shromáždění egyptských kněží, jež bylo vydáno v roce 196 př. n. 1. Text zaznamenává výsady, které faraón Ptolemaios udělil egyptskému lidu, a podrobně vyjmenovává pocty, které mají na oplátku kněží poskytnout faraónovi. Uvádí se tam například, že „slavnost se pořádá pro krále Ptolemaia, navěky žijícího, milovaného Ptahem, bohem zjeveným a děkovným, každoročně



Obrázek 54: Rosettská deska, popsaná v roce 196 pf. n. 1. a znovuobjevená roku 1799, obsahuje stejný text ve třech typech písma: hieroglyfy (nahoře), démotika (uprostřed) a řečtina (dole).v chrámech po celé zemi od prvního dne měsíce Troth po pět dní, v nichž jest nositi věnce a konati oběti, úlitby a ostatní obvyklé pocty". Jestliže ostatní dva texty obsahují stejné nařízení, rozluštění hieroglyfů a démotiky může vypadat jako snadný úkol. Přesto se vyskytly tři významné překážky. Za prvé, Rosettská deska je vážně poškozená (viz obrázek 54). Řecký text se skládá z 54 řádků, z nichž je 26 posledních řádků poškozených. Nápis démotikou se skládá ze 32 řádků, začátky

prvních 14 řádků jsou poškozeny (je třeba si uvědomit, že démotika a hieroglyfy se psaly zprava doleva). Hieroglyfický text je v nejhorším stavu, polovina řádků chybí úplně a zbývajících 14 řádků (odpovídajících posledním 28 řádkům řeckého textu) částečně chybí. Druhou překážkou rozluštění je to, že dvě formy egyptského písma zaznamenávají starý egyptský jazyk, kterým nikdo po nejméně osm století nemluvil. Zatímco bylo možné najít řadu egyptských symbolů, které odpovídají řeckým slovům, což by umožnilo archeologům vypracovat význam egyptských symbolů, bylo nemožné určit zvukovou podobu egyptských slov. Dokud archeologové nevěděli, jak se egyptská slova vyslovovala, nemohli odvodit fonetiku symbolů. Nakonec zde existoval i problém intelektuálního odkazu Kirchera, který stále vedl archeology k tomu, aby přemýšleli o egyptském písmu jako o piktogramech, nikoli jako o fonogramech, a proto jen několik lidí vůbec uvažovalo o tom, že se pustí do fonetického luštění hieroglyfů.

Jedním z prvních vědců, který zpochybnil předpoklad, že hieroglyfy jsou obrázkovým písmem, byl Thomas Young, zázračné dítě a polyglot. Narodil se roku 1773 v Milvertonu v hrabství Somerset a ve věku dvou let už uměl plynně číst. Ve čtrnácti letech studoval řečtinu, latinu, francouzštinu, italštinu, hebrejštinu, chaldejštinu, syrskou a samařskou aramejštinu, arabštinu, perštinu, turečtinu a etiopštinu. Když vstoupil do Emmanuel College v Cambridgi, jeho genialita mu vysloužila přezdívku „mladý fenomén" [Young = angl. mladý, pozn. překl.]. V Cambridgi studoval medicínu, ale říkalo se, že jej zajímaly pouze nemoci, a nikoli pacienti, kteří jimi trpěli. Postupně se zaměřil více na výzkum a méně na péči o nemocné.

Young vykonal pozoruhodnou řadu medicínských pokusů, z nichž mnohé měly za cíl vysvětlit, jak funguje lidské oko. Zjistil, že vnímání barev je výsledkem spolupráce tří oddělených typů re-ceptorů, z nichž každý je citlivý na jednu ze tří základních barev. Tím, že kolem bulvy živého oka pokládal kovové prstence, ukázal,

že zaostřování nevyžaduje zakřivení celého oka. Nakonec došel k závěru, že všechnu práci obstarává čočka uvnitř oka. Zájem o optiku jej dovedl k *fyzice* a tím k další řadě objevů. Napsal klasickou stať o povaze světla *The Undulatory Theory ofLight* (Vlnovou teorii světla), vytvořil nové a lepší vysvětlení přílivu a odlivu, formálně definoval pojem energie a publikoval zásadní objevy z teorie pružnosti. Young byl podle všeho schopen řešit problémy v téměř každém oboru, což mu vždy neprospívalo. Jeho mysl se dala tak snadno upoutat, že skákal z předmětu na předmět a v novém problému se angažoval dříve, než dokončil minulý.

Když Young uslyšel o Rosettské desce, stala se pro něj neodolatelnou výzvou. V létě roku 1814 se vydal na svou každoroční dovolenou do pobřežního letoviska ve Worthingu a vzal s sebou kopie tří nápisů. Průlom nastal, když se zaměřil na sadu hieroglyfů v oválném rámu, zvanou *kartuš.* Odhadl, že tyto hieroglyfy jsou zvýrazněny, protože představují něco velmi důležitého, možná jméno faraóna Ptolemaia - protože řecká podoba jeho jména se v řeckém textu vyskytovala. Pokud by tomu tak skutečně bylo, umožnilo byto Youngovi objevit fonetiku odpovídajících hieroglyfů, protože faraónovo jméno by se vyslovovalo zhruba

stejně nehledě na jazyk. Kartuš s Ptolemaiem se na Rosettské desce opakuje šestkrát, někdy v takzvané standardní verzi a někdy v delší, propracovanější verzi. Young předpokládal, že delší verze představuje Ptolemaiovo jméno i s jeho titulem, soustředil se na symboly, které se objevily v kratší verzi, a odhadoval zvukovou podobu každého hieroglyfu (viz tabulka 13).

Přestože to tehdy nevěděl, podařilo se Youngovi přiřadit většině hieroglyfů jejich správný fonetický význam. Naštěstí vzal první dva hieroglyfy □, O, které byly v nápisu umístěny nad sebou, nikoli vedle sebe, v jejich správném fonetickém pořadí. Písař tak hieroglyfy umístil z estetických důvodů, na úkor fonetické zřetelnosti. Písaři měli sklon psát tímto způsobem, aby se vyhnuli mezerám a udrželi vizuální harmonii; někdy dokonce prohodili hlásky bez ohledu na jakékoli smysluplné hláskování pouze proto, aby zvýšili krásu nápisu. Po tomto rozluštění Young objevil kartuši v nápise okopírovaném z chrámu v Karnaku v oblasti Théb, o němž tušil, že je to jméno ptolemaiovské královny Bereniky. Opakoval svou strategii (výsledky viz tabulka 14).

Ze třinácti hieroglyfů v obou kartuších Young určil polovinu naprosto přesně a další čtvrtinu částečně správně. Dobře také identifikoval symbol, který zakončoval slova ženského rodu a který byl kladen zájmena královen a bohyň. Přestože nemohl vědět, do jaké míry uspěl, skutečnost, že se symboly *i\I* objevily v obou kartuších, kde v obou případech představovaly i, napověděla Youngovi, že je

Hieroglyf	Youngova zvuková podoba	Skutečná zvuková podoba
□	p	p
○	t	t
	neurčitý zvuk	o
	lo nebo ole	l
	ma nebo m	m
	i	i nebo y
	oš nebo os	s

Tabulka 13: Youngovo rozluštění (° fl ^ Hí| P] - kartuše s Ptolemaiem (standardní verze) z Rosettské desky.

Hieroglyf	Youngova zvuková podoba	Skutečná zvuková podoba
	bir	b
	e	r
	n	n
	i	i
	neurčitý zvuk	k
	ke nebo ken	a
	koncovka ženského rodu	koncovka ženského rodu

Tabulka 14: Youngovo rozluštění *(ji.* (q s^^j - kartuše Bereniky z chrámu v Karnaku.

na správné cestě. Tak získal jistotu nezbytnou k tomu, aby mohl pokračovat v dalším luštění. Jeho práce však náhle skončila. Zdá se, že měl příliš velkou úctu ke

Kircherovu argumentu, že hieroglyfy jsou piktogramy, a nebyl připraven rozbít toto paradigma. Své vlastní fonetické objevy omluvil tím, že zakladatelem ptolemaiovské dynastie byl Lagus, jeden z generálů Alexandra Velikého. Jinak řečeno, Ptole-maiovci byli cizinci, a proto Young vyslovil hypotézu, že jejich jména se musela hláskovat foneticky, neboť pro ně nebyl žádný přirozený piktogram v standardním seznamu hieroglyfů. Své myšlenky shrnul tak, že porovnal hieroglyfy s čínskými znaky, kterým Evropané tehdy právě začínali rozumět:

‚Je nadmíru zajímavé sledovat některé kroky, kterými se zřejmě alfabe-tické písmo vyvinulo z hieroglyfického; proces, který může být vskutku do jisté míry ilustrován způsobem, jakým moderní čínština vyjadřuje cizí kombinace zvuků. Znaky jsou redukovány na fonetickou hodnotu příslušnou značkou, místo aby si ponechaly svůj přirozený význam; a tato značka se v některých moderních tištěných knihách velmi přibližuje kroužkům, ve kterých jsou jména zapsána hieroglyfy."

Young nazval svůj úspěch „zábavou na pár hodin volného času". Hieroglyfy jej přestaly zajímat a svou práci uzavřel článkem pro *Dodatek encyklopedie Britannica* z roku 1819.

V téže době byl již připraven slibný mladý francouzský lingvista Jean-Francpois Champollion dotáhnout Youngovy myšlenky do konce. Přestože mu ještě nebylo ani třicet let, hieroglyfy ho fascinovaly **již** téměř dvacet let. Jeho vášeň se datovala od roku 1800, kdy fran-couzský matematik Jean-Baptiste Fourier, jeden z Napoleonových „pekinézů", zasvětil desetiletého Champolliona do své sbírky egyptských památek, z nichž mnohé byly ozdobeny bizarními nápisy. Fourier mu vysvětlil, že nikdo nedokáže přeložit toto tajemné písmo, načež chlapec slíbil, že on jednoho dne tajemství rozluští. O pouhých sedm let později jako sedmnáctiletý zveřejnil článek *Egypte souš les Pharaons* (Egypt za vlády faraónů). Text byl tak průkopnický, že Champolliona ihned zvolili za člena Akademie v Grenoblů. Když Champollion uslyšel, že se stal profesorem, byl tak ohromený, že na místě omdlel.

Champollion pak i nadále ohromoval své vrstevníky, ovládal latinu, řečtinu, hebrejštinu, etiopštinu, sanskrt, staroíránské jazyky, arabštinu, syrštinu, chaldejštinu, perštinu a čínštinu - to vše proto, aby se vyzbrojil na útok na hieroglyfy. Jeho posedlost dobře ilustruje příhoda z roku 1808, kdy na ulici narazil na starého přítele. Ten se mezi řečí zmínil, že známý egyptolog Alexandre Lenoir vydal úplné vyluštění hieroglyfů. Champolliona to tak zničilo, že opět na místě omdlel. (Patrně měl na omdlévání docela talent.) Zdálo se, že jediným smyslem jeho života je to, zda bude první, kdo přečte písmo starých Egypťanů. Naštěstí pro Champolliona bylo Lenoirovo vyluštění stejně fantaskní jako Kircherovy pokusy ze 17. století a výzva přetrvala.

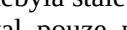
V roce 1822 aplikoval Champollion Youngův postup na další kartuše. Britský přírodovědec W. J. Bankes přivezl obelisk s řeckým a hieroglyfickým nápisem do Dorsetu a současně publikoval litografii těchto dvojjazyčných textů, které obsahovaly také kartuše Ptolemaia a Kleopatry. Champollion si obstaral jejich kopii a nakonec se mu podařilo přiřadit jednotlivým hieroglyfům fonetickou podo-

bu (viz tabulka 15). Písmena p, t, o, 1 a e jsou pro obě jména společná, ve čtyřech případech jsou představována stejným hieroglyfem u Ptolemaia i Kleopatry a pouze v jednom případě (u písmene t) je rozpor. Champollion předpokládal, že zvuk t může být představován dvěma hieroglyfy, stejně jako se hláska k může v angličtině zapisovat písmeny c nebo k, například ve slovech „cat" (kočka) a „kid" (děcko). Povzbuzen svým úspěchem, *začal* se Champollion věnovat kartuším i bez řeckých textů. Kdekoli to bylo možné, nahrazoval hieroglyfy fonetickým zápisem, který odvodil z kartuší Ptolemaia a Kleopatry. Jeho první záhadná kartuše (viz tabulka 16) obsahovala jedno z nejdůležitějších jmen starověku. Champollionovi bylo zřejmé, že kartuše, ve které bylo pravděpodobně napsáno a-1-?-s-e-?-t-r-?, představuje jméno alksentrs - v řečtině Alexandros, tedy Alexandr. Champollion rovněž pochopil, že písaři neradi používali samohlásky a často je vynechávali, předpokládali totiž, že čtenáři nebudou mít s doplněním chybějících samohlásek problémy. S dalšími dvěma rozluštěnými hieroglyfy studoval mladý vědec další nápisy a rozluštil řadu kartuší. Přesto však byl veškerý pokrok, kterého dosáhl, pouhým pokračováním Youngovy práce. Všechna jména

Hieroglyf	Zvuková podoba	Hieroglyf	Zvuková podoba
	p		c
	t		l
	o		e
	l		o
	m		p
	e		a
	s		t
			r
			a

Tabulka 15: Champollionovo rozluštění a – kartuše Ptolemaia a Kleopatry z Bankesova obelisku.

Hieroglyf	Zvuková podoba	Hieroglyf	Zvuková podoba
	a		?
	l		t
	?;		r
	s		?
	e		

Tabulka 16: Champollionovo vyluštění  – kartuše Alexandra.

jako Alexandr nebo Kleopatra nebyla stále prokázána, a podporovala tak teorii, že fonetický zápis se užíval pouze pro slova, která nepatřila do tradičního egyptského slovníku.

Avšak krátce nato, 14. září 1822, obdržel Champollion reliéfy z chrámu Abú Simbel, jež obsahovaly kartuše předcházející antickému období. Jejich

význam spočíval v tom, že byly dost staré na to, aby obsahovaly tradiční egyptská jména, přesto se v nich jména hláskovala. Byl to jasný důkaz proti teorii, že se hláskování uplatňovalo pouze pro jména cizího původu. Champollion se soustředil na kar-tuši, která obsahovala pouze čtyři hieroglyfy (©fŘjj{^|. První dva symboly neznal, ale dvojici znaků na konci p(l rozluštil již dříve z kartuše Alexandra (alksentrs) a určil, že jde o dvě písmena s-s. V tomto bodě Champollion použil své rozsáhlé lingvistické znalosti. Přestože koptština, přímý potomek staroegyptského jazyka, přestala být živým jazykem vil. století n. 1., stále však existovala v ustrnulé formě v liturgii křesťanského koptského náboženství. Champollion se koptštinu naučil již jako dospívající a ovládal ji tak plynně, že si koptsky psal deník. Přesto nikdy nebral v úvahu, že by koptština mohla být také jazykem hieroglyfů.

Champolliona napadlo, zda by první znak v kartuši © nemohl být piktogramem znázorňujícím slunce, tzn. že obrázek slunce byl symbolem pro slovo „slunce". Potom se projevila jeho geniální intuice, když usoudil, že zvuková podoba piktogramu je koptské slovo pro slunce ra. Tak získal sekvenci (ra-?-s-s), která se hodila na jméno jediného faraóna. Když vzal Champollion v úvahu iritující vynechávání samohlásek a když odhadl, že zvuková podoba chybějícího písmene je m, muselo pak nutně jít o jméno Ramsese, jednoho z největších faraónů - a také jednoho z nejstarších. Prokletí bylo zlomeno. I stará tradiční jména se hláskovala foneticky! Champollion vrazil do pracovny svého bratra a vykřikl: ‚Je tiens 1' affaire!" („Mám to!"), ale jeho vášeň pro hieroglyfy se znovu ukázala být silnější než on. Ihned zkolaboval a po následujících pět dní byl upoután na lůžko.

Champollion ukázal, že písaři někdy využívali principu rébusu. V rébusu, který stále můžeme najít v dětských hádankách, jsou dlouhá slova rozdělena na jejich fonetické složky, které jsou pak zobrazeny jako piktogramy. Například slovo „telegraf lze rozdělit na dvě části: tele-graf. Slovo lze pak znázornit obrázkem telete a grafu. V příkladu objeveném Champollionem je pouze první slabika (ra) znázorněna obrázkovým rébusem - obrázkem slunce, zatímco zbytek slova je hláskován.

Význam piktogramu slunce v kartuši Ramsese je obrovský, protože značně omezuje výběr jazyka, jímž mluvili písaři. Jejich jazykem nemohla být například řečtina, protože by to znamenalo, že se kartuše vyslovovala „helio-meses". Kartuš dává smysl pouze za předpokladu, že písaři hovořili některou formou koptštiny, protože kartuš by se tak vyslovovala „ra-meses".

Přestože to byla jen jedna z mnoha kartuši, její rozluštění zřetelně prokázalo čtyři základní principy hieroglyfů. Za prvé, jazyk písařů je

přinejmenším příbuzný koptštině - a prostudování dalších hieroglyfů ukázalo, že se jedná přímo o koptštinu. Za druhé, ke znázorňování některých slov se používají piktogramy, například slovo „slunce" je představováno jednoduchým obrázkem slunce. Za třetí, některá dlouhá slova jsou sestavena úplně nebo částečně na principu rébusu. Konečně, u většiny nápisů písaři používali relativně konvenční fonetickou abecedu. Poslední bod je nejdůležitější, Champollion nazval fonetiku „duší" hieroglyfů.

Díky svým hlubokým znalostem koptštiny pak Champollion začal s neomezeným a plodným luštěním hieroglyfů mimo kartuše. Během dvou let identifikoval zvukovou podobu většiny hieroglyfů a objevil, že některé z nich představují kombinaci dvou nebo dokonce tří souhlásek. To někdy umožňovalo písařům napsat slovo buď s pomocí několika jednoduchých, nebo více hláskových hieroglyfů.

Champollion zaslal své originální výsledky v dopise panu Dacie-rovi, stálému sekretáři francouzské *Academie des Inscriptíons.* Roku 1824, ve věku 34 let, zveřejnil Champollion všechny své objevy v knize nazvané *Précis du systéme hiéroglyphique.* Poprvé po čtrnácti stoletích bylo možné číst o historii faraónů, jak ji zapsali jejich písaři. Prolingvisty to byla příležitost studovat vývoj jazyka a písma napříč obdobím, které pokrývá tři tisíce let. Hieroglyfy bylo možné zkoumat od 3. tisíciletí př. n. 1. až do 4. století n. 1. Vědci mohli navíc vývoj hieroglyfů porovnat s hieratikou a démotikou, které již v té době znali.

Po několik let bránily všeobecnému přijetí Champollionova velkolepého úspěchu politika a závist. Zvlášť ostře kritizoval Champol-liona Thomas Young. Při několika příležitostech Young popřel, že jsou hieroglyfy převážně fonetické; jindy tento názor přijal, ale stěžoval si, že on sám dosáhl tohoto závěru ještě před Champollionem a že Francouz pouze vyplnil některé mezery. Velká část Youngova nepřátelství byla dána tím, že Champollion opomenul přiznat jeho zásluhy, přestože je pravděpodobné, že Youngův původní průlom mu poskytl inspiraci k úplnému rozluštění.

V červenci 1828 se Champollion vydal na svou první expedici do Egypta, která trvala osmnáct měsíců. Byla to pro něj pozoruhodná příležitost vidět na vlastní oči nápisy, které předtím spatřil jen na kresbách nebo litografiích. O třicet let dříve Napoleonova expedice nazdařbůh hádala smysl hieroglyfů, které zdobily chrámy, ale nyní je byl Champollion schopen jednoduše číst znak po znaku, a navíc je i správně vyložit. Jeho cesta přišla právě včas. O tři roky později, po uspořádání podrobných poznámek, kreseb a překladů z jeho egyptské cesty, jej ranila mrtvice. Sklony k mdlobám, jimiž trpěl po celý život, byly možná příznakem vážnější nemoci, zhoršené jeho vášnivým a intenzivním studiem. Zemřel 4. března 1832 ve věku jednačtyřiceti let.

Záhada lineárního písma B

Během dvou století po Champollionově průlomu egyptologové stále lépe chápali spletitosti hieroglyfů. Úroveň jejich znalostí je dnes natolik vysoká, že jsou schopni rozluštit dokonce zašifrované hieroglyfy, které patří mezi nejstarší zašifrované texty na světě.

Některé z nápisů nalezených na hrobkách faraónů byly zašifrovány různými metodami včetně substituční šifry. Namísto zavedených hieroglyfů se používaly nově vytvořené symboly a jindy byl namísto správného hieroglyfu použit foneticky rozdílný, ale vzhledově podobný znak. Například hieroglyf „rohatý brejlovec", který

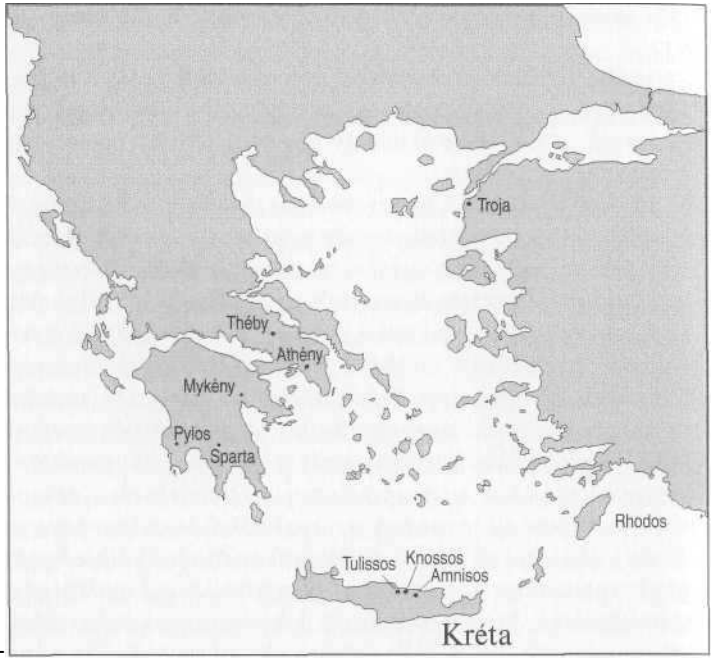
obvykle zastupuje f, mohl být použit namísto hada, který zastupuje z.

U zašifrovaných náhrobních nápisů zpravidla nešlo o to, aby se nedaly rozluštit, spíše měly sloužit jako hádanky vyvolávající zvědavost kolemjdoucích, které nabádaly, aby se na chvíli u hrobky zastavili a zamysleli.

Po zdolání hieroglyfů pokračovali archeologové luštěním dalších starých písem včetně babylonského klínového písma, tureckých run kók-turki a indického slabičného písma brahmí. Dobrou zprávou pro budoucí Champolliony však je, že několik skvělých písem stále čeká na vyluštění, jako třeba písmo Etrusků a některá staroin-dická písma (viz příloha 1). Velká potíž při luštění zbylých písem spočívá v tom, že neexistuje žádná nápověda, nic, co by umožnilo luštitelům získat první náznak obsahu těchto starých textů. Pro egyptské hieroglyfy sloužily jako pomůcky kartuše, díky nimž Young a Champollion získali první představu o fonetických významech hlásek. Bez nápovědy se možná jeví rozluštění starého písma jako neřešitelný úkol, avšak existuje jeden pozoruhodný příklad písma, které bylo rozluštěno bez ohledu na tuto překážku. Lineární písmo B - krétské písmo, které se datuje do doby bronzové, bylo rozluštěno bez pomocných klíčů. Bylo vyřešeno kombinací logiky a inspirace, které jsou mocným příkladem čisté kryptoanalýzy. Rozluštění lineárního písma B je obecně považováno za největší archeologický výkon svého druhu.

Příběh lineárního písma B začíná vykopávkami sira Arthura Evan-se, jednoho z nejvýznamnějších archeologů přelomu 19. a 20. století. Evanse zajímalo období řeckých dějin popisované Homérem v jeho eposech *Ilias* a *Odyssea*. Homér obšírně vypráví o historii trojské války, o řeckém vítězství u Troje a o následujících hrdinských činech Odyssea a také o událostech, které se měly odehrát ve 12. století př. n. 1. Někteří vzdělanci z 19. století odmítli Homérovy eposy jako pouhé legendy, ale v roce 1872 německý archeolog Heinrich Schlie-mann odkryl samo město Tróju blízko západního pobřeží Turecka. Najednou se Homérovy mýty staly skutečnou historií.

Mezi lety 1872 a 1900 archeologové odkryli další důkazy o bohatém období prehelénské historie, předcházející řeckému klasickému věku Pythagora, Platona a Aristotela o zhruba 600 let. Prehelénské období trvalo od roku 2800 do 1100 př. n. 1. a během jeho posledních 400 let dosáhla tehdejší civilizace svého vrcholu. Na



řecké pev-

Obrázek 57: Místa archeologických nálezů v oblasti Egejského moře. Po objevení vzácných nálezů v Mykénách na řecké pevnině se sir Arthur Evans vydal hledat tabulky obsahující písmo. První tabulky s lineárním písmem B byly objeveny na ostrově Kréta, v centru minojské říše.

nině byla kultura soustředěna kolem Mykén, kde archeologové odkryli velké množství artefaktů a cenných sbírek. Sir Arthur Evans byl však zmaten tím, že se nepodařilo najít jakoukoli formu písma. Odmítal věřit, že by tak vyspělá společnost mohla fungovat naprosto bez písma, a rozhodl se dokázat, že mykénská civilizace písmo měla.

Po setkání s různými athénskými obchodníky se starožitnostmi sir Arthur konečně narazil na kameny s rytinami, jež byly patrně pečetěmi z prehelénského období. Znaky na pečetích se zdály být spíše obrázky než opravdovým písmem, podobaly se symbolům užívaným v heraldice. Pečeti měly údajně pocházet z Kréty a konkrétně z lokality Knossos, kde měl být podle legendy palác krále Minoa -střed říše, která ovládala oblast kolem Egejského moře. Sir Arthur se vydal na Krétu a v březnu roku 1900 zahájil vykopávky. Výsledky

se dostavily rychle a byly ohromující. Archeolog odkryl pozůstatky luxusního paláce, protkaného spletitou sítí chodeb a zdobeného freskami mladíků skákajících přes zuřivé býky. Evans usoudil, že sport spočívající ve skákání přes býky je nějak spjat s legendou o Mi-notaurovi, příšeře s býčí hlavou, která se živila mladými lidmi, a napadlo ho, že spletitost palácových chodeb mohla inspirovat pověst o Minotaurově labyrintu.

31. března sir Arthur začal postupně dostávat na světlo poklad, po kterém toužil nejvíce. Nejprve objevil jedinou popsanou hliněnou tabulku, o pár dní později

dřevěnou truhlu, která jich byla plná, a posléze odhalil zásoby písemného materiálu, které překonaly všechna jeho očekávání. Všechny tyto hliněné tabulky byly původně vysušeny na slunci, nikoli vypáleny v peci, aby je šlo jednoduše recyklovat přidáním vody. Dalo by se očekávat, že za dlouhá století tabulky rozmočí déšť a budou navždy zničeny. Jak se však ukázalo, palác v Knossu byl zničen ohněm, který tabulky vypálil a pomohl je tak uchovat po tři tisíciletí. Jejich stav byl tak dobrý, že po jejich nálezu bylo ještě možné rozeznat otisky prstů písařů.

Tabulky se dělily do tří kategorií. První sada tabulek, jež byly datovány mezi léty 2000 a 1650 př. n. 1., se skládala hlavně z kreseb, pravděpodobně piktogramů, zjevně souvisejících se symboly na pečetích, které sir Arthur Evans koupil od obchodníků v Athénách. Druhá sada tabulek, jež byly datovány mezi léty 1750 a 1450 př. n. 1., byla popsána znaky, které se skládaly z čistých linií, a proto byly pojmenovány jako lineární písmo A. Třetí sadu tabulek označili archeologové jako lineární písmo B, a protože to bylo nejmladší písmo, sir Arthur a ostatní archeologové se domnívali, že jim poskytuje největší šance na vyluštění.

Mnoho tabulek zřejmě obsahovalo inventární seznamy. S tolika sloupci numerických znaků bylo poměrně jednoduché pochopit používaný systém pro zápis čísel, avšak fonetické znaky byly daleko víc matoucí. Vypadaly jako nesmyslná sbírka libovolných čmáranic. Historik David Kahn popisoval některé z jednotlivých znaků jako „gotický oblouk uzavřený svislou čarou, žebřík, probodnuté srdce, ohnutý trojzubec s bodcem, třínohý dinosaurus hledící přes rameno, písmeno A protnuté další vodorovnou čarou, obrácené S, do poloviny naplněná vysoká sklenice na pivo, s lukem uvázaným k okraji; další tucet znaků se nepodobá už vůbec ničemu". *Zřejmé* byly pouze dvě věci. Za prvé, směr psaní byl jasně zleva doprava, pro-tože nevyplněné mezery na konci řádků byly vesměs napravo. Za druhé, dalo se rozlišit 90 různých znaků, z čehož vyplynulo, že písmo je téměř jistě slabičné.

Cistě abecední písmo mívá většinou mezi 20 až 40 znaky (například ruština má 36 znaků, arabština 28). Písmo založené na piktogramech se skládá ze stovky nebo tisíce znaků (čínština jich má přes 5 000). Slabičné písmo je někde mezi tím, obsahuje od 50 do 100 znaků. Kromě těchto dvou poznatků bylo lineární písmo B nevyzpytatelným tajemstvím.

Zásadní problém spočíval v tom, že si nikdo nemohl být jist, v jakém jazyku bylo lineární písmo B psáno. Původně se mělo za to, že lineární písmo B bylo psanou formou řečtiny, protože sedm jeho znaků se velmi podobá znakům klasického kyperského písma, jež se jako forma řeckého písma užívalo mezi lety 600 až 200 př. n. 1. Vynořily se však pochybnosti. Nejčastější souhláskou, kterou končí řecká slova, je s, v důsledku toho je nejčastějším koncovým znakem v kyperském písmu *f-, což* představuje slabiku se. Protože znaky jsou slabičné, samotnou souhlásku je třeba psát jako kombinaci

Obrázek 58: Tabulka s lineárním písmem B, datována kolem roku 1400 př. n. 1.souhláska-samohláska s nevyslovovanou samohláskou. Stejný znak se nachází i v lineárním písmu B, ale jen zřídka na koncích slova -tato skutečnost naznačuje, že lineární písmo B nemusí být řečtina. Archeologové došli k obecně přijímanému názoru, že lineární písmo B představuje neznámý a již neexistující jazyk. Když tento jazyk vymizel, písmo zůstalo a ještě se po staletí vyvíjelo až do nástupu kyperského písma, které se používalo pro psaní řečtiny. Tudíž tato dvě písma vypadají podobně, ale vyjadřují naprosto odlišné jazyky.

Sir Arthur Evans byl velkým stoupencem teorie, že lineární písmo B nebylo psanou formou řečtiny, a věřil, že představovalo původní krétský jazyk. Byl přesvědčen, že jeho argument podpoří přesvědčivé archeologické důkazy. Například jeho objevy na ostrově Kréta naznačovaly, že říše krále Minose, známá jako minojské království, byla daleko vyspělejší než mykénská civilizace na pevnině. Minojské království nebylo součástí mykénské říše, ale spíše jejím protiv-

níkem, možná i nadřazenou mocností. K podpoře tohoto názoru sloužil i mýtus o Minotaurovi. Legenda popisovala, jak král Minos nařídil Athéňanům, aby mu pravidelně posílali skupinu mladíků a panen k obětování Minotaurovi. Stručně řečeno, Evans byl toho názoru, že síla minojské říše jí umožnila ponechat si vlastní jazyk a nepřijmout řečtinu, jazyk svých rivalů.

Přestože se všeobecně uznávalo, že Minojci mluvili vlastním ne-řeckým jazykem (a lineární písmo B bylo jeho psanou formou), zůstali mezi vědci jeden či dva odpůrci, kteří zastávali názor, že Minojci mluvili a psali řecky. Sir Arthur nesl tento nesouhlas těžce a použil svého vlivu k potrestání těch, kteří s ním nesouhlasili. Když A. J. B. Wace, profesor archeologie na univerzitě v Cambridgi, promluvil ve prospěch teorie, že lineární písmo B představuje řečtinu, sir Arthur mu znemožnil přístup k vykopávkám a donutil ho, aby opustil British School v Athénách.

Když roku 1939 Carl Blegen z univerzity v Cincinnati objevil další tabulky s lineárním písmem B v Nestorové paláci v Pylosu, polemika mezi „Reky" a jejich odpůrci ještě zesílila. Šlo o mimořádný objev, protože Pylos se nachází na řecké pevnině a podle všech předpokladů měl být součástí mykénské říše, nikoli minojské. Menšina archeologů, kteří se domnívali, že lineární písmo B je řečtina, prohlásila, že to podporuje jejich hypotézy: lineární písmo B bylo nalezeno na řecké pevnině, kde se mluvilo řecky, takže lineární písmo B představuje řečtinu. Lineární písmo B bylo objeveno také na Krétě,

proto Minojci také mluvili řecky. Evansův tábor argumentoval opačně' Minojci na Krétě mluvili minojským jazykem. Lineární písmo B se nachází na Krétě, tudíž lineární písmo B představuje minojský iazyk. Lineární písmo B se objevilo také na pevnině, proto se tam také hovořilo minojský. Sir Arthur byl důrazný: „V Mykénách není pro řecky mluvící dynastie místo... kultura stejně jako jazyk byly minojské až do morku kostí."

Blegenův objev nepřisuzoval Mykéňanům a Minojcům nezbytně jeden jazyk. Ve středověku vedlo mnoho evropských států, nezávisle na svém mluveném jazyku, své písemnosti v latině. Možná, že jazyk lineárního písma B byl podobnou společnou řečí obchodníků egej-ské oblasti a umožňoval pohodlnou výměnu zboží mezi národy, které nemluvily společným jazykem.

Po čtyři desetiletí všechny pokusy rozluštit lineární písmo B skončily neúspěchem. Sir Arthur Evans zemřel v roce 1941, ve věku devadesáti let. Nedožil se toho, aby byl svědkem rozluštění lineárního písma B nebo aby si mohl přečíst obsah textů, které objevil. Vědci však tehdy měli mizivou naději, že lineární písmo B bude vůbec někdy vyluštěno.

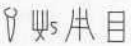
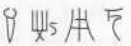
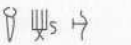
Přemosťující slabika

Po smrti sira Arthura Evanse byly archivy tabulek s lineárním písmem B a jeho vlastní archeologické poznámky k dispozici pouze omezenému okruhu archeologů - totiž jen těm, kteří podporovali jeho teorii, že lineární písmo B představuje svébytný minojský jazyk. Nicméně v polovině 40. let se Alici Koberové, profesorce klasických studií z americké Brooklyn College, podařilo získat přístup k materiálům, které začala pečlivě analyzovat. Těm, kteří ji znali jen zběžně,

připadala Koberová docela obyčejná - staromódní profesorka, ani půvabná, ani charismatická, s realistickým přístupem k životu. Přesto byla její vášeň pro výzkum nezměřitelná. „Pracovala s podmanivou intenzitou," vzpomíná bývalá studentka Eva Brannová, která se pak stala archeoložkou na univerzitě v Yale. Jednou mi řekla, že jediným důkazem pro to, že jste udělali něco doopravdy skvěle, je, když vás zamrazí v zádech."

Koberová si uvědomila, že musí zahodit všechny předsudky, chce-li lineární písmo B rozluštit. Zaměřila se výhradně na struktu-ru písma jako na celek a na tvoření jednotlivých slov. Přitom si povšimla, že některá slova tvoří trojice, které vypadají jako stejné slovo opakované ve třech lehce odlišných formách. V rámci dané trojice se vyskytoval stejný kmen, ale tři různá zakončení. Koberová učinila závěr, že lineární písmo B představuje vysoce ohebný jazyk, jehož slova mění své koncovky tak, aby vyjadřovala rod, čas, pád a podobně. Angličtina není příliš ohebná, anglicky například říkáme I decipher, you decipher, he deciphers - ve třetí osobě slovesu pouze přibývá „s". [Kdežto česky to je „dešifruji, dešifruješ, dešifruje" - čeština je mnohem ohebnější *jazyk, než* angličtina. Pozn. překl.] Starší jazyky používají takových koncovek častěji než moderní. Koberová publikovala článek, kde popsala charakter skloňování u dvou konkrétních skupin slov (viz tabulka 17). Každá skupina si zachovávala kmen a přidávala k němu různá zakončení odpovídající třem různým pádům.

Pro zjednodušení zápisu bylo každému symbolu lineárního písma B přiřazeno dvojciferné číslo (viz tabulka 18). Pomocí těchto čísel lze slova v tabulce 17 přepsat do podoby uvedené v tabulce 19. Obě skupiny symbolů by mohly být podstatnými jmény, která mění svá zakončení podle pádu - v prvním řádku by mohl být nominativ,

	Slovo A	Slovo B
První pád		
Druhý pád		
Třetí pád		

Tabulka 17: Dvě skloňovaná slova v lineárním písmu B.

Tabulka 18: Symboly lineárního písma B a jim přiřazená čísla.

	Slovo A	Slovo B
První pád	25-67-37-57	70-52-41-57
Druhý pád	25-67-37-36	70-52-41-36
Třetí pád	25-67-05	70-52-12

Tabulka 19: Dvě skloňovaná slova v lineárním písmu B přepsaná do čísel.

ve druhém akuzativ a ve třetím řádku například dativ. Je jasné, že první dva znaky v obou skupinách slov (25-67a70-52)jsou součástí kmene, protože se opakují bez ohledu na pád. Avšak třetí znak je matoucí. Jestliže je třetí znak součástí kmene, potom by měl pro dané slovo zůstávat konstantní bez ohledu na pád slova, to se však neděje. Ve slově A je třetím znakem 37 v prvním a druhém pádě, ale ve třetím pádě je 0 5. Ve slovu B je třetím znakem 41 v prvním a druhém pádě, ale ve třetím pádě je 12. Pokud naopak třetí znak není součástí kmene, je

možná součástí koncovky, ale tato možnost je stejně problematická. Pro daný pád by mělo být zakončení stejné bez ohledu na slovo, avšak pro první a druhý pád je třetím znakem 37 ve slově A, ale 41 ve slově B, a pro třetí pád je třetím znakem 0 5 ve slově A, ale 12 ve slově B.

Třetí znaky byly v rozporu s očekáváním, protože se nezdály být součástí ani kmene, ani koncovky. Koberová tento paradox vyřešila tím, že vytvořila teorii, podle níž každý znak zastupuje slabiku, pravděpodobně kombinaci souhlásky následované samohláskou. Navrhla, že třetí slabika může být přemosťující slabikou, která zastupuje část kmene a část zakončení. Souhláska může náležet ke kmeni a samohláska ke koncovce. Aby ilustrovala svou teorii, podala příklad z akkadského jazyka, který má také přemosťující slabiky a je velmi ohebný. *Sadanu* je první pád akkadského podstatného jména, které se změní na *sadani* v druhém a *sadu* ve třetím pádě (viz tabulka 20). Je zřejmé, že tři slova se skládají z kmene sad- a koncovek -anu (první pád), -ani (druhý pád) nebo -u (třetí pád) s -da-, -da- nebo -du jako přemosťující slabikou. Přemosťující slabika je stejná v prvním a dru

První pád	sa-da-nu
Druhý pád	sa-da-ni
Třetí pád	sa-du

Tabulka 20: Přemosťující slabiky v akkadském slově *sadanu.*

hém pádě, ale odlišná ve třetím. To je přesné vzorec pozorovaný u lineárního písma B - proto třetí znak v každém ze zmiňovaných slov v lineárním písmu B musí být přemosťující slabikou.

Sama identifikace ohebného charakteru lineárního písma B a existence přemosťujících slabik znamenala, že Koberová pokročila v rozluštění minojského písma dále než kdokoliv jiný - a to šlo stále o pouhý začátek. Profesorka se chystala k daleko rozsáhlejší dedukci. V akkadském příkladě se přemosťující slabiky mění z *-da* na *-du,* ale souhláska je v obou slabikách stejná. Podobně u lineárního písma B musí slabiky 37 a 05 ve slově A sdílet stejnou souhlásku jako slabiky 41 a 12 ve slově B. Poprvé od okamžiku, kdy Evans objevil lineární písmo B, se začínala vynořovat fakta o fonetice znaků. Koberová také dokázala odvodit další soubor vztahů mezi znaky. Je zřejmé, že první pád ve slovech A a B v lineárním písmu B by měl mít stejné zakončení. Avšak přemosťující slabika se mění z 37 na 41. Z toho vyplývá, že znaky 37 a 41 představují slabiky s různými souhláskami, ale stejnými samohláskami. To by vysvětlovalo, proč se znaky liší, ačkoli zachovávají u obou slov stejné zakončení. Stejně tak u slov ve třetím pádě budou slabiky 0 5 a 12 mít stejnou samohlásku, ale různé souhlásky. Koberová nedovedla přesně stanovit, která samohláska je společná pro 05 a 12, pro 37 a 41; stejně tak nemohla přesně určit, která souhláska je společná pro 37 a 05 a která pro 41 a 12. Nicméně bez ohledu na jejich absolutní zvukovou podobu jednoznačně určila vztahy mezi určitými znaky. Své výsledky shrnula ve formě mřížky (viz tabulka 21). Podle ní je patrné, že sice neměla představu, kterou slabiku představuje znak 37, ale věděla, že její souhláska je sdílena se znakem 05 a samohláska se znakem 41. Podobně nevěděla, kterou slabiku představuje znak 12, ale věděla, že její souhláska je sdílena se znakem 41 a samohláska se znakem 0 5.

Svou metodu aplikovala na další slova a konečně sestrojila mřížku pro deset znaků, která měla dva sloupce se dvěma samohláskami a pět řádků s pěti souhláskami. Je docela dobře možné, že by Koberová učinila další klíčový krok v luštění a dokonce by se jí i podařilo

	Samohláska 1	Samohláska 2
Souhláska 1	37	05
Souhláska 2	41	12

Tabulka 21: Mřížka Koberové pro vztahy mezi znaky lineárního písma B.rozluštit celé písmo. Avšak nežila tak dlouho, aby mohla využít výdobytků vlastní práce. V roce 1950 ve věku 43 let zemřela na rakovinu plic.

Lehkovážná odbočka

Pouze několik měsíců před svou smrtí obdržela Alice Koberová dopis od anglického architekta Michaela Ventrise, kterého lineární písmo B fascinovalo už od dětství. Ventris se narodil 12. července 1922 jako syn důstojníka britské armády; jeho matka byla napůl polského původu. Byla to především ona, která podporovala jeho zájem o archeologii. Pravidelně ho vodila do Britského muzea, kde Michael žasl nad zázraky starých světů. Michael byl bystré dítě se zvláště výrazným talentem na jazyky. Do školy chodil nejprve v Gsta-adu ve Švýcarsku a naučil se plynně francouzsky a německy. Potom se v šesti letech sám naučil polsky.

Stejně jako Jean-Fran^ois Champollion i Ventris se brzy zamiloval do starých písem. V sedmi letech prostudoval knihu o egyptských hieroglyfech - byl to na jeho věk působivý výkon, zvláště vezmeme-li v úvahu, že kniha byla napsána německy. Jeho zájem o písma starých civilizací pokračoval po celé dětství. V roce 1936 se jako čtrnáctiletý nadchl pro věc ještě více, když navštívil přednášku sira Arthura Evanse, objevitele lineárního písma B. Mladý Ventris se dozvěděl o minojské civilizaci a o záhadě lineárního písma B a umínil si, že písmo rozluští. Ten den se zrodila posedlost, která Ventri-sovi zůstala po celý jeho krátký, ale pozoruhodný život.

V pouhých osmnácti letech shrnul své původní myšlenky o lineárním písmu B v článku, který byl následně publikován ve vysoce respektovaném *American Journal ofArchaeology*. Když odevzdal článek, měl se na pozoru, aby editorům časopisu neprozradil svůj věk - ze strachu, že by ho nebrali vážně. Jeho článek velmi podporoval Evansovu kritiku řecké hypotézy a tvrdil: „Teorie, že Minojci mohli být Řeky, je založena na záměrném odhlédnutí od historické věrohodnosti." On sám se domníval, že lineární písmo B bylo příbuzné etruštině - bylo to rozumné stanovisko, protože existovaly důkazy, že Etruskové přišli z egejské oblasti předtím, než se usídlili v Itálii. Přestože článek ničím nepřispěl k rozluštění lineárního písma B, končil optimistickými slovy: „Může se to podařit."

Ventris se nestal profesionálním archeologem, ale architektem, svůj zájem o lineární písmo B si však zachoval. Veškerý volný čas věnoval studiu každého aspektu tohoto písma. Když uslyšel o práci Alice Koberové, toužil se dozvědět o jejím průlomu co nejvíce a písemně ji požádal o bližší podrobnosti. Přestože

zemřela dříve, než mohla odpovědět, její myšlenky žily v jejích publikacích a Ventris je pečlivě studoval. Plně ocenil význam mřížky Koberové a snažil se najít nová slova se společnými kmeny a přemosťujícími slabikami. Její mřížku rozšířil vložením nových znaků, přičemž do ní zahrnul další souhlásky a samohlásky. Po roce intenzivního studia si povšiml něčeho zvláštního - něčeho, co vypadalo jako výjimka z pravidla: všechny znaky lineárního písma B jsou slabiky.

Obecný názor té doby byl, že každý znak lineárního písma B představuje kombinaci souhlásky se samohláskou (konsonantu s vokálem - KV) a že tedy hláskování vyžaduje rozdělit slovo na komponenty KV. Například anglické slovo mi nutě (minuta) by se pak slabikovalo jako m1-nu-te, řada tří slabik KV. Avšak existuje mnoho slov, která nelze na slabiky KV vhodně rozdělit. Například po rozdělení slova „visible" (viditelný) do dvojic hlásek dostaneme vi-s1-b1-e, což představuje problém, protože se pak nejedná o jednoduchou řadu slabik konsonant/vokál. Slovo obsahuje také skupinu složenou ze dvou souhlásek a navíc koncovku -e. Ventris předpokládal, že Mi-nejci tento problém překonali vložením tichého i, aby tak vytvořili pomocnou slabiku -bi-, takže slovo „visible" by se nyní mohlo zapsat jako v1-s1-b1-1e, což už je kombinace slabik KV.

Avšak slovo 1nv1s1ble (neviditelný) zůstává problémem. Ještě jednou je třeba vsunout tichou samohlásku, tentokrát po souhlásce n a b, a změnit je tak ve slabiky KV. Navíc je třeba se vypořádat se samohláskou i na začátku slova: i-ni-vi-si-bi-l e. Počáteční i nelze snadno změnit ve slabiku KV, protože vsunutí tiché souhlásky na začátek slova by mátlo. Stručně řečeno, Ventris dospěl k závěru, že v lineárním písmu B musí existovat znaky, které představují samotné samohlásky - kvůli slovům, jež začínají na samohlásku. Předpokládal, že tyto znaky bude jednoduché vypátrat, protože se zřejmě vyskytují pouze na začátcích slov. Ventris stanovil, jak často se každý znak objevuje na začátku, ve středu a na konci jakéhokoliv slova. Zjistil, že dva zvláštní znaky 08 a 61 se nacházejí převážně na začátcích slov, a usoudil, že nepředstavují slabiky, ale samotné samohlásky.

Ventris publikoval své myšlenky o znacích pro samohlásky a své rozšíření mřížky v řadě *Work Notes* (Pracovní poznámky), kterou rozesílal dalším vědcům zaměřeným na lineární písmo B. 1. července 1952 publikoval svůj nejvýznačnější závěr *Work Notě 20,* který se stal bodem zvratu v luštění lineárního písma B. Ventris strávil dva roky rozšiřováním mřížky Koberové do verze, kterou vidíte v tabulce 22. Mřížka se skládá z 5 sloupců pro samohlásky a z 15 řad pro souhlásky, celkem ze 75 buněk s 5 přidanými buňkami pro samostatné samohlásky. Ventris vložil znaky zhruba do poloviny buněk. Mřížka je pravou pokladnicí informací. Například z šestého řádku je možné stanovit, že znaky pro slabiky 3 7, 0 5 a 6 9 sdílejí stejnou souhlásku VI, ale obsahují různé samohlásky 1, 2 a 4. Ventris neměl představu o skutečných hodnotách souhlásek VI nebo

samohlásek 1, 2 a 4. Do tohoto okamžiku odolával pokušení přiřazovat zvukovou podobu jakémukoli ze znaků. Nicméně cítil, že právě teď nastal čas dát na některá tušení, a zkusil uhádnout několik zvukových významů a prozkoumat důsledky.

Ventris si všiml tří slov, která se stále objevovala na několika řádcích tabulek lineárního písma B: 08-73-30-12, 70-52-12 a 69-53-12. Pomocí čiré intuice odhadl, že tato slova mohou být názvy důležitých měst. Ventris už odhadl, že znak 0 8 je samohláska, a proto by jméno prvního města mělo začínat na samohlásku. Jediné význačné jméno, které odpovídalo schématu, bylo Amnisos, důležité přístavní město. Pokud by měl pravdu, potom by druhý a třetí znak 73 a 30 představovaly -m1- a -n1-. Tyto dvě slabiky obsahovaly stejnou samohlásku i, takže by čísla 73 a 30 měla být v mřížce ve stejném sloupci samohlásek - a skutečně je tomu tak. Poslední znak 12 by představoval -so-, přičemž na koncové s by už žádný znak nezůstal. Ventris se rozhodl problém chybějícího s prozatím ignorovat a pokračoval v překladu:

Město 1 = 08-73-30-l2=a-mi-n1-so = Amnisos.

Byl to jen dohad, ale jeho důsledek byl pro Ventrisovu mřížku ohromný. Například znak 12, který vypadal, že představuje -so-, je v druhém sloupci samohlásek a v sedmé řadě souhlásek. Z toho vyplývá, pokud byl odhad správný, že všechny ostatní slabič-né znaky ve druhém sloupci samohlásek obsahují samohlásku o a všechny ostatní slabičné znaky v sedmé řadě souhlásek obsahují souhlásku s.

		Samohlásky				
		1	2	3	4	5
Souhlásky	I					57
	II	40		75		54
	III	39				03
	IV		36			
	V		14			01
	VI	37	05		69	
	VII	41	12			31
	VIII	30	52	24	55	06
	IX	73	15			80
	X		70	44		
	XI	53				76
	XII		02	27		
	XIII					
	XIV			13		
	XV		32	78		
	Samohlásky		61			08

Tabulka 22: Ventrisova rozšířená mřížka pro vztahy mezi znaky lineárního písma B. Přestože mřížka nespecifikuje konkrétní samohlásky nebo souhlásky, osvětluje, Jaké znaky sdílejí společné samohlásky nebo souhlásky. Například všechny znaky v prvním sloupci sdílejí stejnou samohlásku, označenou 1.Když Ventris zkoumal název druhého města, povšiml si, že také obsahuje znak 12: -so-. Další dva znaky 70 a 52 byly ve stejném sloupci samohlásek jako -so-, z čehož vyplývalo, že tyto znaky také obsahují samohlásku o. U druhého města mohl tedy vsunout -so-a o tam, kam patřily, a nechat volná místa pro chybějící souhlásky, což vedlo ke schématu:

Město 2 =70-52-12 =?o-?o-so=?

Mohl by to být Knossos? Znaky mohly představovat ko-no-so. Ventris znovu ignoroval problém chybějícího koncového s, alespoň prozatím. Potěšilo ho, že znak 52, který měl podle předpokladu představovat -no-, byl ve stejné řadě souhlásek jako znak 30, který podle předpokladu měl představovat -n1 - ve jméně Amnisos. To bylo uklidňující, protože pokud obsahovaly stejnou souhlásku n, potom měly být opravdu ve stejné řadě souhlásek. Pomocí informací o slabikách ze dvou dosud odhadnutých jmen vložil Ventris do názvu třetího města následující písmena:

Město 3 =69-53-12 =??-?1-so.

Jediné jméno, které se zdálo vhodné, bylo Tulissos (tu-li-so), důležité město ve střední Krétě. Znovu chybělo na konci s a znovu tento problém Ventris ignoroval. Dosud zkušebně určil tři místní jména a zvukové významy osmi různých znaků:

Město 1 =08-73-30-12 =a-mi-ni-so = Amnisos. Město 2 =70-52-12 = ko-no-so = Knossos. Město 3 =69-53-12 =tu-H-S0 = Tulissos.

Důsledek identifikace osmi znaků byl ohromný. Ventris mohl odvodit hodnoty souhlásek nebo samohlásek mnoha dalších znaků v mřížce, pokud byly ve stejné řadě nebo sloupci. Tím pádem mnoho znaků odhalilo část své slabiky a několik jich šlo určit přesně. Například znak 05 je ve stejném sloupci jako 12 (so), 52 (no) a 70 (ko), atak musí obsahovat o jako svou samohlásku. Podle stejné úvahy je znak 05 ve stejné řadě jako znak 69 (tu), a proto musí obsahovat t jako svou souhlásku. Znak 05 tedy představuje slabiku -to-. Pokud se podíváme na znak 31, zjistíme, že je ve stejném sloupci jako znak 08 (a) a zároveň ve stejné řadě jako znak 12 (s). Proto znak 31 představuje slabiku -sa-.

Odvodit slabiky, které jsou zastoupeny znaky 0 5 a 31, bylo zvláště důležité, protože to Vernisovi dovolilo přečíst dvě celá slova 05-12a05-31, která se často objevovala na konci seznamů. Ventris už věděl že znak 12 představuje slabiku -so-, protože se tento znak objevil ve slově Tulissos, a proto 05-12 lze přečíst jako to-so. Druhé slovo 0 5-31 by se pak četlo jako to-sa. To byl obdivuhodný výsledek. Tato slova se nalézala na konci seznamů, experti proto tušili, že znamenají celkem". Ventris je přečetl jako toso a tosa a uvědomil si, že jsou nápadně podobná archaickému řeckému slovu *tossos* a *tossa, což* je mužský a ženský tvar s významem „tolik". Od svých čtrnácti let, od chvíle, kdy vyslechl přednášku sira Arthura Evanse, stále věřil, že minojský jazyk nemůže být řečtinou. Teď odkryl slova, která byla jasným důkazem, jenž hovořil ve prospěch řečtiny jako *jazyka,* lineárního písma B.

Původní tvrzení, že lineární písmo B není pravděpodobně založeno na řečtině,

vycházelo mimo jiné ze starých kyperských nápisů, z nichž bylo patrné, že řecká slova jsou na rozdíl od lineárního písma B běžně zakončena hláskou s. Ventris objevil, že slova lineárního písma B vskutku zřídka končí na s, ale možná to bylo jednoduše proto, že se hláska s vynechávala jako součást konvence zápisu. Amnisos, Knossos, Tulissos a *tossos* byly také zapsány bez s na konci, takže se zdálo, že se písaři prostě neobtěžovali koncovku s zapisovat a její doplnění ponechávali na čtenáři.

Ventris brzy rozluštil několik dalších slov, která se sice také podobala řečtině, přesto však ještě stále nebyl úplně přesvědčen, že lineární písmo B je řeckým písmem. Teoreticky by se těch několik slov, která rozluštil, mohlo považovat za prvky minojského jazyka, které byly převzaty zvenčí. Cizinec, který přijede do britského hotelu, může občas zaslechnout slova jako „rendezvous" nebo „bon appetit", přesto by z nich mylně usuzoval, že Britové mluví francouzsky. Navíc Ventris narazil na slova, která mu nedávala žádný smysl, a tak je považoval za argument ve prospěch dosud neznámého jazyka. Ve *Work Notě 20* sice hypotézu o řečtině přímo nezavrhl, dal jí však nálepku „lehkovážná odbočka".Tuto teorii uzavřel slovy: „Pokud bych ji sledoval, obával bych se, že by mne tato linie luštění dříve či později přivedla do slepé uličky nebo by se nakonec rozplynula v absurdnostech."

Přes své pochybnosti Ventris dál sledoval i řeckou linii. Zatímco byla *Work Notě 20* stále v oběhu, objevoval další řecká slova. Identifikoval *slova*, *poimen* (pastýř), *kemmeus* (hrnčíř), *chrusovorgos* (zlatník)a *chalkeus* (bronzotepec), a dokonce přeložil několik celých vět. Žádná z očekávaných absurdit mu cestu nezkřížila. Poprvé za tři tisíce let začaly němé nápisy lineárního písma B znovu tiše promlouvat a jazyk, jímž mluvily, byl bezpochyby řečtinou.

V této době, kdy Ventris postupoval s luštěním písma poměrně rychle, byl náhodou požádán, aby vystoupil v rádiu BBC a promluvil k posluchačům o tajemství minojského písma. Ventris se rozhodl, že by to mohla být ideální příležitost pro zveřejnění jeho objevů. Po spíše nudné diskusi o minojských dějinách a lineárním písmu B učinil revoluční prohlášení: „Během posledních několika týdnů jsem došel k závěru, že tabulky z Knossu a Pylosu musí být přece jen psány v řečtině - sice v obtížně čitelné a archaické řečtině, která je o pět set let starší než Homérova řečtina a je psána spíše ve zkrácených formách, ale přesto se jedná o řečtinu." Jedním z posluchačů byl John Chadwick, vědec z Cambridge, který se o luštění lineárního písma B zajímal od třicátých let. Během války pracoval jako kryp-toanalytik v Alexandrii, kde luštil italské šifry, pak přesídlil do Blet-chley Park a svou pozornost soustředil na japonské šifry. Po válce se znovu pokoušel rozluštit lineární písmo B, tentokrát pomocí technik, které se naučil, když pracoval na vojenských kódech. Naneštěstí s malým úspěchem.

Když uslyšel rozhlasový rozhovor, byl naprosto zaražen Ventriso-vým zdánlivě pošetilým tvrzením. Chadwick společně s dalšími vědci kteří poslouchali vysílání, zavrhl Ventrisovy názory jako práci amatéra - jímž v podstatě Ventris opravdu byl. Přesto si jako profesor řečtiny Chadwick uvědomil, že by mu jeho posluchači mohli klást otázky týkající se Ventrisova tvrzení, a proto se rozhodl náležitě

připravit a prověřit Ventrisův názor do všech podrobností. Opatřil si kopii Ventrisových poznámek *Work Notě* a prostudoval je v očekávání, že budou plné děr. Za několik dní se však skeptický vědec stal jedním z prvních zastánců Ventrisovy teorie o lineárním písmu B založeném na řečtině. Chadwick začal mladého architekta brzy obdivovat:

Jeho mozek pracuje udivující rychlostí, takže je schopen promýšlet všechny důsledky určitého předpokladu ještě předtím, než jej vysloví. Má hluboký cit pro realitu situace. Mykéňané pro něj nejsou vágní abstrakcí, ale živoucími lidmi, do jejichž myšlenek se mu daří proniknout. Zdůrazňuje vizuální přístup k problému: s vizuální stránkou textů se obeznámil do té míry, že rozsáhlé úseky textu jsou otištěny v jeho mysli dlouho předtím, než jim rozluštění dá smysl. Pouhá fotografická paměť však nestačí, a tak mu pomáhá jeho vzdělání architekta. Jeho oči nevidí ve stavbě pouhou fasádu, zmatek ornamentálních a strukturálních prvků: hledí do nitra a rozlišují významné části vzoru, jednotlivé prvky struktury a kostru celé stavby. Ventris také dokáže rozlišit mezi matoucí odlišností tajemných znaků, vidí v nich vzory a pravidelnosti, které prozrazují ukrytou strukturu. Právě tato kvalita, schopnost vidět řád ve zdánlivém zmatku, je neklamným znakem velkého člověka."

Ventrisovi však chyběla jedna konkrétní dovednost, totiž důkladná znalost staré řečtiny. Jediné formální vzdělání v řečtině získal jako chlapec ve Stowe School, takže svého objevu nemohl plně využít. Například nebyl schopen vysvětlit některá z rozluštěných slov, protože nepatřila do jeho slovní zásoby. Řecká filologie a studium historického vývoje řeckého jazyka byly specializací Johna Chadwic-ka, který byl proto dobře připraven ukázat, jak tato problematická slova odpovídají teoriím o vývoji nejstarších forem řečtiny. Chadwick a Ventris tvořili dohromady dokonalé partnerství.

Homérova řečtina je stará tři tisíce let, ale řečtina lineárního písma B je o dalších pět set let starší. Aby jí Chadwick porozuměl, musel aplikovat své znalosti staré řečtiny na jazyk lineárního písma B. Bral přitom v potaz tři způsoby, jimiž se jazyk vyvíjí. Za prvé se během doby mění jeho výslovnost. Například řecké slovo „lazebník"se změnilo z *levotrochovoi* v lineárním písmu B na *loutrochoi* v časech Homérových. Za druhé prochází změnami také gramatika. Například v lineárním písmu B je zakončení pro genitiv *-oio,* ale v klasické řečtině je nahrazeno koncovkou *-ou.* Za třetí se může dramaticky vyvíjet slovní zásoba. Některá slova se rodí, jiná umírají, další mění svůj smysl. V lineárním písmu B znamenalo *harmo* „kolo", ale v pozdější řečtině stejné slovo znamená „válečný vůz". Chadwick poukázal na to, že to je podobné tomu, jak se v moderní angličtině používá slovo „wheels" (kola) pro označení auta.

S Ventrisovými schopnostmi luštění a s Chadwickovou odborností v řečtině dvojice mužů pokračovala v přesvědčování zbytku světa, že lineární písmo B je vskutku řečtinou. Rychlost překladu se zvyšovala každým dnem. V Chadwickově zprávě o jejich práci *The Decipherment ofLinear B* (Rozluštění lineárního písma B) se píše:

„Kryptoanalýza je vědou dedukce a kontrolovaného experimentu; hypotézy se tvoří, testují a často zamítají. Ale ostatní nápady, které projdou zkouškami, se rozrůstají, až nakonec v určitém momentu stojí experimentátor na pevné půdě: jeho

hypotéza je ucelená, na povrch vy-plouvají všechny souvislosti a významy. Kód se ‚rozlamuje'. Nejlépe to lze asi definovat jako bod, v němž se pravděpodobná vodítka vynořují rychleji, než je lze sledovat. Je to jako start řetězové reakce v atomové fyzice; jakmile se překročí kritické množství, reakce se šíří sama."

Krátce poté již Chadwick s Ventrisem předváděli své dokonalé zvládnutí problému tak, že jeden druhému psali krátké vzkazy v lineárním písmu B.

Neformálním testem, nakolik je rozluštění textu přesné, je určení počtu bohů. Badatelé, kteří byli v minulosti na špatné cestě, překvapivě vytvářeli nesmyslná slova, která vysvětlovali jako názvy dosud neznámých božstev. Chadwick a Ventris však potřebovali pouze čtyři božská jména, nadto vesměs jména bohů dobře známých.

V roce 1953, jisti si svou analýzou, podrobně popsali svou práci v pojednání skromně pojmenovaném *Evidence for Greek Dialect in the Mycenaean Arcbives* (Důkaz řeckého dialektu v mykénských archivech), jež vyšlo v *The Journal ofHellenic Studies.* Archeologové na celém světě si začali uvědomovat, že jsou svědky revoluce. Německý vědec Ernst Sittig v dopise Ventrisovi shrnul náladu akademické obce: „Opakuji: vaše důkazy jsou kryptograficky nejzajímavější, o jakých jsem kdy slyšel, a jsou vskutku fascinující. Pokud máte

pravdu, pak jsou metody archeologie, etnologie, historie a filologie posledních padesáti let dohnány ad absurdum."

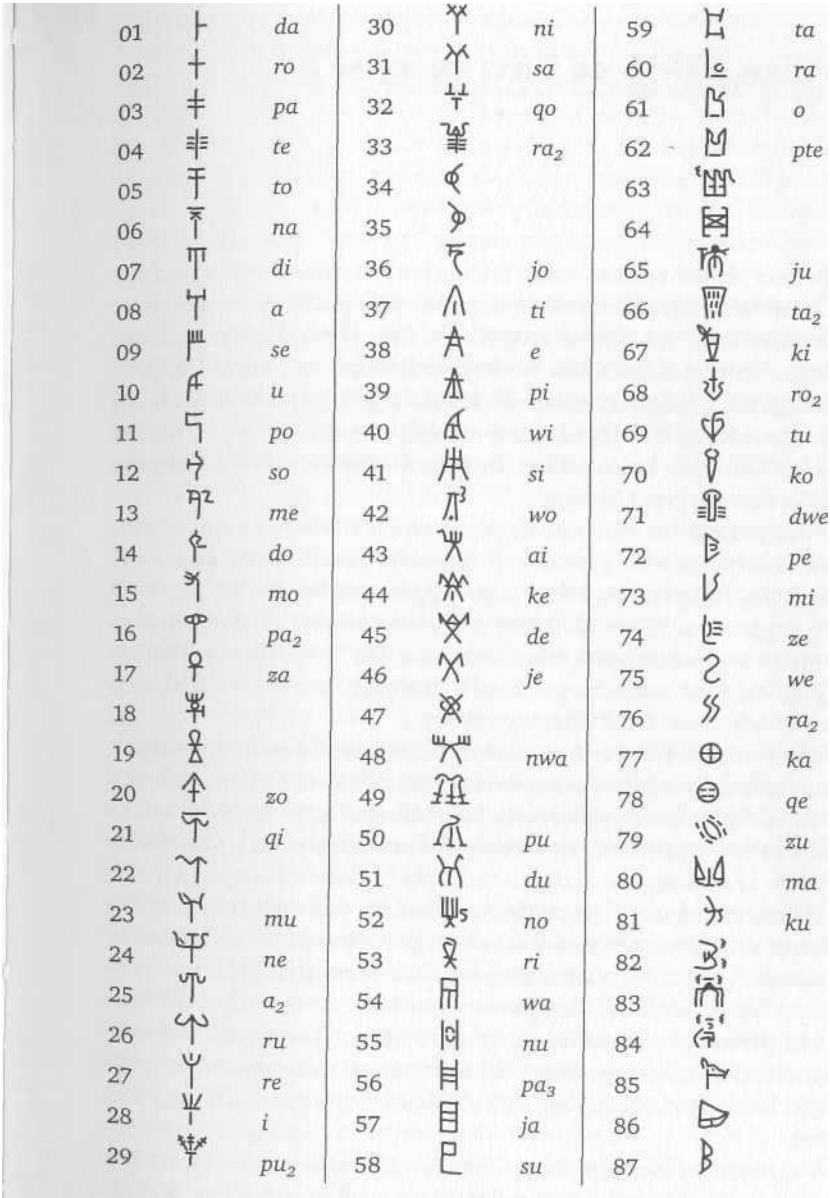
Tabulky s lineárním písmem B popíraly téměř všechno, co tvrdil sir Arthur Evans a jeho generace. Jednak šlo o jednoduchý fakt, že lineární písmo B je řečtina. Za druhé, pokud Minojci na Krétě psali řecky a pravděpodobně také řecky mluvili, pak je třeba přehodnotit pohled na minojské dějiny. Teď se zdá, že dominantní mocností v regionu byly Mykény a že minojská Kréta byla menším státem, jehož obyvatelé mluvili jazykem jejich mocnějšího souseda. Nicméně existují důkazy, že před rokem 1450 př. n. 1. byla minojská říše opravdu nezávislým státem s vlastním jazykem. Právě tou dobou lineární písmo B nahradilo starší lineární písmo A, a přestože obě písma vypadají velmi podobně, lineární písmo A zatím nikdo nerozluštil. Lineární písmo A proto pravděpodobně představuje jazyk odlišný od lineárního písma B. Zdá se pravděpodobné, že zhruba okolo roku 1450 př. n. 1. Mykéňané vojensky porazili Minojce, vnutili jim vlastní jazyk a přeměnili lineární písmo A na lineární písmo B tak, aby fungovalo jako písmo pro řečtinu.

Vyluštění lineárního písma B osvětlilo nejen širší historické souvislosti, ale doplnilo také některé detaily. Tak například: vykopávky v Pylosu neodhalily žádné hodnotnější předměty v jinak přepychovém paláci. To vedlo k podezření, že palác záměrně zapálili *nájezdníci,* kteří z něj nejdříve odnesli hodnotné předměty. Přestože tabulky s lineárním písmem B v Pylosu výslovně nepopisují takový útok, narážejí na přípravy k invazi. Najedná tabulce je zaznamenáno, jak se speciální vojenská jednotka vydala bránit pobřeží, zatímco další tabulka obsahuje příkaz přetavit bronzové ozdoby do hrotů oštěpů. Třetí tabulka, napsaná méně úhledně než předchozí dvě, popisuje pečlivě propracovaný chrámový rituál, který pravděpodobně zahrnoval lidskou oběť. Většina tabulek s lineárním písmem B

obsahuje úhledný text, což by znamenalo, že písaři začínali s hrubým konceptem, který později zničili. Nejméně úhledné tabulky mají vynechané řádky, napůl zaplněné linky a text, který pokračuje až na druhou stranu. Možné vysvětlení je takové, že tato tabulka obsahovala žádost o božskou přímluvu tváří v tvář invazi, ale než ji stihli přepsat načisto, palác byl dobyt.

Převážná část tabulek s lineárním písmem B tvoří seznamy, které popisují každodenní transakce. Naznačují existenci byrokracie, která se může měřit s kteroukoli v historii, množství úředníků, kte-ří zaznamenávali podrobnosti o vyrobeném zboží a zemědělských produktech. Chadwick přirovnával archiv tabulek k *Domesday Book* a profesor Denys Page popisoval úroveň podrobných záznamů takto: „Ať se ovce sčítaly až do závratného počtu dvaceti pěti tisíc, stále jim stálo za to zaznamenat fakt, *že jedno zvíře* dodal nějaký Koma-vens... Zdá se pravděpodobné, že nikdo nemohl zasít zrno, zpracovat ani gram bronzu, utkat šaty, pást kozu či krmit vepře, aniž by se to neobjevilo ve formuláři v královském paláci." Tyto palácové záznamy se mohou zdát všední, ale jsou v podstatě hluboce romantické, protože jsou blízce spojeny s *Odysseou* a *Iliadou.* Když písaři v Knossu a Pylosu zaznamenávali své denní transakce, odehrávala se trojská válka. Jazyk lineárního písma B je jazykem Odyssea.

24. června 1953 Ventris uspořádal veřejnou přednášku, ve které načrtl rozluštění lineárního písma B. Následující den o ní psaly *The Times* hned vedle komentáře o nedávném dobytí Everestu. Díky tomu se Ventrisův a Chadwickův výkon proslavil jako „Everest řecké archeologie". Následujícího roku se oba rozhodli napsat souhrnnou třídílnou monografii o své práci, která by zahrnovala popis rozluštění, detailní analýzu tří stovek tabulek, slovník 630 mykénských slov a seznam zvukových podob téměř všech znaků lineárního písma B (viz tabulka 23). *Documents in Mycenaean Greek* byl dokončen v létě 1955 a připraven k vydání na podzim roku 1956. Několik týdnů před vydáním, 6. září 1956, však Michael Ventris zemřel. Když se vracel autem pozdě v noci domů, narazil jeho vůz na severní výpadovce z Londýna blízko Hatfieldu do nákladního auta. John Chadwick vzdal poctu svému kolegovi - muži, který se vyrovnal Cham-pollionovi a který také zemřel v tragicky mladém věku, slovy: „Práce, kterou udělal, žije a jeho jméno bude připomínáno tak dlouho, dokud budou lidé studovat jazyk a civilizaci starých Řeků."



abulka 23: Znaky lineárního písma B s jejich čísly a zvukovými podobami.**6**

Alice a Bob se baví veřejně

Během druhé světové války měli britští kryptoanalytici nad německými kryptografy navrch, a to především proto, že muži a ženy z Bletchley Park, kteří šli

ve stopách Poláků, vyvinuli první technologie pro luštění šifer. Vedle Turingových bomb, se kterými Britové rozlomili šifru Enigma, vynalezli také další přístroj na luštění kódů Colossus, určený k boji proti ještě silnější německé šifře Lorenz. Byl to právě Colossus, který během druhé poloviny 20. století určil směr dalšího rozvoje kryptografie.

Šifra známá jako Lorenz se používala k šifrování komunikace mezi Hitlerem a jeho generály. K šifrování sloužil přístroj Lorenz SZ40, který fungoval podobně jako Enigma, ale byl daleko složitější a pro kryptoanalytiky z Bletchley představoval ještě větší výzvu. Nicméně dva kryptoanalytici John Tiltman a Bili Tutte objevili slabinu ve způsobu, jakým se šifra používala, skulinku, kterou dokázal Bletchley využít, a číst tak Hitlerovy vzkazy.

Rozlomit šifru Lorenz vyžadovalo kombinaci hledání, porovnávání, statistické analýzy a pečlivého zvažování, což vše přesahovalo technické možnosti bomb. Ty byly schopny provádět specificky úkol s velkou rychlostí, ale nebyly dostatečně pružné, aby mohly zacházet se záludnými vlastnostmi šifry Lorenz. Zprávy zašifrované Lorenzem musely být rozlomeny ručně, což vyžadovalo týdny usilovné námahy, za tuto dobu byly však zprávy již do značné míry zastaralé. Až Max Newman, matematik z Bletchley, přišel na způsob, jak zmechanizovat kryptoanalýzu Lorenzovy šifry. Newman navrhl přístroj vycházející do značné míry z Turingova konceptu univerzálního stroje, který byl schopen adaptace na různé problémy. Dnes bychom jej nejspíš nazvali programovatelným počítačem.

Uskutečnění Newmanova plánu se zdálo být technicky nemožné, takže velení Bletchley jej odložilo do šuplíku. Naštěstí se inženýr Tommy Flowers, který se zúčastnil diskusí o Newmanově plánu,

rozhodl tuto skepsi nepřijmout a pustil se do konstrukce přístroje. Ve výzkumném středisku britských pošt v Dollis Hill v severním Londýně strávil Flowers konstrukcí přístroje na základě Newmano-vých plánů deset měsíců. Výsledkem byl Colossus, který do Bletchley Park dorazil 8. prosince 1943. Skládal se z 1 500 elektronek, jež byly mnohem rychlejší než pomalá elektromechanická relé používaná v bombách. Ale důležitější než rychlost byl fakt, že Colossus byl programovatelný. Proto je Colossus předchůdcem moderního číslicového počítače.

Colossus, stejně jako všechno ostatní v Bletchley Park, byl po válce zničen a ti, kteří na něm pracovali, měli o přístroji zakázáno mluvit. Když Tommy Flowers dostal rozkaz zničit jeho výkresovou dokumentaci, poslušně ji odnesl do kotelny a spálil. Plány prvního počítače na světě byly navěky ztraceny. Utajení vedlo k tomu, že si zásluhy za vynález počítače připsali nakonec jiní vědci. V roce 1945 sestavili J. Presper Eckert a John W. Mauchly z University of Penn-sylvania přístroj ENIAC (Electronic Numerical Integrátor and Cal-culator), který se skládal z 18 000 elektronek a byl schopný vykonat 5 000 výpočtů za vteřinu. Po desetiletí byl za předchůdce všech počítačů považován právě ENIAC, a nikoli Colossus.

Kryptoanalytici přispěli ke vzniku moderního počítače a po válce pokračovali v rozvíjení a aplikacích počítačové technologie pro luštění všech typů šifer. Nyní mohli využívat rychlosti a pružnosti programovatelných počítačů a zkoušet všechny možné klíče, dokud nenalezli ten správný. Kryptografové se jich však

nezalekli a v pravou chvíli *začali* využívat vymoženosti počítačů k tvorbě šifer, které se stávaly stále složitějšími. V poválečné bitvě mezi tvůrci a luštiteli kódů hrály počítače zásadní roli.

Práce s počítačem při zašifrování zprávy se do značné míry podobá tradičním formám šifrování. Mezi počítačovým šifrováním a technikami mechanického šifrování, které byly základem šifer jako Enigma, jsou pouze tři významné rozdíly. První rozdíl spočívá v tom, že mechanický šifrovací přístroj je limitován možnostmi své omezené konstrukce, zatímco počítač může napodobit hypotetický šifrovací přístroj nezměrné složitosti. Počítač lze například naprogramovat tak, aby napodobil činnost stovek scramblerů, z nichž některé se točí po směru hodinových ručiček, některé proti směru, některé zmizí po každém desátém písmenu, některé rotují rychleji [a] rychleji, jak šifrování pokračuje. Takový mechanický přístroj bybylo téměř nemožné postavit, ale jeho „virtuální" počítačový ekvivalent může generovat velmi bezpečnou šifru.

Druhý rozdíl je v rychlosti. Elektronika pracuje daleko rychleji než mechanické scramblery: počítač naprogramovaný na napodobení šifry Enigmy zašifruje dlouhou zprávu během okamžiku. I počítač naprogramovaný na provádění mnohem složitějších forem šifrování dokáže dokončit tento úkol v rozumném čase.

Třetí a asi nejdůležitější rozdíl je v tom, že počítač šifruje ve skutečnosti čísla, nikoli písmena abecedy. Počítače pracují pouze s binárními čísly - s posloupností jedniček a nul známými jako *binary digits* (binární čísla), zkráceně *bits* (bity). Před šifrováním se proto musí každá zpráva převést do binárních čísel. Tento převod lze provést podle různých protokolů, jako například American Standard Code for Information Interchange, ASCII (vyslov aski). ASCII přiřazuje každému písmenu abecedy binární číslo o sedmi číslicích*. Prozatím nám postačí, když si představíme binární čísla pouze jako posloupnost jedniček a nul, které jednoznačným způsobem určují každé písmeno (viz tabulka 24), stejně jako Morseova abeceda určuje každé písmeno jednoznačnou sérií teček a čárek. Existuje 128 (2^7) způsobů, jak uspořádat kombinaci 7 binárních číslic, takže ASCII může sestavit až 128 různých znaků. Toto množství poskytuje dostatek možností k definování všech malých písmen abecedy (např. a - 1100001) a nezbytných interpunkčních znamének (např. ! = 0100001), stejně jako dalších symbolů (např. & = 0100110). Jakmile je zpráva převedena do binární podoby, šifrování může začít.

I když pracujeme s počítači a čísly, nikoli s přístroji a písmeny proces zašifrování probíhá stále jako za starých časů, a to na *základe* principu substituce a transpozice, při kterém se prvky zprávy nahrazují jinými znaky nebo se mění jejich pozice, případně probíhají obě tyto změny najednou. Každé zašifrování, i to sebesložitější, lze rozdělit na tyto dvě jednoduché operace. Následující dva příklady ukazují, jak jednoduché je šifrování pomocí počítačů. Ukážeme si, jak může počítač realizovat elementární substituční šifru a elementární transpoziční šifru.

* To se však týká jeho nejzákladnější verze. Běžné osobní počítače již po léta používají modifikovanou verzi ASCII kódu, která má osm binárních číslic namísto sedmi a tedy 256

různých znaků. Díky tomu lze v ASCII sadě reprezentovat např. česká písmena s diakritickými znaménky.

Nejdříve si představme, že chceme zašifrovat zprávu HELLO použitím jednoduché počítačové verze transpoziční šifry. Než může šifrování vůbec začít, musíme přeložit zprávu do ASCII podle tabulky 24: Otevřenýtext= HELLO = 1001000 1000101 1001100 1001100 1001111

Jedna z nejjednodušších forem transpoziční šifry spočívá v tom, že se vzájemně vymění první a druhá číslice, třetí a čtvrtá a tak dále. V tomto případě zůstane poslední číslice nezměněná, protože číslic je lichý počet. Abychom viděli operaci jasněji, odstranil jsem mezery mezi bloky ASCII v původním otevřeném textu a vytvořil tak jediný souvislý řetězec, který je zapsán pro snazší porovnání přesně nad výsledným šifrovým textem:

Otevřenýtext = 1001000100010110011001001100 1001111 Šifrovýtext = 0110001000101001100110001100 0110111

Zajímavým aspektem transpozice na úrovni binárních číslic je fakt, že se transpozice může odehrát uvnitř písmene. Navíc si bity jednoho písmene mohou měnit místo s bity písmene sousedního. Například výměnou sedmého a osmého čísla se poslední nula z písmene H vymění za počáteční jedničku v písmeni E. Zašifrovaná zpráva je souvislou posloupností 35 binárních číslic, kterou lze poslat příjemci, který pak invertuje transpozici, aby vytvořil původní řádek binárních číslic. Nakonec příjemce prostřednictvím ASCII digitální číslice převede, aby znovu vytvořil zprávu HELLO.

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1011000
L	1001100	Y	1011001
M	1001101	Z	1011010

Tabulka 24: Binární čísla ASCII pro velká písmena.Dále si představme, že si přejeme zašifrovat stejnou zprávu HELLO, ale tentokrát použijeme jednoduchou počítačovou verzi substituční šifry. Znovu začínáme před šifrováním konverzí zprávy do ASCII. Jako obvykle vychází substituce z klíče, který byl dohodnut mezi odesilatelem a příjemcem. V tomto případě je klíčem slovo DAVID přeložené do ASCII, s nímž se pracuje následujícím způsobem: každý prvek otevřeného textu se „přičte" k odpovídajícímu prvku klíče. Sčítání binárních číslic se řídí dvěma jednoduchými pravidly. Pokud jsou prvky otevřeného textu a klíče stejné, prvek otevřeného textu je nahrazen nulou v šifrovém textu. Když se prvky ve zprávě a klíči liší, prvek otevřeného textu se nahradí v šifrovém textu jedničkou.

Původní zpráva HELLO

Zpráva v ASCII 1001000100010110011001001100100111
Klíč = DAV ID 1000100100000110101101001001100010
Šifrový text 0001100000010000110100000101000101 1

Výsledná zašifrovaná zpráva je jediným řádkem 35 binárních číslic, které mohou být poslány příjemci. Ten použije stejný klíč, aby obrátil substituci a znovu tak vytvořil původní řetězec binárních číslic. Nakonec příjemce převede binární číslice přes ASCII, aby vytvořil zprávu HELLO.

Šifrování pomocí počítače bylo v počátcích omezeno pouze na jejich vlastníky, což v raných dobách znamenalo vládu a armádu. Řada vědeckých, technologických a inženýrských objevů však šifrování pomocí počítače postupně zpřístupnila. V roce 1947 vědci v AT&T Bell Laboratories vynalezli tranzistor, levnou alternativu elektronky. Komerční využití počítačů se stalo realitou v roce 1951, kdy firmy jako například Ferranti začaly vyrábět počítače na zakázku. V roce 1953 uvedla IBM na trh svůj první počítač a o čtyři roky později představila Fortran, programovací jazyk, který umožnil „obyčejným lidem" psát počítačové programy. Vynález integrovaného obvodu v roce 1959 znamenal začátek nové éry výpočetní techniky.

Během 60. let výkon počítačů vzrostl a ceny klesly. Firmy si je mohly snáze dovolit a mimo jiné je začaly využívat pro šifrování důležité komunikace, jakou jsou převody peněz nebo delikátní obchodní vyjednávání. Jak si stále více a více firem kupovalo počítače a šifrování se šířilo, kryptografové stáli před novými problémy a těžkostmi, které neexistovaly, dokud byla kryptografie výlučnou oblastí vlády a armády. Jedním z hlavních problémů- byla otázka standardizace. Podnik sice může používat určitý šifrovací systém, aby zabezpečil bezpečnou interní komunikaci, ale poslat tajnou zprávu jiné organizaci již nelze, ledaže by příjemce používal stejný systém šifrování. Americký standardizační úřad National Bureau for Stan-dards začal od 15. května 1973 řešit tento problém tím, že formálně požádal o návrhy standardního šifrovacího systému, který by umožnil firmám utajenou komunikaci o obchodních otázkách.

Jedním z nejpokročilejších šifrovacích algoritmů a kandidátem na standard byl produkt IBM známý jako Lucifer. Vyvinul jej Horst Feistel, německý emigrant, který v roce 1934 přijel do Spojených států. Právě když se měl stát americkým občanem, Spojené státy vstoupily do války, což znamenalo, že na něj uvalily domácí vězení až do roku 1944. Po několik následujících let Feistel potlačoval svůj zájem o kryptografii, aby nevzbudil podezření amerických úřadů. Když nakonec *začal* s výzkumem šifer ve výzkumném středisku vojenského letectva Air Force's Cambridge Research Center, dostal se brzy do potíží s organizací National Security Agency (NSA), která dodnes nese celkovou odpovědnost za zajištění bezpečnosti vojenských a vládních komunikací a již tenkrát se mimo jiné *zabývala*, zachycováním a luštěním cizí komunikace. NSA zaměstnává více matematiků, nakupuje více počítačového hardwaru a zachycuje více zpráv než kterákoliv podobná organizace na světě. V pronikání do důvěrné komunikace je světovou jedničkou.

NSA neměla proti Feistelově minulosti námitky, pouze chtěla mít monopol na kryptografický výzkum. Zřejmě zařídila, aby byl Feistelův výzkumný projekt zastaven. V 60. letech se Feistel přesunul do Mitre Corporation, ale NSA na něho stále vyvíjela svůj tlak, až jej podruhé donutila zanechat práce. Feistel nakonec skončil v IBM - v laboratoři Thomase J. Watsona poblíž New Yorku, kde po několik let mohl vést svůj výzkum, aniž by ho kdokoli obtěžoval. Tam na počátku 70. let vyvinul systém Lucifer.

Lucifer šifruje zprávy podle následujícího schématu: nejdříve se zpráva převede do dlouhého řetězce bitů. Pak se řetězec rozdělí na bloky o 128 bitech a každý blok se šifruje samostatně. Když se soustředíme na jeden takový blok, jeho 128 bitů se rozdělí na dva půlbloky o 64 číslicích, jež můžeme označit $Levý^0$ a $Pravý^0$. Bity v části Pravý" pak projdou

„mandlem", který je změní podle složitých pra-videi. „Zmandlovaná" část Pravý^0 se přičte k Levý^0 a vytvoří se tak nový půlblok se 64 bity pojmenovaný Pravý^1. Původní Pravý^0 se označí jako Levý^1. Tato soustava operací se nazývá „kolo". Celý proces se v dalším kole opakuje, začíná však s novými půlbloky Levý^1 a Pravý^1 a končí s půlbloky Levý^2 a Pravý^2. Tak proběhne celkem šestnáct kol. Proces šifrování připomíná hnětení těsta. Představte si dlouhý plát těsta, na němž je napsána zpráva. Nejdříve se rozdělí do 128 cm dlouhých pásů. Potom se vezme polovina každého pásu, která se promísí („mandluje"), přeloží napůl a prohněte s druhou polovinou, čímž vznikne nový blok. Celý proces se opakuje tak dlouho, až je zpráva zcela promíchána. Po 16 kolech hnětení se šifrový text odešle a na druhém konci se inverzním procesem dešifruje.

Přesné podrobnosti „mandlovací" funkce se mohou měnit. Její vlastnosti jsou určeny klíčem, na němž se dohodnou odesilatel a příjemce. Jinými slovy, zprávu lze zašifrovat nesčíslným množstvím různých způsobů, jež *záleží* na tom, jaký klíč se zvolí. Klíčem používaným v počítačové kryptografii jsou jednoduše čísla. Proto se odesilatel a příjemce musí kvůli definici klíče pouze dohodnout na určitém čísle. Šifrování vyžaduje, aby odesilatel zadal klíčové číslo a zprávu do Lucifera, který potom na výstupu poskytne šifrový text. U dešifrování je tomu naopak: vstupem je klíč a šifrový text, výstupem otevřený text.

Lucifer byl obecně považován zajeden z nejsilnějších komerčně dostupných šifrovacích produktů, proto jej používalo mnoho různých organizací. Zdálo se nevyhnutelné, že tento šifrovací systém bude přijat jako americký standard, ale NSA zasáhla do Feistelovv práce ještě jednou. Lucifer byl totiž tak silný, že mohl sloužit jako šifrovací standard, s nímž by si ale NSA neporadila. Není žádným překvapením, že NSA nechtěla schválit žádný šifrovací standard, který by nedokázala prolomit. Říká se, že než NSA dovolila přijmout za standard Lucifera, lobbovala se záměrem oslabit jeho jeden aspekt, a to počet možných klíčů.

Počet možných klíčů je jedním ze zásadních faktorů, jež určují sílu jakékoliv šifry. Kryptoanalytik, který se snaží rozluštit zašifrovanou zprávu, se může pokusit vyzkoušet všechny možné klíče; čím větší je jejich počet, tím déle bude trvat, než najde ten pravý. V případě pouhého milionu možných klíčů by kryptoanalytik s výkonným počítačem nalezl správný klíč za několik minut a takto rozluštil zachycenou zprávu. Pokud je však počet možných klíčů dostatečně velký, je nalezení toho správného klíče prakticky nemožné. Jestliže se měl Lucifer stát šifrovacím standardem, pak NSA chtěla zajistit, aby pracoval pouze s omezeným počtem klíčů.

NSA argumentovala ve prospěch omezení počtu klíčů na zhruba 100 000 000 000 000 000 možností (technicky řečeno na 56 bitů, protože v binárním zápise sestává toto číslo z 56 číslic). NSA se zřejmě domnívala, že takový klíč by běžné společnosti mohl poskytnout dostatečnou bezpečnost, protože žádná civilní organizace tehdy neměla tak výkonný počítač, aby mohla v rozumném čase prověřit každý možný klíč. Sama NSA by však díky svému přístupu k nejvýkonnější výpočetní technice byla schopna takové zprávy ještě vyluštit. 56bitová verze Feistelova Lucifera byla oficiálně přijata 23. listopadu 1976 a byla nazvána

Data Encryption Standard (DES). O čtvrt století později je DES stále ještě americkým oficiálním standardem pro šifrování.*

Přijetí DES vyřešilo problém standardizace, a tím povzbudilo firmy, aby k zajištění bezpečnosti používaly kryptografii. DES byla natolik silná šifra, že zaručila bezpečnost proti útokům ze strany případných komerčních rivalů. Společnost vybavená běžně dostupnými počítači se prakticky nemohla prolomit do zprávy zašifrované v DES, protože počet možných klíčů byl dostatečně velký. Naneštěstí, bez ohledu na standardizaci a sílu DES, se podniky musely potýkat ještě s jedním zásadním problémem, a sice s *distribucí klíčů.*

Představte si, že banka chce poslat klientovi telefonní linkou důvěrná data, ale obává se, že někdo může linku odposlouchávat. Banka tedy zvolí klíč a k zašifrování zprávy použije DES. Klient pak jednak musí, chce-li zprávu dešifrovat, mít na svém počítači kopii algoritmu DES, jednak musí vědět, jaký klíč byl použit k šifrování zprávy. Jak banka klienta o klíči informuje? Nemůže jej poslat telefonní linkou, protože má podezření, že je odposlouchávána. Jediný zaručeně bezpečný způsob je předat klíč osobně, což je časově náročný úkol. Méně bezpečné, ale praktičtější řešení je poslat klíč po ku-rýrovi. V 70. letech 20. století se banky snažily distribuovat klíče

* Vletech 1998-1999 proběhlo několik luštících akcí (od sestrojení hardwarového luštícího stroje DES-Crackeru po spojení ohromného množství počítačů prostřednictvím internetu), které vážně podlomily důvěru v DES. Od roku 2002 proto úlohu DES nahrazuje nový standard AES (Advanced Encryption Standard). (Pozn. odborného lektora.)

prostřednictvím speciálních kurýrů, kteří museli být prověřeni a zároveň patřili k nejdůvěryhodnějším zaměstnancům banky. Tito kurýři jezdili po celém světě se zamčenými kufříky a osobně distribuovali klíče každému, kdo měl následující týden dostat od banky zprávu. Jak rostla velikost obchodní sítě a počet zpráv v oběhu, bylo nutné distribuovat stále více klíčů, až nakonec banky shledaly, že se tento distribuční proces stává logistickou noční můrou a že režijní náklady jej neúnosně zatěžují.

Problém distribuce klíčů soužil kryptografy po celá staletí. Například během druhé světové války muselo německé vrchní velení distribuovat měsíční knihu denních klíčů všem operátorům Enig-my, což byl ohromný logistický problém. Také ponorky, jež často trávily mnoho času mimo základnu, musely nějak pravidelnou dodávku klíčů obdržet. Již uživatelé Vigeněrovy šifry hledali způsob, jak dostat klíčové slovo od odesilatele k příjemci. Problém distribuce klíčů se může stát pro šifru skutečnou pastí, a to bez ohledu na to, jak je šifra bezpečná.

Vládní a vojenské kruhy se dokázaly s problémem distribuce klíčů do určité míry vyrovnat tak, že jej řešily silou svých peněz a dalších prostředků. Jejich zprávy byly tak důležité, že pro bezpečnou distribuci klíčů byli odesilatelé připraveni udělat cokoli. Klíče používané americkou vládou spravuje a distribuuje COMSEC (Communications Security). V 70. letech byl COMSEC odpovědný za transport několika tun klíčů denně. Když lodě převážející materiál COMSEC dorazily do přístavu, na palubu vstoupili pověření úředníci, vyzvedli stohy děrných

štítků, děrných pásek, disket nebo jiných médií, na nichž byly klíče uloženy, a doručili je určeným příjemcům.

Distribuce klíčů možná vypadá jako banální záležitost, přesto se však stala nejvýznamnějším problémem poválečné kryptografie. Když chtěly dvě strany bezpečně komunikovat, musely se spoléhat na třetí stranu, která doručila klíč, což se stalo nejslabším článkem řetězu bezpečnosti. Dilema komerčního sektoru bylo zřejmé - jestliže vláda přes všechny své vynaložené prostředky těžce zápolila, aby zajistila bezpečnou distribuci klíčů, jak mohly civilní společnosti doufat, že dosáhnou spolehlivé distribuce klíčů, aniž by zbankrotovaly?

Navzdory převládajícímu názoru, že problém distribuce klíčů je neřešitelný, tým specialistů s neotřelým myšlením proti všem předpokladům zvítězil a v polovině 70. let přišel s brilantním řešením.

Specialisté vymysleli šifrovací systém, který jako by popíral veškerou logiku. Přestože počítače změnily implementaci šifer, největší revolucí v kryptografii 20. století byl vývoj metod, které překonaly problém distribuce klíčů. Tento průlom je považován za největší kryp-tografický úspěch od vynálezu monoalfabetické šifry před dvěma tisíci lety.

Bůh odměňuje blázny

Whitfield Diffie je jedním z nejtemperamentnějších kryptogra-fů své generace. Už na pohled je osobou plnou překvapení a protikladů. Jeho bezvadný oblek odráží fakt, že byl po většinu 90. let zaměstnán u jedné z největších amerických počítačových společností - v současnosti má na vizitce s logem firmy Sun Microsystems napsáno „Vynikající inženýr". Vlasy po ramena a dlouhé bílé vousy prozrazují, že jeho srdce stále zůstalo věrné šedesátým letům. Diffie strávil hodně času u počítače, ale vypadá, že by se cítil stejně dobře v bombajském ašramu. Diffie si je vědom toho, že jeho oblékání a zjev mohou mít na ostatní lidi vliv, což komentuje slovy: „Lidé si vždy myslí, že jsem vyšší než ve skutečnosti. Říká se o mně, že to je efekt Tygra: Neboť skáče vysoko, zdá se větší naoko.*"

* Verš z Milneova *Medvídka Pú*, který v běžném českém překladu chybí. Pozn. překl.

Diffie se narodil roku 1944 a většinu svého mládí strávil v newyorské čtvrti Queens. Již v dětském věku ho začala fascinovat matematika. Četl knihy od *The Chemical Rubber Company Handbook ofMa-thematical Tables* (Příručka matematických tabulek společnosti vyrábějící umělou pryž) až po *Course ofPure Mathematics* (Kurs čisté matematiky) od G. H. Hardyho. Matematiku studoval na Massachusetts Institute of Technology, který absolvoval v roce 1965. Potom měl řadu zaměstnání spojených s počítačovou bezpečností, až se začátkem 70. let vypracoval na jednoho z mála skutečně nezávislých expertů na bezpečnost. Diffie byl svobodně uvažující kryptograf, nezaměstnávala ho vláda ani velké korporace. Dnes je zřejmé, že byl prvním šifrujícím punkerem neboli *cipherpunkem.*

Diffieho velmi zajímal problém distribuce klíčů. Uvědomil si, že kdo najde jeho řešení, zapíše se do historie jako jeden z největších kryptografů všech dob. Diffie byl problémem tak *zaujat,* že jej učinil nejdůležitější položkou ve svém speciálním zápisníku nazvaném „Problémy pro ambiciózní teorii kryptografie".

Část Diffieho motivace vycházela z jeho vize propojeného světa. V 60. letech 20. století financovalo americké ministerstvo obrany špičkovou výzkumnou organizaci zvanou Advanced Research Projects Agency (ARPA), k jejímž hlavním úkolům patřilo najít způsob, jak propojit vojenské počítače na velké vzdálenosti. To by umožnilo poškozeným počítačům přenést své úkoly na jiný počítač sítě. Hlavním cílem bylo zvýšit odolnost infrastruktury počítačů Pentagonu vůči jadernému útoku, ale síť měla také umožnit vědcům vzájemně si posílat zprávy a provádět výpočty s využitím volné kapacity vzdálených počítačů. ARPANet vznikl roku 1969 spojením čtyř počítačů na různých místech USA. ARPANet stále rostl a roku 1982 se proměnil v internet. Koncem 80. let k němu získali přístup také uživatelé mimo vládu a mimo akademické kruhy a jejich počet začal prudce růst. Dnes již více než sto milionů lidí používá internet k výměně informací a posílání *zpráv* elektronickou poštou.

Když byl ARPANet ještě v plenkách, Diffie byl už natolik prozíravý, že předpověděl příchod informační superdálnice a digitální revoluce. Obyčejní lidé budou mít jednoho dne své vlastní počítače a tyto počítače budou propojeny přes telefonní linky, říkal. Diffie byl přesvědčen, že pokud budou lidé používat své počítače k zasílání e-mailů, mají právo své zprávy šifrovat, aby si zajistili soukromí. Šifrování však vyžaduje bezpečnou výměnu klíčů. Jestliže vláda a velké

korporace vyřešily distribuci klíčů jen s velkými obtížemi, veřejnost byla zcela bez šancí - pak by však byla zbavena práva na soukromí.

Diffie si představil dvě navzájem cizí osoby, které se setkají na internetu, a uvažoval, jak si mohou zasílat zašifrované zprávy. Bral v úvahu také scénář, kdy si chce osoba přes internet něco koupit. Jak může poslat e-mail obsahující šifrované údaje o kreditní kartě tak, aby je mohl dešifrovat pouze internetový obchodník? V obou případech se *zdálo,* že dvě strany musejí sdílet klíč, ale jak si mohou klíče bezpečně vyměnit? Počet náhodných kontaktů a spontánních e-mailů mezi veřejností by byl enormní a to by znamenalo, že distribuce klíčů by nefungovala. Diffie se obával, že nutnost distribuce klíčů zabrání veřejnosti v přístupu k soukromí ve světě digitálních informací. Stal se přímo posedlý touhou najít řešení tohoto problému.

Roku 1974 navštívil Diffie, stále ještě jako kryptograf na volné noze, laboratoř Thomase J. Watsona ve společnosti IBM, kam jej pozvali, aby přednášel. Hovořil o různých strategiích, jak zaútočit na problém distribuce klíčů, ale všechny jeho myšlenky byly velmi nezávazné a přítomní posluchači se netajili skepsí, co se naděje na úspěch týče. Jediná pozitivní odezva na Diffieho prezentaci přišla od Alana Konheima, jednoho z vedoucích expertů na kryptografii v IBM, který poznamenal, že měl nedávno podobnou přednášku ve Watsonově laboratoři i někdo jiný. Šlo o Martina Hellmana, profesora Stanfordovy univerzity v Kalifornii. Téhož večera Diffie sedl do auta a vyrazil na cestu k západnímu pobřeží dlouhou 5 000 km, aby se setkal s patrně jediným člověkem, jenž zřejmě sdílel jeho posedlost. Spojenectví Diffieho a Hellmana se nakonec stalo jedním z nejdynamičtějších partnerství v kryptografii.

Martin Hellman se narodil roku 1945 v židovské čtvrti v Bronxu, ale když mu

byly čtyři roky, jeho rodina se přestěhovala do části města, kde převažovali irští katolíci. Podle Hellmana to trvale změnilo jeho postoj k životu: „Ostatní děti chodily do kostela a učily se, že židé zabili Krista, začaly mi proto říkat kristovrah. Také mě tloukly. Napřed jsem chtěl být jako ostatní děti, chtěl jsem vánoční stromeček s vánočními dárky. Ale potom jsem si uvědomil, že nemohu být jako ostatní, a v sebeobraně jsem přijal postoj »kdo by chtěl být jako všichni ostatní?«" Hellmanův zájem o šifry souvisí s jeho touhou po odlišnosti. Kolegové mu říkali, že je blázen, když dělá výzkum v kryptografii, protože soutěží s NSA a jejím rozpočtem ně-kolika miliard dolarů. Jak by mohl doufat, že odhalí něco, co by už *tamti* nevěděli? A pokud by něco přece objevil, NSA by to prohlásila za tajné.

Když Hellman začal s výzkumnou prací, narazil na knihu *The Codebreakers* (Luštitelé kódů) od historika Davida Kahna. Tato kníhaje prvním detailním rozborem vývoje šifer a jako taková je dokonalým slabikářem začínajícího kryptografa. *The Codebreakers* byla Hellmanovým jediným společníkem, dokud mu v září 1974 nečekaně nezavolal Whitfield Diffie, který zrovna přejel celý kontinent, aby se s ním setkal. Hellman o Diffiem nikdy neslyšel, a tak bez velkého nadšení souhlasil s půlhodinovou schůzkou téhož odpoledne později. Po schůzce si Hellman uvědomil, že Diffie je nejlépe informovanou osobou, kterou kdy potkal. Jejich pocity byly vzájemné. Hellman na to vzpomíná slovy: „Slíbil jsem své ženě, že budu doma hlídat děti, tak šel domů se mnou a společně jsme povečeřeli. Odešel kolem půlnoci. Naše osobnosti se do značné míry liší - on patří mnohem více k undergroundu než já - ale střetnutí osobností nakonec vedlo k symbióze. Bylo to pro mě jako závan čerstvého vzduchu. Pracovat ve vzduchoprázdnu bylo doopravdy těžké."

Poněvadž neměl Hellman dostatek prostředků, nemohl si dovolit zaměstnat svou novou spřízněnou duši jako výzkumníka. Namísto toho se Diffie zapsal jako postgraduální student. Hellman a Diffie začali společně studovat problém distribuce klíče, přičemž

ze všech sil hledali alternativu k únavnému úkolu fyzického transportu klíčů na velké vzdálenosti. Postupem času se k nim připojil Ralph Merkle. Byl to intelektuální „nomád", který odešel z jiné výzkumné skupiny, jejíž profesor neměl žádné pochopení pro absurdní sen vyřešit problém distribuce klíčů. Hellman uvádí:

„Ralph byl stejně jako my ochotný být za blázna. Chcete-li dosáhnout úspěchu v základním výzkumu, je bláznovství podmínkou, protože jen blázni stále zkoušejí nové věci. Máte nápad číslo 1, nadchnete se pro něj a on selže. Potom máte nápad číslo 2, nadchnete se, on však selže. Potom máte nápad číslo 99, nadchnete se - a on selže. Pouze blázen se dokáže nadchnout i pro stý nápad, protože někdy je jich potřeba opravdu sto, než jeden uspěje. Nejste-li dostatečně šílení, abyste se dokázali udržet v nadšení, pak nebudete mít na takovou práci dost energie a motivace. Bůh odměňuje blázny."

Celý problém distribuce klíčů je klasická situace typu Hlava 22. Pokud si dva lidé chtějí poslat tajnou zprávu telefonicky, odesilatel ji musí zašifrovat. K šifrovaní tajné zprávy musí použít klíč, který je sám o sobě tajný, takže nastává problém, jak jej odeslat příjemci, aby bylo možné poslat tajnou zprávu. Shrnuto: dříve než dva lidé mohou sdílet tajemství (šifrovanou zprávu), musí už jedno tajemství (klíč) sdílet.

Když uvažujeme o problému distribuce klíčů, je užitečné představit si Alici, Boba a Evu, tři fiktivní osoby, které se staly jakýmisi „průměrnými účastníky" pro diskuse o kryptografii. V typické situaci chce Alice poslat zprávu Bobovi nebo naopak, Eva se snaží zprávu zachytit. Když Alice posílá soukromé zprávy Bobovi, každou z nich před odesláním zašifruje, pokaždé jiným klíčem. Alice čelí problému distribuce klíčů, protože musí bezpečně dopravit klíče Bobovi, jinak by nemohl zprávu dešifrovat. Jeden způsob, jak problém vyřešit, je sejít se jednou týdně a vyměnit si dostatečné množství klíčů, aby to pokrylo zprávy, které mohou být zaslány během příštích sedmi dnů. Osobní výměna klíčů je jistě bezpečná, ale nepohodlná, a pokud Alice nebo Bob například onemocní, systém přestane fungovat. Další možností je, že by Alice a Bob mohli najmout kurýry, čímž by sice klesla bezpečnost a vzrostly náklady, ale aspoň část práce by se přenesla na někoho jiného. Tak či onak, zdá [se]> ze distribuce klíčů je nevyhnutelná. Po dva tisíce let to bylo pokládáno za axiom kryptografie - neoddiskutovatelnou pravdu. Nic-méně existuje jeden myšlenkový experiment, který vypadá, jako by tento axiom popíral.

Představte si, že Alice a Bob žijí v zemi, kde je poštovní systém naprosto nemravný a poštovní zaměstnanci čtou veškerou nechráněnou korespondenci. Alice chce poslat velmi soukromou zprávu Bobovi. Vloží ji do kovové skříňky, tu zavře a zamkne. Zamčenou skříňku pošle poštou a nechá si klíč. Když skříňka dorazí k Bobovi, nemůže ji otevřít, protože nemá klíč. Alice by mohla uvažovat o vložení klíče do další skříňky, kterou zamkne a odešle Bobovi, ale bez klíče k druhému zámku nemůže Bob otevřít druhou skříňku a tak se dostat ke klíči, který otevírá první skříňku. Zdánlivě jediným řešením je, aby Alice udělala kopii svého klíče a dala jej Bobovi v předstihu, když se například sejdou na kávu. Doposud jsem pouze shrnul starý známý problém v novém kabátě. Vyhnout se distribuci klíčů se zdá logicky nemožné - je jisté, že když chce Alice zamknout něco ve skříňce tak, aby ji mohl odemknout pouze Bob, musí mu dát kopii klíče. Kryptograficky řečeno, když Alice chce zašifrovat zprávu tak, aby ji mohl dešifrovat pouze Bob, musí mu dát kopii klíče. Výměna klíčů je nevyhnutelnou částí šifrování. Opravdu?

Nyní si představte následující scénář. Stejně jako předtím chce Alice poslat velmi osobní zprávu Bobovi. Znovu vloží svou tajnou zprávu do kovové skříňky, zamkne ji a pošle. Když skříňka dorazí, Bob na ni přidá svůj vlastní zámek a pošle skříňku zpět Alici. Když nyní Alice dostane skříňku, je zabezpečena dvěma zámky. Sejme svůj vlastní zámek a ponechá jen Bobův. Pošle skříňku nazpět Bobovi. A tady je zásadní rozdíl: Bob nyní může otevřít skříňku, protože je zabezpečena pouze jeho vlastním zámkem, k němuž má klíč - pouze on a nikdo jiný.

Důsledky tohoto scénáře jsou ohromující. Úvaha dokazuje, že lze bezpečně

vyměnit tajnou zprávu mezi dvěma osobami, aniž by si nutně musely vyměnit klíč. Poprvé máme naději, že výměna klíčů nemusí být nevyhnutelnou součástí kryptografie.* Nyní můžeme příběh vyprávět znovu, tentokrát v pojmech kryptografie. Alice použije vlastní klíč k zašifrování zprávy Bobovi, který ji znovu zašifruje svým vlastním klíčem a pošle ji nazpět. Když Alice dostane dva

* Výměna klíčů bude pravděpodobně vždy v centru pozornosti kryptografie- Nemusí to být ale nevyhnutelně neřešitelný problém. (Pozn. odborného lektora.)

krát zašifrovanou zprávu, odstraní své vlastní zašifrování a vrátí zprávu Bobovi, který pak snadno odstraní vlastní zašifrování a zprávu přečte.

Zdá se, že problém distribuce klíčů lze vyřešit, protože schéma dvojitého šifrování nevyžaduje íýměnu klíčů. Nicméně zde existuje zásadní překážka, jež brání implementaci systému, v němž Alice zašifruje, Bob zašifruje, Alice dešifruje a Bob dešifruje. Problémem je pořadí, ve kterém se provádí šifrování a dešifrování. Obecně je pořadí šifrování a dešifrování důležité a musí se řídit pravidlem „last on, first off' (jako poslední dovnitř, jako první ven). Jinými slovy, poslední šifrovací krok musí odpovídat prvnímu kroku dešifrování. Ve výše zmíněném scénáři Bob šifroval jako druhý v pořadí, měl by tedy dešifrovat jako první, ale ve skutečnosti to byla Alice, která nejprve odstranila své zašifrování. Důležitost pořadí je snáze pochopitelná, když se zamyslíme nad něčím, co děláme každý den. Ráno si oblečeme ponožky a potom obujeme boty a večer si zujeme boty před svlečením ponožek - je nemožné sundat si ponožky před botami. Musíme se řídit pravidlem „jako poslední dovnitř, jako první ven".

Některé velmi jednoduché šifry (například Caesarova) jsou tak prosté, že pořadí nehraje roli. V 70. letech 20. století se však zdálo, že se jakákoli forma silného šifrování musí vždy řídit výše uvedeným pravidlem. Pokud je zpráva zašifrována Aliciným a pak Bobovým klíčem, potom musí být dešifrována Bobovým klíčem předtím, než ji smí dešifrovat Alice. Pořadí je rozhodující dokonce i u monoalfabetické substituční šifry. Představte si, že Alice a Bob mají vlastní klíče, jak je to naznačeno v následujícím příkladu, a podívejme se, co se děje, když je pořadí nesprávné. Alice použije svůj klíč k zašifrování zprávy Bobovi, potom Bob znovu zašifruje výsledek svým vlastním klíčem; Alice použije svůj klíč, aby provedla částečné dešifrování, a nakonec se Bob snaží použít svůj klíč k provedení úplného dešifrování.

Alicin klíč

```
abcdefghij                    kimnopqrstuvwxyz
HFSUGTAKVDEOYJBPNXWCQRIMZL
```

Bobův klíč

```
abcdefghij                    kimnopqrstuvwxyz
CPMGATNOJEFWIQBURYHXSDZKLV
```

zpráva **meetme at noon**

Zašifrovaná Aliciným klíčem	YGGCYG HC JBBJ
Zašifrovaná Bobovým klíčem	**LNNM LN OM EPPE**
Dešifrovaná Aliciným klíčem	**ZQQX ZQ LX KPPK**

Dešifrovaná Bobovým klíčem **Wnnt wn yt Xbbx**

Výsledek nedává smysl. Můžete si však sami ověřit, že pokud se pořadí dešifrování obrátí a Bob dešifruje před Alicí, takže se dodrží pravidlo „jako poslední dovnitř, jako první ven", výsledkem bude původní zpráva. Pokud je pořadí důležité, jak je možné, že se systém jevil jako funkční v myšlenkovém experimentu se zamčenými skříňkami? U visacích zámků na pořadí *nezáleží.* Skříňku mohu zamknout pomocí dvaceti zámků a odemknout je v jakémkoli pořadí -a nakonec se skříňka otevře. Šifrovací systémy jsou na pořadí bohužel citlivější.

I když myšlenka nadvakrát zamčené skříňky ve světě kryptografie nefunguje, inspirovala Diffieho a Hellmana k hledání praktické metody, jež by obešla problém distribuce klíčů. Měsíc za měsícem trávili hledáním řešení. Přestože každý jejich nápad skončil neúspěchem, chovali se jako správní blázni a vytrvali. Jejich výzkum se týkal různých matematických^íí»fe«'. Funkce je matematická operace, která přiřadí jednomu číslu jiné číslo. Například „zdvojnásobení" je funkce, protože přiřadí číslu 3 číslo 6 nebo číslu 9 jeho dvojnásobek 18. O všech formách počítačového šifrování můžeme uvažovat jako o funkcích, protože přiřadí jednomu číslu v otevřeném textu jiné číslo v textu šifrovém.

Většina matematických funkcí jsou tzv. funkce obousměrné, protože je lze jednoduše provést v jednom i druhém směru. Zdvojnásobení je obousměrná funkce, protože je stejně jednoduché zdvojnásobit číslo jako obrátit operaci a dostat se od zdvojnásobeného čísla zpět k původnímu. Pokud víme, že výsledek zdvojnásobení je 26, je triviální obrátit - matematici říkají invertovat - funkci a odvodit, že původní číslo bylo 13. Nejjednodušší způsob, jak pochopit pojem obousměrné funkce, spočívá v příkladu z každodenního života. Rozsvícení světlaje funkce, protože změní obyčejnou žárovku ve svítící žárovku. Funkce je obousměrná, protože pokud je vypínač zapnutý, je jednoduché světlo vypnout a vrátit žárovku do původního stavu.

Diffieho a Hellmana obousměrné funkce nezajímaly. Svou pozornost zaměřili na funkce jednosměrné. Jak *název* napovídá, jed

nosměrnou funkci je snadné provést, ale těžké obrátit. Obousměrné funkce jsou vratné, jednosměrné nikoli. Smíchání žluté a modré barvy pro vytvoření zelené je jednosměrná funkce, protože je jednoduché barvy smíchat, ale nemožné oddělit. Jinou jednosměrnou funkcí je rozklepnutí vajíčka: je jednoduché vajíčko rozbít, ale nemožné vrátit do původního stavu. Proto se jednosměrným funkcím někdy říká „Humpty Dumpty funkce".*

Modulární aritmetika, jíž se ve škole někdy říká *hodinová aritmetika,* je oblast matematiky, která je na jednosměrné funkce bohatá. V modulární aritmetice pracuje matematik s konečnou množinou čísel uspořádaných do kruhu, což připomíná čísla na ciferníku hodin. Například obrázek 64 ukazuje hodiny pro modulo 7 (formální zápis mod 7), které však mají pouze 7 čísel od 0 do 6. Abychom vypočítali 2 + 3, začneme u 2 a posuneme se o 3 místa na 5, což je stejný výsledek jako v normální aritmetice. Pro vypočtení 2 + 6 začneme u dvou a posuneme se o 6 míst, ale tentokrát uděláme více než celou obrátku a dorazíme k číslul, což není výsledek, který bychom obdrželi v normální aritmetice. Tyto

výsledky mohou být vyjádřeny takto:

2 + 3 = 5 (mod 7) a 2 + 6 = 1 (mod 7)

Modulární aritmetika je relativně snadná a používáme ji každý den, když mluvíme o čase. Když je devět hodin a schůzku máme za 8 hodin, řekneme, že se sejdeme v pět, nikoli v sedmnáct. V duchu jsme vypočítali 9 + 8 (mod 12). Představte si hodiny, podívejte se na 9, posuňte se o 8 míst a skončíte na 5:

9 + 8 = 5 (mod 12)

Namísto názorné pomůcky s hodinami používají matematici pro modulární výpočty následující postup: nejdříve provedou výpočet v normální aritmetice. Když chtějí znát výsledek v (mod *x),* vydělí normální výsledek číslem *x* a zapíšou zbytek po dělení. Tento zbytek je výsledkem v (mod *x).* Abychom vypočetli 11x9 (mod 13) budeme postupovat takto:

* Podle říkanky anglických dětí: „Humpty Dumpty sat on the wall / Humpty Dum-Pty had a great fall / And all the king's horses / And all the king's men / Couldn't put Humpty together again." Humpty Dumpty není nic jiného než vajíčko.

11 x 9 = 99

99/13 = 7, zbytek 8

tedy 11 x 9 - 8 (mod 13)

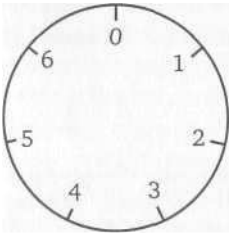
Funkce se v prostředí modulární aritmetiky často chovají nevyzpytatelně, což z nich někdy dělá jednosměrné funkce. Porovnejme jednoduchou funkci v normální aritmetice se stejnou jednoduchou funkcí v aritmetice modulární. V prvním prostředí bude vhodně zvolená funkce obousměrná, ve druhém jednosměrná, tedy irever-zibilní, nevratná. Jako příklad si vezmeme funkci 3*. Ta znamená: vezmi číslo *x* a vynásob číslo 3 samo sebou .r-krát. Pokud například *x = 2*, potom:

$y = 3^2 = 3x3 = 9$

Jinými slovy, tato funkce přiřadí číslu 2 číslo 9. V normální aritmetice s rostoucí hodnotou *x* roste v tomto případě také hodnota funkce. Pokud bychom znali hodnotu funkce, bylo by relativně jednoduché postupovat nazpět a vyvodit původní číslo. Například pokud je funkční hodnota 81, snadno přijdeme na to, že *x* je 4, protože $3^4 = 81$. Když uděláme chybu a odhadneme, že *x* je 5, můžeme vypočítat, že $3^5 = 243$, což nám jasně řekne, že náš odhad pro *x* byl příliš vysoký. Snížíme tedy odhad na 4 a dostaneme správnou odpověď. Zkrátka, i když zpočátku hádáme špatně, nakonec se ke správné hodnotě *x* dopracujeme.

V modulární aritmetice se táž funkce nechová tak rozumně. Představme si, že se dozvíme, že 3* (mod 7) je jedna a máme najít hodnotu *x.* Žádná hodnota nám nevytane na mysli, protože nejsme v modulární aritmetice zběhlí. Můžeme hádat, že *x* - 5 a vypočítat 3^S (mod 7). To je 5, což je příliš veliké číslo - hledáme výsledek 1. Můžeme zkusit snížit hodnotu *x.* Ale to bychom se vydali špatným směrem, protože skutečný výsledek je *x* = 6.

Obrázek 64: V modulární aritmetice se pracuje s konečnou množinou čísel, kterou si můžeme představit jako čísla na ciferníku hodin. V tomto případě vypočítáme *6 + 5* modulo 7 tak, že začneme u čísla 6 a posuneme se o pět míst, což dává číslo 4.



V normální aritmetice můžeme testovat čísla a odhadnout, zda již přihořívá, nebo je to stále „samá voda". Prostředí modulární aritmetiky nedává žádné užitečné nápovědy a inverze funkcí je daleko těžší. Jediný způsob, jak invertovat funkci v modulární aritmetice, často spočívá v sestavení tabulky funkčních hodnot pro mnoho hodnot *x*, dokud se nenajde správný výsledek. Tabulka 25 ukazuje výsledek výpočtu několika hodnot funkcí v obou aritmetikách: normální a modulární. Jasně nám ukazuje nepředvídatelné chování funkcí v modulární aritmetice. Přestože sestavení takové tabulky pro malá čísla je jen trochu nudné, u velkých čísel může představovat značný problém. Představte si, že máte vytvořit tabulku hodnot například pro funkci 453* (mod 21 997). To je klasický příklad jednosměrné funkce, protože lze snadno vypočítat její hodnotu pro libovolné *x*, ale když vám zadám naopak hodnotu funkce, řekněme 5 787, měli byste s inverzní funkcí a výpočtem příslušného *x* obrovské problémy. Výpočet funkční hodnoty 5 787 mi *zabral jen* pár vteřin, ale vám by trvalo celé hodiny sestavit tabulku a nalézt *x*.

Po dvou letech soustředění na modulární aritmetiku a jednosměrné funkce se Hellmanovo bláznovství začalo vyplácet. Na jaře 1976 přišel na strategii vyřešení problému výměny klíčů. Během půlhodiny zběsilých výpočtů, chvatně naškrábaných na papír, dokázal, že se Alice a Bob mohou dohodnout na klíči, aniž by se sešli, a takto popřel axiom, který platil po staletí. Hellmanův nápad spočíval v jednosměrné funkci ve formě *Y"* (mod *P).* Nejdříve se Alice a Bob dohodnou na hodnotách pro *Y a.P*. Mohou je zvolit skoro libovolně, jen s malým omezením, jako například aby *Y* bylo menší než *P*. Tyto hodnoty nejsou tajemstvím, takže Alice může zatelefonovat Bobovi a třeba navrhnout, žeY=7aP= 11. I když není telefonní linka bezpečná a protivná Eva tuto konverzaci uslyší, v podstatě na tom - jak uvidíme později - *nezáleží.* Alice a Bob se tedy domluvili na jednosměrné funkci 7* (mod 11). Od této chvíle mo

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
$3^x \pmod 7$	3	2	6	4	5	1

Tabulka 25: Hodnoty funkce 3* vypočtené v normální aritmetice (řádek 2) a v modulární aritmetice (řádek 3). Funkce je v normální aritmetice stále rostoucí, v modulární aritmetice tuto vlastnost nelze určit.hou začít vytvářet tajný klíč, aniž by se setkali. Protože postupují paralelně, vysvětlím jejich jednání ve dvou sloupcích v tabulce 26.

Když projdete všechny kroky v tabulce 26, uvidíte, že - aniž by se setkali -

Alice a Bob se dohodli na stejném klíči, který nyní mohou použít k šifrování zpráv. Mohou své číslo, tedy 9, využít například jako klíč pro šifru DES. (DES ve skutečnosti používá jako klíče daleko větší čísla, takže proces výměny popsaný v tabulce 26 by bylo třeba provést s daleko většími čísly; pak by jeho výsledkem mohl být použitelný klíč DES.) Pomocí Hellmanova schématu se Alice a Bob byli schopni domluvit na klíči, aniž by se předtím museli sejít a klíče si navzájem sdělit. Tajný klíč byl dohodnut výměnou informací normální telefonní linkou. Ale pokud Eva jejich linku odposlouchávala, dá se s určitostí říci, že také zná klíč?

Podívejme se na Hellmanovo schéma z Evina úhlu pohledu. Pokud odposlouchává linku, zná pouze následující fakta: funkce je *7″* (mod 11). Alice poslala oc= 2. Bob poslal (3 = 4. Aby Eva našla klíč, musí udělat buď totéž co Bob, tedy změnit a v klíč tím, že zná *B,* nebo totéž co Alice, tedy změnit (3 v klíč tím, že zná *A.* Eva však nezná hodnotu *A* ani *B,* protože Alice a Bob si tato čísla nevyměnili a zachovali je v tajnosti. Eva je v koncích. Má pouze jedinou naději: teoreticky může vypočítat *A* z hodnoty a, protože a vznikla důsledkem vložení *A* do funkce, a Eva funkci zná. Nebo může vypočítat *B* z hodnoty (3, protože |3 byla výsledkem vložení *B* do funkce. Naneštěstí pro Evu je funkce jednosměrná, takže Alice může snadno proměnit *A* na a a Bob lehce změní *B* na (3, avšak pro Evu je velmi těžké proces obrátit, zvláště když jsou čísla velmi velká.

Bob a Alice si vyměnili právě tolik informací, aby mohli ustanovit klíč, ale tato informace nestačí Evě, aby mohla klíč vypočítat. Jako analogii k Hellmanově schématu si představte šifru, která nějakým způsobem používá jako klíče barvy. Nejdřív předpokládejme, že každý včetně Alice, Boba a Evy má třílitrovou nádobu obsahující litr žluté barvy. Alice a Bob se chtějí domluvit na tajném klíči, proto každý z nich přidá do nádoby jeden litr jejich vlastní tajné barvy. Alice může například přidat purpur, zatímco Bob přidá karmín. Oba pošlou svou nádobu s namíchanou barvou druhému partnerovi. Nakonec vezme Alice Bobovu směs a přidá litr vlastní tajné barvy, Bob stejně tak vezme Alicinu směs a přidá litr vlastní tajné barvy. Obě nádoby by nyní měly obsahovat stejnou barvu, protože obě obsahují jeden litr žluté, jeden litr purpurové a jeden litr

	Alice	Bob
Krok 1	Alice zvolí například číslo 3 a uchová jej v tajnosti. Její číslo označíme jako *A*.	Bob zvolí například číslo 6 a uchová jej v tajnosti. Jeho číslo označíme jako *B*.
Krok 2	Alice vloží 3 do jednosměrné funkce a vypočítá výsledek 7^A (mod 11): 7^3 (mod 11) = 343 (mod 11) = 2.	Bob vloží 6 do jednosměrné funkce a vypočítá výsledek 7^B (mod 11): 7^6 (mod 11) = 117 649 (mod 11) = 4.
Krok 3	Alice nazve výsledek tohoto výpočtu α a pošle svůj výsledek (2) Bobovi.	Bob nazve výsledek tohoto výpočtu β a pošle svůj výsledek (4) Alici.
Výměna	Normálně by právě toto byl rozhodující moment, protože Alice a Bob si vyměňují informace, a tudíž se Evě naskýtá příležitost naslouchat a dozvědět se všechny podrobnosti. Ukáže se však, že Eva sice může naslouchat, ale bezpečnost systému neovlivní. Alice a Bob mohou klidně použít stejnou telefonní linku, kterou se domlouvali na hodnotách *Y* a *P*, a Eva může zachytit dvě čísla, která si sdělují, tedy 2 a 4. Tato čísla však nejsou klíčem, a proto nezáleží na tom, zda je Eva zná.	
Krok 4	Alice vezme Bobův výsledek a vypočítá β^A (mod 11): 4^3 (mod 11) = 64 (mod 11) = 9.	Bob vezme Alicin výsledek a vypočítá α^B (mod 11): 2^6 (mod 11) = 64 (mod 11) = 9.
Klíč	Alice a Bob zázračně dospěli ke stejnému číslu – 9. To je klíč!	

karmíno

Tabulka 26: Obecná jednosměrná funkce je *Y** (moci *P).* Alice a Bob zvolili hodnoty Faí>, čímž se shodli na jednosměrné funkci *7"* (mod 11).

vé. Tato výsledná barva, která vznikla dvojnásobným promícháním obsahu nádoby, slouží jako klíč. Alice neví, kterou barvu přidal Bob, a Bob nemá představu, kterou barvu přidala Alice, ale oba dospěli ke stejné směsi. Eva mezitím zuří. I kdyby zachytila barvy v době výměn, nemůže zjistit konečnou barvu, která je smluveným klíčem. Může spatřit zabarvení směsi, která obsahuje původní žlutou a Ali-cinu tajnou barvu, na její pouti k Bobovi a může také zahlédnout zabarvení směsi, která obsahuje kromě žluté také Bobovu tajnou barvu, na její cestě k Alici, ale aby zjistila klíč, potřebuje znát Alici-nu a Bobovu původní tajnou barvu. Tyto tajné barvy se však ze smě-si nedají nijak zjistit - ani odebráním vzorku. Míchání barev je jednosměrná funkce.

Hellman dostal rozhodující nápad, když jedné noci pracoval doma, takže po dokončení výpočtu bylo již příliš pozdě, aby zavolal Diffiemu a Merklovi. Musel čekat do následujícího rána, než svůj objev odhalil jediným lidem na světě, kteří věřili, že problém distribuce klíčů má vůbec řešení. „Múza mi to pošeptala," říká Hellman, „ale my všichni jsme položili společně základy." Diffie okamžitě roz-

poznal sílu Hellmanova objevu: „Marty vysvětlil svůj systém výměny klíčů v celé jeho zdrcující jednoduchosti. Když jsem ho poslouchal, uvědomil jsem si, že ta představa byla po nějaký čas zasuta někde v mé hlavě, ale nikdy se neprodrala ven."

Schéma výměny klíčů Diffíe-Hellman-Merkle ve své základní podobě umožňuje Alici a Bobovi sdílet tajemství veřejnými prostředky. Jde o jeden z nejméně intuitivních objevů v historii přírodních věd. Kryptografové museli kvůli němu přepsat pravidla šifrování. Diffie, Hellman a Merkle veřejně oznámili svůj objev na National Computer Conference v červnu 1976 a ohromili publikum expertů na kryptografii. Následujícího roku zažádali o patent. Napříště se Alice a Bob už nemuseli setkávat, aby si vyměnili klíč. Místo toho Alice mohla jen zavolat Boba telefonem, vyměnit si s ním pár čísel, vzájemně ustanovit tajný klíč a přikročit k šifrování.

Přestože výměna klíčů Diffie-Hellman-Merkle byla obrovským skokem dopředu, systém nebyl dokonalý, protože byl nepohodlný. Představte si, že Alice žije na Havaji a chce poslat mail Bobovi v Istanbulu. Bob pravděpodobně spí, ale krása e-mailu spočívá v tom, í e Alice může zaslat mail kdykoli. Zpráva bude čekat v Bobově počítači, až se probudí. Pokud však Alice chce svou zprávu zašifrovat, potřebuje se s Bobem dohodnout na klíči, a aby provedli výměnu klíčů, musí být oba ve stejný čas připojeni on-line - ustanovení klíče totiž vyžaduje vzájemnou výměnu informací. Alice tedy musí počkat, až se Bob vzbudí. Nebo může odeslat svou část výměny klíčů a čekat 12 hodin na Bobovu odpověď. Pak je klíč ustanoven a Alice může, pokud nespí zase ona, zašifrovat a poslat zprávu. Hellmanova výměna klíčů rozhodně neodpovídá asynchronní podstatě e-mailu.

Přesto Hellman rozbil na kusy jedno z dogmat kryptografie a dokázal, že Alice a Bob se nemusí setkat, aby se dohodli na tajném klíči. Teď už bylo jen třeba zavést efektivnější metodu pro distribuci klíčů.

Zrození kryptografie s veřejným klíčem

Mary Fisherová nikdy nezapomene na to, jak ji poprvé Whitfield Diffie požádal o schůzku. „Věděl, že jsem nadšenec pro vesmír, tak navrhl, abychom se šli podívat na odpálení rakety. Whit vysvětlil, že ten večer odjíždí, aby viděl start Skylabu, tak jsme jeli celou noc a dostali jsme se tam okolo tří hodin ráno. Ptáček byl na cestě, jak se tehdy říkalo. Whit měl novinářskou akreditaci, já však ne. Když tedy chtěli můj průkaz a ptali se, kdo jsem, Whit řekl: ‚Moje žena.' To bylo 16. listopadu 1973." Nakonec se opravdu vzali a během prvních let manželství Mary podporovala svého manžela v jeho kryp-tografických meditacích. Diffie byl stále na postgraduálu, což znamenalo, že dostával pouze skrovný plat. Mary, vystudovaná archeoložka, přijala práci u British Petroleum, aby měli z čeho žít.

Když Martin Hellman vyvíjel svou metodu, Whitfield Diffie pracoval na úplně odlišném přístupu k řešení problému distribuce klíčů. Často

procházel dlouhými obdobími neproduktivního přemýšlení, v roce 1975 byl už tak frustrovaný, že se v rozhovoru s Mary označil za pouhého neúspěšného vědce, z něhož nikdy nic nebude. Dokonce jí řekl, že by si měla najít někoho jiného. Mary mu však vyjádřila naprostou důvěru. Pouhé dva týdny poté Diffie přišel se svou vskutku brilantní myšlenkou.

Ještě dnes si dovede vzpomenout, jak mu ta myšlenka probleskla hlavou a on skoro omdlel: „Šel jsem dolů pro colu a málem jsem na svůj nápad zapomněl. Uvědomoval jsem si, že jsem přemýšlel o něčem zajímavém, ale nemohl si vzpomenout, co to přesně bylo. Pak se to vrátilo ve skutečně adrenalinovém přívalu vzrušení. Opravdu jsem si byl poprvé během své práce v kryptografii jist, že jsem objevil něco skutečně hodnotného. Vše, co jsem v oboru do té doby objevil, mi náhle připadalo jako maličkosti." Bylo teprve brzy odpoledne a Diffie musel čekat několik hodin, než se vrátí jeho žena. „Whit čekal u dveří," vzpomíná Mary. „Řekl, že se mi chce s něčím svěřit, a měl zvláštní výraz ve tváři. Vešla jsem dovnitř a on řekl: ‚Po-sad" se, prosím, chci s tebou mluvit. Domnívám se, že jsem udělal velký objev - vím, že jsem první, kdo to dokázal.' Svět se na chvíli zastavil. Připadala jsem si jako v hollywoodském filmu."

Diffie vymyslel nový typ šifry, která zahrnovala takzvaný *asymetrický klíč*. Všechny způsoby šifrování dosud popsané v této knize jsou *symetrické*, což znamená, že proces dešifrování je přesným opa-kem šifrování. Například přístroj Enigma používal určitý klíč k zašifrování *zprávy* a příjemce použil identický přístroj se stejným klíčem k dešifrování. Podobně se při šifrování v DES používá klíč, který funguje v 16 kolech šifrování, a při dešifrování se pracuje s týmž klíčem, který platí v 16 kolech v opačném směru. Odesilatel i příjemce pracují se stejnou informací a používají stejný klíč k šifrování i dešifrování - jejich vztah je tedy symetrický. V systému asymetrických klíčů, jak název napovídá, klíče pro zašifrování a pro dešifrování totožné nejsou. V asymetrické šifře, pokud Alice zná šifrovací klíč, může zprávu zašifrovat, ale ne dešifrovat. Aby ji dešifrovala, musí mít přístup k dešifrovacímu klíči. Tento rozdíl mezi šifrovacím a dešifrovacím klíčem je speciální vlastností asymetrické šifry.

V tomto bodě stojí za to zdůraznit, že přestože Diffie formuloval obecný pojem asymetrické šifry, nevěděl, jak ji realizovat. Už pouhý pojem asymetrické šifry však byl revoluční. Pokud by kryptografové vymysleli reálně fungující asymetrickou šifru, tedy systém, který by splňoval Diffieho podmínky, pak by byly důsledky pro Alici a Boba nesmírné. Alice by mohla vytvořit vlastní dvojici klíčů: šifrovací a dešifrovací. Pokud bychom předpokládali, že asymetrická šifra je druh počítačového šifrování, potom Alicin šifrovací klíč je číslo a její dešifrovací klíč je jiné číslo. Alice uchová v tajnosti dešifrovací klíč, jemuž se pak bude říkat Alicin *soukromý klíč*. Šifrovací klíč však zveřejní tak, aby k němu měl každý přístup, ten pak nazveme Alicin *veřejný klíč*. Pokud chce Bob Alici poslat zprávu, najde její veřejný klíč, který se bude uvádět v něčem podobném, jako je telefonní seznam.

Bob použije Alicin veřejný klíč k zašifrování zprávy. Zašifrovanou zprávu pošle Alici, která ji dešifruje pomocí svého soukromého dešifrovacího klíče. Podobně když Charlie, Dawn nebo Edward chtějí poslat Alici šifrovanou zprávu, také si vyhledají Alicin veřejný šifrovací klíč. V každém případě má pouze Alice a nikdo jiný přístup k soukromému dešifrovacímu klíči, který je zapotřebí k dešifrování zprávy.

Obrovská výhoda tohoto systému spočívá v tom, že neobsahuje žádnou synchronní komunikaci, jak tomu bylo při výměně klíčů Diffie-Hellman-Merkle. Bob nemusí čekat na informace od Alice, aby jí mohl zašifrovat a odeslat zprávu, pouze musí vyhledat její veřejný šifrovací klíč. Kromě toho řeší asymetrická šifra také problém distribuce klíčů. Alice není nucena dopravit veřejný šifrovací klíč Bobovi tajně: naopak, nyní může svůj veřejný šifrovací klíč zveřejnit

tak široce, jak je to jen možné. Chce, aby celý svět znal její veřejný šifrovací klíč, aby jej každý mohl použít k zaslání šifrované zprávy. Zároveň, i když celý svět zná Alicin veřejný klíč, nikdo, ani zlá Eva, nemůže jím zašifrovanou zprávu dešifrovat, protože znalost veřejného klíče není v dešifrování nic platná. Jakmile Bob jednou zašifruje zprávu pomocí Alicina veřejného klíče, není ji schopen rozluštit ani on sám. To může udělat pouze Alice, která má soukromý klíč.

To je naprostý opak tradiční symetrické šifry. V té je šifrovací a dešifrovací klíč totožný, takže Alice a Bob by museli být velmi obezřetní, aby zajistili, že klíč nepadne Evě do rukou. To je podstata problému distribuce klíčů.

Když se vrátíme k analogii se zámky, můžeme si představit asymetrickou kryptografii následujícím způsobem: kdokoli může zamknout zámek jednoduše tak, že jej zaklapne, ale jedině ta osoba, která má klíč, jej může odemknout. Zamknutí je snadné, zvládne to kdokoli, ale odemknutí (tedy dešifrování) je schopen provést pouze vlastník klíče. Triviální znalost toho, jak zaklapnout zámek, aby byl zamčený, nám neříká nic o tom, jak jej odemknout. Pokud rozvedeme tuto analogii dále, představíme si, že Alice navrhne zámek a klíč. Uschová klíč, ale vyrobí stovky kopií zámku a rozveze je na pošty všude po světě. Pokud chce Bob poslat zprávu, vloží ji do skříňky, jde na místní poštu, řekne si o „Alicin zámek" a zamkne skříňku. Teď už Bob skříňku neodemkne, ale když ji Alice obdrží, může ji otevřít svým klíčem, který nemá nikdo jiný. Zámek a proces zaklapnutí je ekvivalentní veřejnému šifrovacímu klíči, protože každý má přístup k zámkům a každý může použít zámek k tomu, aby zapečetil zprávu ve skříňce. Klíč k zámku je ekvivalentní soukromému dešifrovacímu klíči, protože jej má pouze Alice, pouze ona může otevřít zámek a pouze ona má přístup ke zprávě ve skříňce.

Systém vypadá jednoduše, pokud je vysvětlen v pojmech zámků, ale není zdaleka triviální najít matematickou funkci, která vykoná stejnou práci - něco, co lze začlenit do realizovatelného kryptogra-fického systému. Aby se asymetrická šifra proměnila ze skvělého nápadu v praktický objev, musel někdo objevit vhodnou matematickou funkci. Diffie uvažoval o speciálním typu jednosměrné funkce, kterou by šlo za speciálních podmínek invertovat. V Diffieho asymetrickém systému Bob zašifruje zprávu veřejným klíčem, ale nemůže ji dešifrovat - to je v podstatě jednosměrná funkce. Alice vsak zprávu dešifrovat

může, protože má svůj soukromý klíč, speci-ální informaci, která jí umožní funkci invertovat. Znovu jsou dobrou analogií zámky - zaklapnutí visacího zámku je jednosměrná funkce, protože obvykle je těžké zámek otevřít, pokud nemáte něco speciálního, tedy klíč.

Diffie publikoval íiáčrt své myšlenky v létě 1975, poté se ostatní vědci přidali k hledání vhodné jednosměrné funkce, která by splňovala podmínky nutné pro asymetrickou šifru. Na začátku byli všichni plni optimismu, ale do konce roku nikdo vhodného kandidáta nenašel. Jak měsíce plynuly, zdálo se čím dál více pravděpodobné, že speciální jednosměrné funkce potřebných vlastností neexistují. Zdálo se, že Diffieho myšlenka funguje v teorii, ale ne v praxi. Přesto tým Diffieho, Hellmana a Merkla způsobil v kryptografickém světě revoluci. Přesvědčili zbytek světa, že problém distribuce klíčů má řešení, a vytvořili model výměny klíčů Diffie-Hellman-Merkle -uskutečnitelný, ale nedokonalý systém. Také navrhli koncept asymetrické šifry - sice dokonalý, ale ještě neuskutečnitelný systém. Ve svém výzkumu pokračovali na Stanfordově univerzitě ve snaze najít speciální jednosměrnou funkci, která by učinila asymetrickou šifru skutečností. Nedokázali to. Závod v hledání asymetrické šifry vyhrála jiná trojice výzkumníků, usazená 5 000 km daleko na východním pobřeží Ameriky.

Podezřelá prvočísla

„Vešel jsem do pracovny Rona Rivesta," vzpomíná Leonard Adie-man, „a Ron měl ten článek v ruce. Povídá: ‚Tihle kluci ze Stanfordu to fakt zmákli,' a pokračoval složitými detaily. Vzpomínám si, že jsem si pomyslel: ‚To je pěkné, Rone, ale rád bych si s tebou o něčem promluvil.' Vůbec nic jsem netušil o historii kryptografie a vůbec mě nezajímalo, co říká." Autory článku, který tak zaujal Rona Rivesta, byli Diffie a Hellman, v článku se popisoval koncept asymetrické šifry. Rivest nakonec přesvědčil Adlemana, že problém může obsahovat nějakou zajímavou matematickou myšlenku, a společně se rozhodli najít jednosměrnou funkci, která by splňovala podmínky asymetrické šifry. K jejich lovu se připojil Adi Shamir. Všichni tři muži byli výzkumníci z osmého poschodí laboratoře počítačových věd MIT.

Rivest, Shamir a Adleman vytvořili dokonalý tým. Rivest je počítačový vědec s obrovskou schopností absorbovat nové myšlenky

a aplikovat je na nepravděpodobných místech. Vždy držel krok s posledními vědeckými objevy, které ho inspirovaly k tomu, že přicházel s celou řadou podivných a zajímavých návrhů na jednosměrnou funkci jako srdce asymetrické šifry. Každý z nich však byl nějakým způsobem chybný. Shamir, další počítačový vědec, má bleskový intelekt a schopnost vidět skrz nepodstatné věci, soustředit se na jádro problému. Také on přicházel s nápady na realizaci asymetrické šifry, ale i jeho návrhy byly neúspěšné. Adleman, matematik s obrovskou energií, disciplínou a trpělivostí, se zaměřil na hledání chyb v nápadech Rivesta a Shamira v obavě, aby neplýtvali časem, kdyby se vydali po falešné stopě. Rivest a Shamir přicházeli po celý rok s novými a novými nápady a Adleman strávil tentýž

rok tím, že je rozcupovával. Trojice již začínala ztrácet naději; vědci si neuvědomovali, že tato série porážek je nezbytnou součástí jejich výzkumu a že je postupně vede od neplodných nápadů k zajímavějším myšlenkám. Jejich snaha byla nakonec odměněna.

V dubnu 1977 slavili všichni tři společně pesach, vypili trochu více košer vína a poté se po půlnoci rozešli do svých domovů. Rivest, který nemohl spát, si lehl na gauč a četl matematickou učebnici. Začal znovu přemítat nad otázkou, se kterou si lámal hlavu už týdny - je možné vytvořit asymetrickou šifru? Je možné najít jednosměrnou funkci, která může být převrácena pouze tehdy, když příjemce má nějakou speciální informaci? Najednou se mlha rozestoupila a Rivest dostal nápad. Zbytek noci strávil formalizací své myšlenky. Do úsvitu napsal v podstatě celý odborný článek. Rivestdosáhl objevu, který však vyrostl z jeho roční spolupráce s Shamirem a Adlemanem, bez nich by nebyl možný. Proto zakončil svou stať tím, že uvedl autory seřazené podle abecedy: Adleman, Rivest, Shamir.

Následujícího rána předal Rivest článek Adlemanovi, který se jej jako obvykle pokusil rozcupovat na kusy, ale tentokrát nemohl žádné chyby najít. Jeho jediná výtka se týkala seznamu autorů. „Řekl jsem Ronovi, aby mé jméno vynechal," vzpomíná si Adleman. „Řekl jsem mu, že to byl jeho objev, ne můj. Ale Ron nesouhlasil a tak jsme o tom diskutovali. Shodli jsme se, že půjdu domů a přes noc to zvážím. Dalšího dne jsem Ronovi navrhl, že budu třetím autorem. Měl jsem za to, že půjde o nejméně významný článek, pod jakým budu kdy podepsán." Adleman se nemohl mýlit více. Systém nazvaný RSA (Rivest, Shamir, Adleman), nikoli tedy jak bylo původně zamýšleno ARS, se stal nejvlivnějším pojmem moderní kryptografie.

Než se pustíme do zkoumání Rivestovy myšlenky, zde je krátké připomenutí toho, co vědci potřebovali najít, aby vytvořili asymetrickou šifru.

(1) Alice musí vytvořit veřejný klíč, který pak zveřejní, aby jej Bob (a kdokoliv jiný) mohl použít k šifrování zpráv určených jí. Protože je šifrování veřejným klíčem jednosměrná funkce, musí být prakticky nemožné ji invertovat a Aliciny zprávy dešifrovat.

(2) Alice naopak potřebuje dešifrovat zprávy, jež obdrží. Musí proto mít soukromý klíč, speciální informaci, která jí umožní obrátit efekt veřejného klíče. Tudíž Alice (a pouze Alice) musí mít možnost dešifrovat jakoukoli zprávu, kterou obdrží.

Základem Rivestovy asymetrické šifry je jednosměrná funkce téhož typu jako modulární funkce popsané v této kapitole dříve. Ri-vestovu jednosměrnou funkci lze použít k zašifrování zprávy. Zpráva není ničím jiným než číslem, toto číslo se vloží do funkce a výsledkem je šifrový text, další číslo. Nebudu Rivestovu jednosměrnou funkci popisovat do detailů (ty můžete najít v příloze J), ale vysvětlím jeden její zvláštní aspekt, známý jednoduše jako *N*, protože právě tento aspekt umožňuje tuto jednosměrnou funkci za určitých podmínek invertovat a tím ji předurčuje pro roli asymetrické šifry.

N je důležité, protože je proměnnou součástí jednosměrné funkce, což znamená, že si každá osoba může vybrat vlastní hodnotu *N* a personalizovat tak jednosměrnou funkci. Aby Alice stanovila svou

osobní hodnotu *N,* zvolí dvě prvočísla *p* a *q,* která mezi sebou vynásobí. Prvočíslo je takové číslo, které nemá jiné dělitele než sebe sama a číslo 1. Například 7 je prvočíslo, protože žádná čísla kromě 1 a 7 jej nedělí beze zbytku. Podobně 13 je prvočíslo, protože žádná čísla kromě 1 a 13 jej nedělí beze zbytku. 8 však prvočíslo není, protože je beze zbytku dělitelné ještě 2 a 4.

Alice tedy vybere svá prvočísla*p* = 17 159 a *q* = 10 247. Vynásobením čísel mezi sebou dostane *N* = 17 159 x 10 247 = 175 828 273. Ali-cino *N* se stane jejím veřejným šifrovacím klíčem. Může jej tisknout na své vizitky, publikovat na internetu nebo zveřejnit v seznamu veřejných klíčů spolu s hodnotami *N* kohokoli dalšího. Když chce Bob zašifrovat zprávu pro Alici, najde Alicinu hodnotu *N,* tedy číslo 175 828 273, a potom ji vloží do obecné podoby jednosměrné funkce, která je také veřejně známá. Bob má nyní jednosměrnou funkci konkretizovanou Aliciným veřejnými klíčem - můžeme jí říkat Ali-cina jednosměrná funkce. Aby zašifroval zprávu pro Alici, vezme Alicinu jednosměrnou funkci, vloží zprávu, zapíše výsledek a pošle jej Alici.

V této chvíli je zašifrovaná zpráva bezpečná, protože ji nikdo není schopen dešifrovat. Zpráva byla zašifrována jednosměrnou funkcí; inverze takové funkce, jež by byla nezbytná pro dešifrování, je krajně obtížná, jak již víme. Jak však může sama Alice zprávu dešifrovat? Jak může invertovat jednosměrnou funkci? Rivest navrhl jednosměrnou funkci tak, aby ji mohl invertovat ten (nebo ta), kdo zná hodnoty/? a *q,* dvou prvočísel, jejichž násobek dal číslo *N.* Ačkoli Alice řekla celému světu, *že její* hodnota iVje 175 828 273, neodhalila své hodnoty/? a *q,* takže pouze ona disponuje speciální informací nutnou pro dešifrování zpráv určených její osobě.

AT je tedy veřejný klíč, informace, která je k dispozici každému -informace potřebná k šifrování zpráv pro Alici, zatímco *p* a *q* jsou soukromým klíčem, dostupným pouze Alici - informace nutná pro dešifrování těchto zpráv.

Detailní popis toho, jak se pomocí *p* a *q* invertuje jednosměrná funkce, je v příloze J. Jedna otázka však vyvstane okamžitě. Když každý zná veřejný klíč *N,* potom mohou jistě i ostatní lidé určit soukromý *klíčp aqa.* číst Aliciny zprávy, že? Vždyť JVje součinem/; a *q.* Ve skutečnosti je tomu tak, že pokud je *N* dostatečně velké, je prakticky nemožné z něj odvodit £ a *q,* a to je možná ten nejkrásnější a nejelegantnější aspekt asymetrické šifry RSA.Alice vytvořila *N* tak, že zvolila p *a.q a.* potom je vynásobila. Podstata věci spočívá v tom, že takové násobení je samo o sobě jednosměrnou funkcí. Dá se to snadno ukázat. Vezměme dvě prvočísla, třeba 9 419 a 1 993, a vynásobme je mezi sebou. S kapesní kalkulačkou máme za několik vteřin výsledek: 18 206 927. Když je však zadáno číslo 18 206 927 a máme najít jeho prvočíselné činitele (tedy dvě čísla, která po vynásobení dají 18 206 927), zabere to mnohem více času. S kapesní kalkulačkou byste nad tím strávili určitě půl dne.

Systém asymetrické kryptografie známýjako RSA je jednou z forem kryptografie s veřejným klíčem. Abychom zjistili, jak je RSA bezpečný, můžeme jej prozkoumat z Evina pohledu a zkusit rozluštit zprávu, kterou zaslala Alice Bobovi. Aby Alice zašifrovala zprávu pro Boba, musí nejprve vyhledat Bobův veřejný klíč. Bob si pro jeho vytvoření vybral svá vlastní prvočísla^ a q_B, která navzájem vynásobil, aby dostal N_B. Uchoval $p_B a . q_B v$ tajnosti, protože tvoří jeho soukromý dešifrovací klíč, ale zveřejnil N_B, které je rovno 408 508 091. Alice vloží Bobův veřejný klíč N_B do obecné jednosměrné šifrovací funkce a zašifruje svou zprávu. Když zašifrovaná zpráva *dorazí,* Bob invertuje funkci a dešifruje zprávu pomocí svých hodnot pro p_B a q_B, které tvoří jeho soukromý klíč. Mezitím Eva zprávu zachytila. Její jediná naděje na dešifrování zprávy spočívá v inverzi jednosměrné funkce a to je možné pouze tehdy, když zná^$_B$ a q_B. Bob zachovaly a q_B v tajnosti, ale Eva jako každý jiný ví, že N_B je 408 508 091. Eva se snaží nalézt hodnoty p_B a q_B tím, že vypočítá, která čísla by bylo nutné vynásobit, aby výsledek byl 408 508 091, což je proces známýjako *faktorizace.*

Faktorizace je časově velmi náročná. Jak dlouho by trvalo Evě nalézt činitele čísla 408 508 091? Existují různé postupy, jak zkoušet faktorizovat Ng. Přestože některé způsoby jsou rychlejší než ostatní, nejjednodušším postupem je ověřování každého prvočísla, zda dělí N_B beze zbytku. Například 3 je prvočíslo, ale není činitelem čísla 408 508 091, protože 3 nedělí 408 508 091 beze zbytku. Takže Eva přejde k dalšímu prvočíslu - 5. Ani 5 není činitelem uvedeného čísla, takže Eva přejde k dalšímu prvočíslu - a tak dále. Nakonec Eva dojde k číslu 18 313, které je 2 000. prvočíslem v pořadí a zároveň je skutečně činitelem 408 508 091. Když našla jednoho činitele, je už snadné najít dalšího, jímž je 22 307. Pokud má Eva kalkulačku a dokáže ověřit čtyři prvočísla za minutu, zabralo by jí 500 minut čili více než 8 hodin nalézt p_B a q_B. Jinými slovy, Eva by dokázala vypočítat Bobův soukromý klíč a tedy rozluštit zachycenou zprávu za necelý den.

To není příliš vysoká úroveň bezpečnosti, ale Bob mohl vybrat daleko větší prvočísla a zvýšit tak bezpečnost svého soukromého klíče. Například si mohl vybrat prvočísla řádu 10^{65} (to je jednička následovaná 65 nulami neboli sto tisíc milionů milionů milionů milionů milionů milionů milionů milionů milionů milionů). Jeho výběr by vedl k hodnotě N přibližně 10^{65} x 10^{65}, což je 10^{130}. Počítač vynásobí dvě prvočísla a určí tak N ve zlomku vteřiny, ale pokud by Eva chtěla obrátit proces a vypočítat £ a q, zabralo by jí to mnohem delší čas. Jak dlouhý přesně by byl, to by *záleželo* na rychlosti Evina počítače. Expert na bezpečnost Simson Garfinkel odhaduje,

že počítači s procesorem 100 MHz Intel Pentium a s 8 MB RAM by zabralo zhruba 50 let, než by faktorizoval číslo řádu 10^{130}. Kryptografové mají sklony k podezřívavosti a berou v úvahu ty nejhorší scénáře, jako třeba celosvětové spiknutí k rozlomení jejich šifer. Garfinkel uvažoval, co by se stalo, kdyby se dohromady spiklo sto milionů osobních počítačů. Číslo řádu $10^{130}$by pak mohlo být faktorizováno v cca 15 vteřinách. Proto nyní převládá názor, že pro opravdovou bezpečnost je nezbytné používat ještě větší prvočísla. Pro důležité bankovní transakce se doporučuje *N* minimálně 10^{308}, což je deset milionů miliard miliard miliard miliard miliard miliard miliard miliard miliard miliard miliard miliard miliard miliard miliard miliard miliard miliard miliardkrát více než 10^{130}.1 při spojeném úsilí sta milionů osobních počítačů by trvalo více než tisíc let, než by taková šifra byla prolomena. S dostatečně velkými hodnotami *p* a *q* je RSA nedobytná.

Nejznámějším rizikem pro RSA je, že by někdy v budoucnosti někdo našel rychlý způsob, jak faktorizovat *N*. *Lze* si představit, že za několik desítek let - nebo třeba zítra - někdo objeví metodu rychlé faktorizace, a od toho okamžiku bude RSA nepoužitelná. Nicméně, matematici takovou zkratku hledají neúspěšně přes dva tisíce let a faktorizace stále zůstává časově náročným výpočtem. Většina matematiků se domnívá, že to plyne z podstaty věci a že existuje nějaká matematická zákonitost, která takovou zkratku nepřipouští. Mají-li pravdu, pak je RSA v dohledné budoucnosti bezpečná.

Obrovská výhoda kryptografie s veřejným klíčem RSA spočívá v tom, že řeší naráz všechny problémy spojené s tradičními šiframi a výměnou klíčů. Alice se už nemusí starat o bezpečný přenos klíčeBobovi ani o to, že Eva může klíč zachytit. Alice vůbec nedbá o to, kdo může její veřejný klíč spatřit- čím je zájemců více, tím lépe, protože veřejný klíč slouží k šifrování, nikoli k dešifrování. Jediné, co je třeba utajit, je soukromý klíč k dešifrování; Alice by jej měla mít stále u sebe.

RSA poprvé pronikla na veřejnost v srpnu *1977*, když Martin Gardner napsal článek *nazvaný Nový druh šifry, jejíž rozlomení by zabralo miliony let* pro svůj sloupek Mathematical Games v časopise *Scientific American.* Po vysvětlení, jak kryptografie s veřejným klíčem funguje, vyhlásil Gardner čtenářskou soutěž. Otiskl zašifrovaný text a také uvedl veřejný klíč, který použil k zašifrování:

N = 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541

Soutěžním úkolem bylo faktorizovat *N* na *p* a *q* a pak tato čísla použít k dešifrování zprávy. Cena činila sto dolarů. Gardner neměl prostor, aby vysvětlil podrobnosti RSA, a místo toho navrhl čtenářům, aby si o detaily napsali do laboratoře počítačových věd MIT. Rivest, Shamir a Adleman byli překvapeni 3

000 žádostí, jež obdrželi. Neodpověděli hned, protože se báli, že by takovým předčasným zveřejněním ohrozili udělení patentu. Když se tato záležitost úspěšně vyřešila, trojice uspořádala oslavu, na níž profesoři a studenti jedli pizzu, pili pivo a vkládali do obálek technické instrukce pro čtenáře *Scientific American.*

V případě Gardnerovy výzvy trvalo 17 let, než byla šifra rozlomena. 26. dubna 1994 tým 600 dobrovolníků oznámil činitele *N:*

q - 3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577

p = 32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533

S těmito hodnotami soukromého klíče dokázal kdokoli zprávu dešifrovat. Zpráva měla podobu řady čísel, ale když je změnili v písmena, zněla: „the magie words are squeamish ossifrage" (magická slova jsou orlosup bradatý). Problém faktorizace byl rozdělen mezi dobrovolníky, kteří pocházeli z navzájem tak vzdálených zemí jako Austrálie, Británie, Amerika nebo Venezuela. Dobrovolníci využíva-li

volný čas na svých pracovních stanicích, serverech a superpočítačích každý z nich se vypořádával se zlomkem problému. V podstatě se síť počítačů po celém světě spojila a pracovala zároveň, aby zvládla Gardnerovu výzvu. I když vezmeme v úvahu tak enormní soustředěné úsilí, mohou být někteří čtenáři překvapeni, že RSA byla prolomena v tak krátkém čase - ale je třeba si uvědomit, že Gardnerova soutěž obsahovala relativně malou hodnotu *N* - pouze v řádu 10^{129}. Současní uživatelé RSA volí daleko větší hodnoty, když chtějí zabezpečit důležité informace. Dnes je běžnou praxí šifrovat zprávy s hodnotou *N* tak vysokou, že by všechny počítače na zeměkouli potřebovaly k rozlomení šifry delší čas, než je dosud známé stáří vesmíru.

Alternativní historie kryptografie s veřejným klíčem

Během posledních dvaceti let se Diffie, Hellman a Merkle proslavili po celém světě jako vědci, kteří vymysleli koncept kryptografie s veřejným klíčem, zatímco Rivest, Shamir a Adleman byli oceňováni jako vynálezci RSA, který je považován za nejkrásnější implementaci veřejného klíče. Nedávno se však ukázalo, že historii je třeba přepsat. Podle informací britské vlády byla kryptografie s veřejným klíčem původně vynalezena v Governement Communicati-on Headquaters (GCHQ) v Cheltenhamu, v přísně tajné instituci, jež vznikla po druhé světové válce ze zbytků Bletchley Parku. Je to příběh pozoruhodné vynalézavosti, anonymních hrdinů a přísného utajení, jež trvalo po desetiletí.

Příběh začíná na konci 60. let 20. století, kdy si britská armáda začala dělat starosti s problémem distribuce klíčů. Vojenské kruhy přemýšlely o budoucnosti a zvažovaly scénář, v němž by miniaturizace rádií a snížení jejich ceny vedly k tomu, že by mohl každý voják být v průběžném rádiovém kontaktu se svým velitelem. K tomu podle nich mohlo dojít už v následujícím desetiletí. Výhody všeobecné komunikace by byly obrovské, ale komunikaci by bylo nutné šifrovat a problém distribuce klíčů se zdál nepřekonatelný. V té době byla jedinou formou kryptografie symetrická šifra, takže by bylo třeba bezpečně doručit klíč všem

členům komunikační sítě. Každá komunikační expanze by však byla nakonec zastavena tíhou distribuce klíčů. Na počátku roku 1969 požádala armáda Jamese Ellise, jedno-ho z nejpřednějších britských vládních kryptografů, aby prozkoumal způsoby, jak se vypořádat s problémem distribuce klíčů.

Ellis byl trochu excentrik. Pyšnil se tím, že procestoval polovinu světa dříve, než se narodil - byl počat v Británii, ale narodil se v Austrálii. Jako dítě se vrátil do Londýna a vyrůstal v East Endu dvacátých let. Ve škole se zajímal především o přírodní vědy, později studoval fyziku na Imperiál College a pak se stal členem Post Office Research Station v Dollis Hillu, tedy právě tam, kde Tommy Flowers sestavil Colossus, první dešifrovací počítač. Kryptografická divize v Dollis Hillu nakonec přešla do GCHQ, a tak se 1. dubna 1965 Ellis přestěhoval do Cheltenhamu, aby se připojil k nově vzniklé skupině Communications-Electronics Security Group (CESG), speciální sekci GCHQ zaměřené na zajištění bezpečnosti britských telekomunikací. Protože Ellis pracoval na otázkách národní bezpečnosti, musel se zavázat k mlčenlivosti po celou svou kariéru. Manželka a děti věděli, že pracuje v GCHQ, netušili však nic o jeho objevech a neměli ponětí, že je jedním z nejvýznačnějších britských kryptografů.

Navzdory svým schopnostem nebyl Ellis nikdy pověřen vedením některé důležité výzkumné skupiny v GCHQ. Byl brilantní, ale také

nepředvídatelný, introvertní a nebyl přirozeným týmovým hráčem. Jeho kolega Richard Walton vzpomíná:

Byl to dost svérázný pracovník a moc se nehodil do každodenních záležitostí GCHQ. Ale byl naprosto výjimečný, co se týče vnášení nových myšlenek. Ve své práci se musel někdy potýkat s absurdními nápady, ale byl velmi kreativní a vždy připraven zpochybňovat ortodoxní názory. Byli bychom ve velkém průšvihu, kdyby byl každý v GCHQ jako on, ale můžeme tolerovat větší procento takových lidí než většina jiných organizací. Máme jich celkem dost."

Jedním z Ellisových největších přínosů byla jeho šíře znalostí. Četl každý vědecký časopis, který se mu dostal do rukou, a nikdy nic nevyhodil. Z bezpečnostních důvodů museli zaměstnanci GCHQ každý večer uklidit své pracovní stoly a vše schovat do zamčených skříní. Ellisovy skříně byly proto stále přecpány těmi nejobskurněj-šími publikacemi. Vydobyl si pověst kryptografického guru; když ostatní výzkumníci narazili na neřešitelný problém, zaťukali na jeho dveře ve víře, že jeho rozsáhlé znalosti a originalita přístupu jim poskytnou řešení. Patrně právě proto byl pověřen prozkoumáním problému distribuce klíčů.

Náklady na distribuci klíčů byly enormní a stávaly se limitujícím faktorem pro expanzi šifrování. Dokonce i snížení ceny distribuce klíčů o 10 % by významně snížilo armádní rozpočet na bezpečnost. Ellis však okamžitě *začal* hledat radikální a úplné řešení místo toho, aby si z problému ukrojil jen malý díl. „Vždy přistupoval k problému tak, že se ptal: Je to skutečně to, co chceme udělat?" říká

Walton. James byl prostě James, takže jedna z prvních věcí, které udělal, bylo zpochybnění názoru, že je nezbytné sdílet tajná data, tedy klíč. Nebyl žádný zákon, který by říkal, že musíte mít sdílená tajná data. To bylo něco, co šlo zpochybnit."

Ellis začal zdolávat problém tak, že prohledal svou pokladnici vědeckých statí. O mnoho let později si připomněl okamžik, kdy objevil, že distribuce klíčů není nevyhnutelnou součástí kryptografie:

„Událost, která změnila toto stanovisko, bylo objevení zprávy společnosti Bell Telephone od neznámého autora z doby druhé světové války. Zpráva popisovala důmyslnou myšlenku bezpečného telefonního rozhovoru. Navrhovala, aby volaná strana zastřela obsah hovoru tím, že na linku přidá šum. Pak jej může zase odstranit, protože to byla ona, kdojej přidal, a zná tedy přesné charakteristiky tohoto šumu. Systém má očividné praktické nevýhody a nebyl nikdy použit, ale nápad je to zajímavý. Rozdíl mezi tímto a konvenčním šifrováním je ten, že v tomto případě se na procesu šifrování podílí příjemce... Tak se zrodila má myšlenka."

Sum je technický termín pro jakýkoli signál, který ruší komunikaci. Obvykle vzniká přirozeným způsobem a jeho nejprotivnější rys spočívá v tom, že je naprosto náhodný, což znamená, že jeho odstranění ze zprávy je velmi složité. Pokud je rádiový komunikační systém kvalitní, potom je hladina šumu nízká a zpráva je jasně slyšitelná, pokud je však hladina šumu vysoká a přehluší zprávu, není způsob, jak zprávu získat zpět. Ellis navrhl, aby příjemce - naše známá Alice - úmyslně vytvořila šum, který by změřila před jeho přidáním do komunikačního kanálu, jenž ji spojuje s Bobem. Bob potom pošle zprávu Alici, a i když Eva odposlouchává komunikační kanál, zprávě neporozumí, protože taje ukryta v šumu. Eva by nebyla schopna oddělit šum od zprávy. Jedinou osobou, která by mohla odstranit šum a porozumět zprávě, je Alice, proutže má jedinečnou výhodu - zná přesnou povahu šumu, protože jej tam předtím přidala. Ellis si uvědomil, že bezpečnosti by tak bylo dosaženo bez výměny klíčů. Klíčem je šum a jedině Alice potřebuje znát jeho podrobnosti.

V interním memorandu Ellis podrobně popisuje svůj myšlenkový postup: „Další otázka byla zřejmá. Dá se dosáhnout analogického stavu pomocí běžného šifrování? Můžeme vytvořit bezpečnou zašifrovanou zprávu, srozumitelnou pro autorizovaného příjemce, bez předchozí tajné výměny klíče? Tato otázka mě napadla jednou v noci v posteli a důkaz její teoretické možnosti zabral jen pár minut. Máme existenční důkaz. Dříve nemyslitelné je ve skutečnosti možné." (Existenční důkaz v matematice prokazuje, že určitý koncept je možný, ale *nezabývá* se detaily jeho realizace.) Jinými slovy: do tohoto okamžiku bylo řešení problému distribuce klíčů jako hledání jehly v kupce sena - s možností, že tam jehla ani není. Ellis nyní věděl, že tam někde jehla je.

Ellisova vize byla velmi podobná myšlence Diffieho, Hellmana a Merkla, ovšem s tím rozdílem, že měl několik let náskok. Nikdo však o Ellisově práci nevěděl, protože Ellis byl zaměstnancem britské vlády a byl zavázán k mlčenlivosti. Na konci roku 1969 se Ellis ocitl ve stejné slepé uličce, do které se trojice ze Stanfordu dostala roku 1975. Sám pro sebe dokázal, že kryptografie s

veřejným klíčem

(neboli šifrování bez utajení, jak to nazýval on) je možná, a rozvinul koncept veřejných a soukromých klíčů. Věděl také, že potřebuje na-iít speciální jednosměrnou funkci, takovou, která může být invertována, pokud má příjemce přístup k speciální informaci. Naneštěstí nebyl Ellis matematik. Experimentoval s několika matematickými funkcemi, ale brzy si uvědomil, že bez pomoci jiných specialistů nebude moci pokračovat.

V tomto bodě Ellis odhalil svůj objev nadřízeným. Jejich reakce je stále ještě tajná, ale v osobním rozhovoru byl Richard Walton kvůli mně ochoten parafrázovat různá tehdejší memoranda. Seděl s kufříkem na klíně, víko zakrývalo papíry, abych je neviděl, a listoval dokumenty:

„Nemůžu vám ukázat dokumenty, které zde mám, protože jsou orazítkovány ošklivými slovy jako PŘÍSNĚ TAJNÉ. V podstatě se stalo to, že se Jamesova myšlenka dostala k nejvyššímu šéfovi, který ji někomu přidělil tak, jak to nejvyšší šéfové dělají, takže se na ni mohli podívat experti. Prohlásili, že Jamesovo tvrzení je naprostá pravda. Jinými slovy, potvrdili, že ten chlap není blázen. Nepřišli však na způsob, jak jeho myšlenky realizovat. Jamesova genialita v nich zanechala dojem, ale nikdo nevěděl, co s tím."

Po následující tři roky se nejbystřejší mozky z GCHQ pokoušely nalézt jednosměrnou funkci, která by splňovala Ellisovy nároky, ale neobjevily nic. Potom přišel do týmu v září 1973 nový matematik. Clifford Cocks právě absolvoval Cambridge, kde se specializoval na teorii čísel, jednu z nejčistších forem matematiky. Když se dostal do GCHQ, věděl velmi málo o šifrování a o stínovém světě vojenské a diplomatické komunikace, proto mu byl přidělen instruktor Nick Patterson, který jej provázel prvními týdny u GCHQ.

Po šesti týdnech řekl Patterson Cocksovi o „skutečně praštěném nápadu". Nastínil Ellisovu teorii kryptografie s veřejným klíčem a vysvětlil mu, že zatím nikdo nedokázal najít matematickou funkci, která by odpovídala jeho požadavkům. Patterson to Cocksovi řekl jako zajímavost, protože to byla nejvíce vzrušující kryptografic-ká myšlenka široko daleko - ne proto, že by očekával Cocksův zájem o řešení problému. Nicméně, jak Cocks vysvětluje, ještě téhož dne se pustil do práce: „Nikdo po mně nic nechtěl, tak mě napadlo, ze bych mohl o té věci přemýšlet. Protože jsem dříve pracoval na teorii čísel, bylo přirozené uvažovat o jednosměrných funkcích,o něčem, co můžete provést, nikoli však vrátit zpět. Prvočísla a faktorizace byly přirozeným kandidátem, a to se stalo mým výchozím bodem." Cocks začal formulovat to, co se později stalo známé jako asymetrická šifra RSA. Rivest, Shamir a Adleman objevili své schéma kryptografie s veřejným klíčem v roce 1977, ale již o čtyři roky dříve procházel mladý absolvent Cambridge přesně stejným myšlenkovým procesem. Cocks vzpomíná: „Od začátku do konce mi to nezabralo více než půl hodiny. Byl jsem sám se sebou spokojený. Myslel jsem si: To je pěkné. Dostal jsem problém a vyřešil jsem jej." Cocks však význam svého objevu úplně nedocenil. Nebyl si vědom toho, že nejbystřejší mozky

GCHQ bojovaly s tímto problémem po tři roky, a nevěděl, že udělal jeden z nejvýznamnějších kryp-tografických průlomů století. Cocksova naivita může být částečnou příčinou jeho úspěchu, protože mu poskytla sebedůvěru, kterou by jinak možná neměl. Cocks řekl svému instruktorovi o svém objevu. Byl to Patterson, kdo o něm podal zprávu vedení. Cocks byl velmi ostýchavý a stále ještě nováček, zatímco zkušený Patterson byl schopen plně docenit všechny souvislosti problému a zvážit technické otázky, které nevyhnutelně vyvstanou. Brzy poté začali naprosto neznámí lidé oslovovat zázračné dítě Cockse a gratulovat mu. Jeden z těchto neznámých byl James Ellis, jenž byl dychtivý seznámit se s mužem, který změnil jeho sen v realitu. Protože Cocks stále nechápal dosah svého výkonu, detaily tohoto setkání na něj příliš nezapůsobily, a tak si nyní, o více než dvě desetiletí později, vůbec na El-lisovu reakci nevzpomíná.

Když si Cocks nakonec uvědomil, co udělal, náhle ho napadlo, jak by asi jeho objev zklamal G. H. Hardyho, jednoho ze skvělých anglických matematiků začátku 20. století. Ve své *Obraně matematikově*, napsané roku 1940*, Hardy hrdě uvedl: „Skutečná matematika nemá žádný vliv na válku. Nikdo ještě neobjevil žádný válečný účel, kterému by mohla sloužit teorie čísel." Skutečnou matematikou mínil čistou matematiku, jakou je teorie čísel, která byla jádrem Cocksovy práce. Cocks dokázal, že se Hardy mýlil. Výdobytky teorie čísel se dnes používají k tomu, aby pomáhaly generálům plánovat bitvy v naprostém bezpečí. Protože jeho práce měla důsledky pro vojenskou komunikaci, měl Cocks, stejně jako Ellis, zakázáno prozradit svůj objev komukoli mimo GCHQ. Pracovat pro přísně tajnou vládní organizaci znamenalo, že nemohl nic říci ani rodičům, ani bývalým spolužákům z Cambridge. Jediná osoba, se kterou o tom mohl mluvit, byla jeho žena Gill, neboť ta také pracovala v GCHQ.

Přestože Cocksův nápad byl jedním z nejmocnějších tajemství GCHQ, byl *zatížen* tím, že předběhl svou dobu. Cocks objevil matematickou funkci, která umožňovala kryptografii s veřejným klíčem, ale stále ještě bylo obtížné systém implementovat. Šifrování prostřednictvím kryptografie s veřejným klíčem vyžadovalo daleko větší výkon počítačů než šifrování symetrickými šiframi jako DES. Na počátku 70. let 20. století byly počítače stále ještě poměrně primitivní a neschopné realizovat šifrování veřejným klíčem v rozumném čase. Proto GCHQ nemohla kryptografii s veřejným klíčem využít. Cocks a Ellis dokázali, že zdánlivě nemožné je možné, ale nikdo nemohl najít způsob, jak z možného učinit skutečné.

Začátkem následujícího roku, tedy v roce 1974, vysvětlil Cocks svou práci na kryptografii s veřejným klíčem Malcolmu Williamso-novi, který do GCHQ nastoupil jako kryptograf. Ti dva byli náhodou staří přátelé. Oba chodili do stejné střední školy v Manchesteru, jejímž mottem bylo *Sapere aude* - „Odvaž se být moudrým". Roku 1968 spolu reprezentovali Británii na matematické olympiádě v Sovětském svazu. Poté, co společně vystudovali Cambridge, se jejich cesty rozešly, ale v GCHQ se opět spojily. Od svých jedenácti let si vyměňovali matematické nápady, ale Cocksův objev kryptografie

* Česky vydalo nakladatelství Prostor v roce 1998.

s veřejným klíčem byla ta nejvíce šokující myšlenka, kterou kdy Williamson slyšel. „Cliff mi vysvětlil svou myšlenku," vzpomíná Willi-amson, „a já tomu skutečně nevěřil. Byl jsem velmi podezíravý, protože to bylo tak podivné."

Williamson se pokusil dokázat, že Cocks udělal chybu a že kryptografie s veřejným klíčem ve skutečnosti neexistuje. Zkoumal matematické aspekty celé záležitosti, hledal nějakou zásadní chybu. Kryptografie s veřejným klíčem se *zdála* být příliš dobrá, než aby mohla být správná. Williamson byl tak odhodlán nalézt chybu, že si vzal problém domů. Od zaměstnanců GCHQ se očekávalo, že nic takového nebudou dělat, protože vše, na čem pracovali, bylo tajné. Nicméně problém uvízl Williamsonovi v hlavě, musel na něj stále myslet. Neuposlechl předpisy a odnesl si práci domů. Hledáním chyby strávil pět hodin. „V podstatě jsem neuspěl," říká Williamson. „Místo toho jsem našel jiné řešení problému distribuce klíčů." Williamson objevil systém výměny klíčů Diffie-Hellman-Merkle zhruba ve stejnou dobu jako Martin Hellman. Jeho první reakce odrážela jeho cynické rozpoložení: „Paráda," pomyslel jsem si, „to jsem zvědav, jestli dokážu najít chybu aspoň v tomhle. Měl jsem tehdy docela špatnou náladu."

Do roku 1975 objevili James Ellis, Clifford Cocks a Malcolm Williamson všechny zásadní aspekty kryptografie s veřejným klíčem, ale museli o tom mlčet. Třem Britům nezbývalo nic jiného,

než nečinně přihlížet a dívat se, jak jejich myšlenky „znovu" objevili Diffie, Hellman, Merkle, Rivest, Shamir a Adleman v průběhu následujících tří let. Je překvapivé, že GCHQ objevila systém RSA před výměnou klíčů Diffie-Hellman-Merkle, zatímco v okolním světě se nejdříve zrodila výměna klíčů Diffie-Hellman-Merkle. Vědecký tisk referoval o objevech ve Stanfordu a v MIT. Tamní vědci, kteří měli dovoleno publikovat svou práci, se mezi komunitou kryptografů proslavili. Když se podíváte na internet pomocí prohledavače, najdete 15 webových stránek zmiňujících se o Cliffordu Cocksovi v porovnání s 1 382 stránkami o Whitfieldovi Diffiem. Cocksův pohled je obdivuhodně umírněný: „Tyhle věci se nedělají kvůli veřejnému uznání." Williamson je stejně věcný: „Moje reakce byla: No dobře, tak to chodí. Srovnal jsem se s tím jednou provždy."

Williamson je v rozpacích pouze z toho, že GCHQ nikdy nepa-tentovala kryptografii s veřejným klíčem. Když Cocks a Williamson dosáhli svých objevů, převládl v GCHQ *názor*, že patentování není možné ze dvou důvodů. Za prvé by vedlo k tomu, že by museli odhalit detaily své práce, což by bylo v rozporu s cíli GCHQ. Za druhé nebylo na počátku 70. let zdaleka jasné, zda matematický algoritmus lze vůbec patentovat. Když Diffie a Hellman zažádali o svůj patent v roce 1976, bylo již zřejmé, že to možné je. V tu chvíli chtěl Williamson zveřejnit svou práci a zablokovat Diffieho a Hellmano-vu přihlášku, ale *zakázali* mu to jeho nadřízení, kteří nebyli natolik prozíraví, aby včas odhalili význam digitální

revoluce a potenciál kryptografie s veřejným klíčem. Začátkem 80. let Williamsonovi šéfové začali svého rozhodnutí litovat. Rozvoj počítačů a internetu jasně ukázal, že RSA a výměna klíčů Diffie-Hellman-Merkle budou představovat úspěšné komerční produkty. Roku 1996 byla společnost RSA Data Security, Inc., zodpovědná za produkty RSA, prodána za 200 milionů dolarů.

Přestože práce v GCHQ stále podléhala utajení, existovala ještě jedna organizace, která o britských výzkumech dobře věděla. Počátkem 80. let americká National Security Agency věděla o práci Ellise, Cockse a Williamsona a pravděpodobně právě touto cestou zaslechl Whitfield Diffie zvěsti o britských objevech. V září 1982 se Diffie rozhodl, že zjistí, co je na tom pravdy, a proto odcestoval se svou ženou do Cheltenhamu, aby si osobně popovídal s Jamesem Ellisem. Setkali se v místní hospodě a Mary byla rychle očarována Ellisovou pozoruhodnou povahou:„Seděli jsme a povídali- a já jsem si najednou uvědomila, že to je jedna z nejúžasnějších osobností, jakou bych si kdy mohla představit. Šíři jeho matematických znalostí nemohu odpovědně posoudit, ale byl to skutečný gentleman, nezměrně skromný, osoba s obrovskou šlechetností duše a noblesou. Tím nemyslím staromódní chování. Ten muž byl prostě kavalír. Byl to dobrý, skutečně dobrý člověk. Jemná duše."

Diffie a Ellis mluvili o různých tématech, od archeologie po úvahy, jak krysy v sudu zlepšují chuť jablečného moštu, ale kdykoliv se konverzace stočila ke kryptografii, Ellis jemně změnil téma. Na konci návštěvy, když už byl Diffie připraven k odchodu, nemohl to již déle vydržet a na rovinu položil Ellisovi otázku, kterou měl po celou dobu v hlavě: „Povězte mi, jak jste vymyslel kryptografii veřejného klíče?" Následovala dlouhá pauza. Ellis nakonec zašeptal: „Nevím, kolik toho smím říci. Řeknu vám jen to, že vy jste udělali daleko více než my."

Přestože lidé z GCHQ byli první, kdo objevili kryptografii veřejného klíče, nijak to nezmenšuje zásluhy akademických vědců, kteří ji znovuobjevili. Byli to oni, kteří si jako první uvědomili potenciál šifrování veřejným klíčem, a byli to právě oni, kteří prosadili jeho implementaci. Navíc je docela dobře možné, že GCHQ by nikdy neodhalila svou práci a zablokovala by tak tuto formu šifrování, která umožnila digitální revoluci dosáhnout svého plného potenciálu. Nakonec je třeba říci, že objev akademických vědců byl zcela nezávislý na objevu GCHQ a že byl intelektuálně na stejné úrovni. Akademické prostředí bylo úplně izolováno od výzkumu podléhajícího utajení, lidé z vysokých škol neměli přístup k nástrojům a tajným informacím z utajené sféry. Výzkumníci pracující pro vládu však přístup k akademické literatuře měli. Tok informací je v této situaci vlastně další jednosměrnou funkcí: informace plynou volně v jednom směru, ale je zakázáno je posílat ve směru opačném.

Když Diffie pověděl Hellmanovi o práci Ellise, Cockse a William-sona,

Hellman zaujal tento postoj: Jejich vlastní objevy by měly být poznámkou pod čarou v historii tajného výzkumu a objevy GCHQ by měly být poznámkou pod čarou v historii akademického výzkumu. Nicméně v této fázi nikdo kromě GCHQ, NSA, Diffieho a Hell-mana o utajeném výzkumu nevěděl, takže jej nebylo možné považovat ani za poznámku pod čarou.

V polovině 80. let se nálada v GCHQ změnila a jeho management *začal zvažovat*, že by práci Ellise, Cockse a Williamsona zveřejnil. Matematika kryptografie s veřejným klíčem byla již veřejně známa a nezdálo se, že existuje jediný důvod zachovávat utajení i nadále. Z praktického hlediska by bylo nesporně výhodné, kdyby Britové odhalili své zásadní práce o kryptografii s veřejným klíčem. Jak vzpomíná Richard Walton:

„Flirtovali jsme s myšlenkou, že vyrukujeme s pravdou ven roku 1984. Pro GCHQ by bylo určitě výhodné, kdyby se jí dostalo většího veřejného uznání. Tou dobou se poptávka po bezpečnostních řešeních uvnitř státního sektoru rozšiřovala i mimo vojenská a diplomatická využití a my potřebovali získat důvěru lidí, kteří s námi nebyli zatím zvyklí jednat. Bylo to uprostřed thatcherismu a my se snažili prorazit názorem ‚vládaje špatná, soukromí je dobré'. Chystali jsme tedy článek k publikování, ale překazil nám to ten neřád Peter Wright, který napsal knihu *Spycatcher*. Už jsme měli naše šéfy skoro připravené k tomu, aby nám publikování schválili, ale pak vypukl skandál kolem Wrightovy knihy. Heslem dne se stalo ‚nevystrkovat hlavu, klobouk do očí'."

Peter Wright byl penzionovaný důstojník britské zpravodajské služby a vydání jeho pamětí *Spycatcher* způsobilo britské vládě řadu trapných situací. Trvalo ještě třináct let, než GCHQ kryptografii s veřejným klíčem odhalila - tedy 28 let po původním Ellisově objevu. Roku 1997 dokončil Clifford Cocks důležitou, ne však utajenoupráci na RSA, která byla zajímavá pro širší komunitu a jejíž publikace by nepředstavovala bezpečnostní riziko. Byl pozván, aby přednášel na konferenci Ústavu aplikované matematiky v Cirencesteru. Předem se očekávalo, že bude posluchárna plná kryptografických expertů. Hrstka posluchačů věděla, že Cocks, který bude přednášet pouze o jednom aspektu RSA, je ve skutečnosti jejím neopěvovaným autorem. Riziko spočívalo v tom, že by někdo mohl položit nepříjemnou otázku, třeba: „Vymyslel jste RSA?" Pokud by taková otázka padla, jak by se měl Cocks zachovat? Podle politiky GCHQ by měl popřít svou roli v rozvoji RSA, takže by byl nucen lhát v odpovědi na otázku, která byla naprosto neškodná. Situace byla zjevně absurdní, a proto GCHQ rozhodla, že nastal čas změnit politiku. Cocks dostal povolení začít přednášku představením stručné historie přínosu GCHQ ke kryptografie s veřejným klíčem.

18. prosince 1997 Cocks přednesl svůj příspěvek. Po téměř třech desetiletích utajení se Ellisovi, Cocksovi a Williamsonovi dostalo uznání, které si zasloužili. James Ellis bohužel zemřel právě o měsíc dříve, 25. listopadu 1997, ve věku 73 let. Jeho jméno je tak dalším pojmem mezi britskými experty na šifry, jejichž přínos

nebyl uznán za jejich života. Průlom Charlese Babbage do Vigeněrovy šifry nebyl během jeho života nikdy odhalen, protože jeho práce byla důležitá pro britské síly na Krymu. Místo toho byly zásluhy za tuto práci připsány Friedrichu Kasiskimu. Podobně tomu bylo s Turingem - jeho přínos během první světové války byl neocenitelný, nicméně vládní politika utajení vyžadovala, aby jeho práce na Enigmě nebyla odhalena.

Roku 1987 napsal Ellis tajný dokument, který shrnuje jeho přínos pro kryptografii s veřejným klíčem. Obsahuje i obecnější myšlenky o utajení, které tak často obklopuje kryptografickou práci:

„Kryptografie je tou nejméně normální vědou. Většina profesionálních vědců usiluje o to, aby byli prvními autory, kteří publikují svou práci, protože hodnota vědecké práce spočívá mimo jiné v jejím zveřejnění. Celá hodnota kryptografie naopak spočívá v minimalizaci informací, jež jsou potenciálnímu nepříteli k dispozici. Profesionální kryptogra-fové obvykle pracují v uzavřených komunitách, které poskytují k zajištění kvality dostatečnou profesionální interakci, ale před lidmi mimo komunitu zachovávají utajení. Odhalení těchto tajemství je obvykle povoleno v zájmu historické přesnosti až poté, co lze prokázat, že z dalšího utajení neplyne žádný prospěch."

7

Docela dobré soukromí

Přesně jak Diffie již počátkem 70. let předpověděl, vstupujeme nyní do informačního věku, do postindustriální éry, v níž jsou informace tím nejcennějším zbožím. Výměna digitálních informací se stala nedílnou součástí naší společnosti. Denně se odesílají desítky milionů e-mailů, elektronická pošta brzy předčí v oblibě poštu tradiční. Internet, byt' stále v plenkách, poskytl infrastrukturu pro digitální obchodování a e-byznys vzkvétá. Peníze plynou kyberprosto-rem - odhaduje se, že každého dne proteče hodnota, která je rovna polovině světového hrubého domácího produktu, sítí Society for Worldwide Interbank Financial Telecommunications (SWIFT). Země, v nichž je zavedeno referendum, začnou brzy hlasovat on-line. Vlády využijí internet ve státní správě například při on-line podávání daňových přiznání.

Úspěch informačního věku však závisí na schopnosti chránit informace putující kolem světa, a ta zase podléhá síle kryptografie. Na šifrování se můžeme dívat jako na zámky a klíče informačního věku. Po dva tisíce let bylo šifrování důležité pouze pro vládní orgány a ozbrojené síly, ale dnes má důležitou úlohu v hladkém průběhu obchodu a zítra se budou obyčejní lidé spoléhat na kryptografii, která bude chránit jejich soukromí. Naštěstí právě nyní, když se začíná informační věk rozvíjet, máme k dispozici výjimečně silné šifrování. Rozvoj kryptografie s veřejným klíčem, zvláště šifry RSA, dal dnešním kryptografům zřetelnou výhodu v jejich ustavičném boji proti kryptoanalytikům. Pokud je hodnota TV dostatečně veliká, zabere pak Evě nalezení p a q tak ohromné množství času, že je šifra RSA prakticky neprolomitelná. Nejdůležitější ze všeho je, že kryptografii s veřejným klíčem neoslabuje žádný problém distribuce klí-cu. RSA poskytuje téměř neprostupné

zámky pro naše nejcennější informace.

Jako každá jiná technologie má i šifrování svou odvrácenou tvář. Chrání totiž nejen komunikaci občanů dbalých zákona, ale i zločin-ců a teroristů. V současnosti používá policie odposlech jako způsob získávání důkazů v důležitých případech, k nimž patří organizovaný zločin a terorismus, to by však bylo nemožné, pokud by měli zločinci k dispozici nerozlomitelné šifry. Na úsvitu jedenadvacátého století je základním dilematem kryptografie nalezení postupů, jež veřejnosti a obchodní sféře zpřístupní šifrování pro maximální využití výhod informačního věku, aniž by takových postupů zároveň mohli zneužít zločinci. Stále se vede aktivní a široká debata o tom, která cesta vpřed je ta pravá. Mnohé náměty byly inspirovány příbě-hem Phila Zimmermanna, muže, jehož pokusy podpořit všeobecné rozšíření silného šifrování vyvolaly paniku u amerických bezpečnostních expertů, ohrozily účinnost mocné National Security Agen-cy a učinily z Zimmermanna samého předmět zájmu FBI a objekt vyšetřování před velkou porotou.

Phil Zimmermann strávil polovinu 70. let na Atlantic University na Floridě, kde studoval fyziku a posléze počítačové vědy. Po absolvování se zdál být předurčen pro úspěšnou kariéru v rychle rostoucím počítačovém průmyslu, ale politické události na počátku 80. let změnily jeho život. Méně se zajímal o technologie křemíkových čipů, více o hrozbu jaderné války. K ostražitosti ho vedla sovětská invaze do Afghánistánu, zvolení Ronalda Reagana prezidentem USA, nestabilita zapříčiněná stárnoucím Brežněvem a rostoucí napětí studené války. Uvažoval dokonce o tom, že se odstěhuje s rodinou na Nový Zéland, neboť se domníval, že to bude jedno z mála míst na

zeměkouli, které bude obyvatelné i po jaderném konfliktu. Ale právě když obdržel pasy a dokumenty potřebné k imigraci, zúčastnil se spolu se svou manželkou mítinku pořádaného Kampaní za jaderné odzbrojení. Místo aby utekli, rozhodli se Zimmermannovi zůstat a bojovat doma. Stali se protijadernými aktivisty v první linii - vedli školení na politická témata a byli zatčeni na nevadské pokusné jaderné střelnici bok po boku s Carlem Saganem a se čtyřmi sty dalších protestujících.

O několik let později, v roce 1988, se stal hlavou Sovětského svazu Michail Gorbačov, hlasatel perestrojky, glasnosti a snížení napětí mezi Východem a Západem. Zimmermannovy obavy se začínaly utišovat, neztratil však svou vášeň pro politický aktivismus, pouze jej zaměřil jiným směrem. Zaměřil se na digitální revoluci a nutnost šifrování:

„Kryptografie bývala obskurní vědou s malým významem pro každodenní život. Historicky měla vždy speciální úlohu ve vojenské a diplomatické komunikaci. Avšak v informačním věku se kryptografie dotýká politické moci, a zvláště mocenských vztahů mezi vládou a lidem. Týká se práva na soukromí, svobody projevu, svobody politického sdružování, svobody tisku, práva na spravedlivý soudní proces, svobody mít klid."

Tyto názory se mohou zdát paranoidní, ale podle Zimmermanna existuje zásadní rozdíl mezi tradiční a digitální komunikací, jenž má podstatný vliv na bezpečnost:

„Když chtěla vláda v minulosti narušit soukromí běžného občana, musela vynaložit určitou námahu, aby zachytila jeho korespondenci, nad párou otevřela a přečetla dopis psaný na papíře nebo aby zaznamenala a zapsala telefonní konverzaci. Je to totéž, jako když chytáte ryby na udici, jednu po druhé. Takový způsob monitorování, náročný na pracovní sílu, není v širším měřítku praktický - naštěstí pro svobodu a demokracii. Dnes nahrazuje elektronická pošta poštu tradiční a brzy se stane běžným prostředkem pro každého člověka, nebude už novinkou jako dnes. Na rozdíl od klasické pošty lze e-mailové zprávy snadno odposlouchávat' a hledat v nich například klíčová slova. Dá se to dělat jednoduše, rutinně, automaticky, nepozorovaně a ve velkém měřítku. To je chytání ryb do sítí - v tom spočívá kvantitativní a kvalitativní orwel-lovský rozdíl ve stavu demokracie."Rozdíl mezi obyčejnou a digitální poštou lze ilustrovat, když si představíme, že Alice posílá pozvánky na oslavu svých narozenin a Eva, kterou nepozvali, chce znát čas a místo oslavy. Pokud Alice použije tradiční metodu rozesílání dopisů, potom je pro Evu velmi těžké jednu z pozvánek zachytit. Eva neví, kde vstoupily Aliciny pozvánky do poštovního systému, protože si Alice může vybrat jakoukoli poštovní schránku ve městě. Její jediná naděje na zachycení jedné z pozvánek spočívá v tom, že zjistí adresu některého z Aliciných přátel a pronikne do místního poštovního úřadu. Potom musí ručně prohlédnout každý dopis. Pokud se jí podaří najít dopis od Alice, bude jej muset nad parou otevřít, aby získala informaci, kterou chce, a potom jej vrátit do původního stavu, aby se vyhnula podezření z porušení listovního tajemství.

V porovnání s tím je Evin úkol podstatně snazší, pokud Alice pošle své pozvánky e-mailem. Když zprávy opouštějí Alicin počítač, odejdou na lokální server, hlavní vstupní místo na internet. Pokud je Eva dostatečně chytrá, může nahlédnout do obsahu lokálního serveru, aniž by opustila svůj dům. Pozvánky obsahují Alicinu e-mailovou adresu; je snadné vytvořit elektronické síto, které vyhledá e-maily s takovou adresou. Jakmile Eva pozvánku nalezne, není zde žádná obálka, kterou by musela otevřít, a žádný problém s přečtením. Navíc nikdo nepozná, že text četla neautorizovaná osoba. Alice nebude vědět, co se děje. Nicméně existuje způsob, jak Evě ve čtení Aliciných e-mailů zabránit: šifrování.

Denně se po světě rozešle přes sto milionů e-mailů a všechny jsou vystaveny riziku odposlechu. Digitální technologie napomohla komunikaci, ale také zvýšila možnost, že tato komunikace bude monitorována. Podle Zimmermanna mají kryptografové povinnost podpořit rozšíření šifrování a tak chránit soukromí jedince:

„Budoucí vláda by mohla disponovat technologickou infrastrukturou, jež je optimalizována pro široký dohled nad společností, v níž lze sledovat aktivity politické opozice, každou finanční transakci, každou komunikaci, každý bit každého e-mailu, každý telefonní hovor. Všechno lze filtrovat a skenovat, automaticky rozpoznávat hlas a přepisovat. Je na čase, aby kryptografie vystoupila ze stínu špionážních a armádních kabinetů, aby vyšla na slunce a stala se nástrojem všech ostatních lidí."

Když byla RSA v roce 1977 objevena, poskytovala alespoň teoreticky zbraň

proti scénáři Velkého bratra, protože díky ní mohli jednotlivci vytvořit vlastní veřejné a soukromé klíče a potom zasílat a přijímat dokonale bezpečné zprávy. To však naráželo na zásadní praktický problém, protože reálný proces šifrování pomocí RSA vyžadoval velký výpočetní výkon v porovnání se symetrickými formami šifrování jako DES. V 80. letech disponovala dostatečně výkonnými počítači, na kterých mohl běžet systém RSA, jen vláda, armáda a velké podniky. Není překvapením, že když RSA Data Security, Inc., společnost založená kvůli obchodnímu využití RSA, vytvořila svůj šifrovací produkt, myslela přitom pouze na tyto zákazníky.

Zimmermann byl naopak přesvědčen, že každý člověk zasluhuje právo na takové soukromí, jaké *nabízí* šifrování RSA, a zaměřil svůj politický aktivismus k dostupnosti RSA pro běžnou populaci. Chtěl využít svého vzdělání v počítačových vědách, aby vytvořil levný a výkonný produkt, jenž by fungoval i na obyčejném osobním počítači. Také chtěl, aby jeho verze RSA měla jednoduché ovládání, aby její uživatel nemusel být expertem na kryptografii. Svůj projekt nazval Docela dobré soukromí (Pretty Good Privacy, PGP). Název byl inspirován maloobchodním řetězcem Ralph's Pretty Good Gro-ceries, jenž byl sponzorem jednoho z Zimmermannových nejoblíbenějších rozhlasových pořadů *Prairie Home Companion* od Garrisona Keillora.

Koncem 80. let pracoval Zimmermann v místě svého bydliště v Boulderu v Coloradu, kde dal postupně dohromady balíček šifrovacího softwaru. Jeho hlavním cílem bylo zrychlit proces šifrování pomocí RSA. Do té doby tomu bylo tak, že když Alice chtěla použít RSA, aby zašifrovala zprávu pro Boba, nejprve vyhledala jeho veřejný klíč a potom na zprávu aplikovala jednosměrnou funkci RSA. Bob naopak dešifruje zprávu pomocí svého soukromého klíče, aby invertoval jednosměrnou funkci RSA. Oba procesy vyžadují značné množství matematických operací, takže zašifrování a dešifrování může, pokud jsou zprávy dlouhé, trvat na osobním počítači několik minut. Pokud Alice posílá denně stovky zpráv, nemůže si dovolit sttávit několik minut šifrováním každé jednotlivé zprávy. Aby Zimmermann urychlil šifrování a dešifrování, použil elegantní trik, kte-fým spojil asymetrické šifrování RSA se staromódním symetrickým šifrováním. Tradiční symetrické šifrování může být stejně bezpečné jako asymetrické, a dokonce je daleko rychlejší na provedení, trpívšak problémem distribuce klíče, který je třeba bezpečně přenést od odesilatele k příjemci. Tady přichází na pomoc RSA, protože ji lze použít k zašifrování symetrického klíče.

Zimmermann si představil následující scénář. Když chce Alice zaslat zašifrovanou zprávu Bobovi, začne tím, že ji zašifruje symetrickou šifrou. Zimmermann navrhl použít šifru známou jako IDEA, která je podobná DES. K šifrování pomocí IDEA musí Alice zvolit klíč. Aby Bob mohl zprávu dešifrovat, Alice potřebuje nějak dostat tento klíč k Bobovi. Alice tento problém překoná tak, že si vyhledá Bobův veřejný klíč pro RSA, který potom použije pro zašifrování klíče k IDEA. Takže Alice nakonec zašle Bobovi dvě věci: zprávu zašifrovanou symetrickou šifrou IDEA a klíč k IDEA zašifrovaný asymetrickou šifrou RSA. Na druhém konci použije Bob svůj soukromý klíč RSA, aby dešifroval klíč k IDEA, a

potom klíčem k IDEA dešifruje vlastní zprávu. Může se to zdát komplikované, ale výhoda je v tom, že zpráva, která může obsahovat velké množství informací, je zašifrována rychlou symetrickou šifrou a že pouze symetrický klíč k IDEA, který sestává z relativně malého množství informací, je zašifrován pomalou asymetrickou šifrou. Zimmermann předpokládal, že tuto kombinaci RSA a IDEA zahrne v produktu PGP, který bude díky uživatelsky přívětivému rozhraní pro uživatele nenáročný na ovládání.

Když Zimmermann vyřešil z velké části problém rychlosti, začlenil do PGP sadu dalších užitečných vlastností. Jednou z nich je generování klíčů. Před použitím RSA musí Alice vytvořit svůj soukromý i veřejný klíč. Vytváření klíčů není triviální, protože vyžaduje vyhledání dvojice obrovských prvočísel. PGP však po Alici nechce nic jiného než lehce pohnout myší. Program se pak pustí do práce a vytvoří dvojici jejího soukromého a veřejného klíče - pohyb myši vnese do hry náhodný faktor, který PGP potřebuje, aby zajistil, že každý uživatel má svou vlastní dvojici prvočísel a tudíž svůj vlastní jedinečný soukromý a veřejný klíč. Na Alici je už jen svůj veřejný klíč zveřejnit.

Dalším užitečným rysem PGP je možnost jeho aplikace na digitální podpis e-mailů. Obyčejný e-mail nenese podpis, což znamená, zeje nemožné ověřit pravého autora elektronické zprávy. Pokud Alice použije e-mail, aby Bobovi poslala milostný dopis, může jej normálně zašifrovat Bobovým veřejným klíčem. Bob pak dopis dešifruje svým soukromým klíčem. Nejprve má radost - ale jak si může být

jist, že je milostný dopis doopravdy od Alice? Mohlo se přece stát, že dopis napsala zlomyslná Eva a podepsala jej Aliciným jménem. Chybí zde jistota, kterou poskytuje podpis ručně napsaný inkoustem, chybí způsob, jak ověřit autorství. Anebo si představte, že banka obdrží e-mail od klienta, jímž dává pokyn, že se mají všechny jeho peníze převést na soukromý bankovní účet na Kajmanských ostrovech. Problém je tentýž: jak může banka bez vlastnoručního podpisu vědět, že e-mail je skutečně od onoho klienta? E-mail mohl napsat zločinec s úmyslem převést cizí peníze na svůj vlastní účet v bance na Kajmanských ostrovech. Internet potřebuje nějakou formu spolehlivého digitálního podpisu.

Digitální podpis PGP je založen na principu, který poprvé vyvinuli Whitfield Diffie a Martin Hellman. Když přišli s myšlenkou oddělených veřejných a soukromých klíčů, uvědomili si, že vedle řešení problému distribuce klíčů by jejich objev mohl také poskytnout přirozený mechanismus pro vytváření e-mailových podpisů. V kapitole 6 jsme se dozvěděli, že veřejný klíč slouží k šifrování a soukromý klíč k dešifrování. Tento proces lze obrátit tak, že se soukromý klíč použije k šifrování a veřejný klíč k dešifrování. Takový způsob šifrování se obvykle opomíjí, protože neposkytuje žádnou bezpečnost. Když Alice použije svůj soukromý klíč, aby zašifrovala zprávu Bobovi, potom může zprávu rozluštit kdokoli, protože každý může mít Alicin veřejný klíč. Tato operace však ověřuje autorství, protože pokud se Bobovi podaří rozluštit zprávu pomocí Alicina veřejného klíče, potom byla zpráva nevyhnutelně zašifrována jejím klíčem soukromým - pouze Alice má přístup ke svému soukromému klíči, takže zprávu musela poslat Alice.

Když tedy chce Alice poslat milostný dopis Bobovi, má dvě možnosti. Buď zašifruje zprávu Bobovým veřejným klíčem, aby zajistila soukromí, nebo ji zašifruje vlastním soukromým klíčem, aby zaručila autorství. Pokud použije obě možnosti, zaručí soukromí i autorství. Existují i rychlejší cesty, jak toho dosáhnout, ale zde si popíšeme jeden způsob, jak může Alice poslat svůj milostný dopis. Nejprve zašifruje zprávu svým soukromým klíčem, potom zašifruje výsledný zašifrovaný text pomocí Bobova veřejného klíče. Představme si zprávu obklopenou křehkou vnitřní skořápkou, která znázorňuje zašifrování Aliciným soukromým klíčem, a pevnou vnější skořápkou, která představuje zašifrování Bobovým veřejným klíčem. Výsledný zašifrovaný text může rozluštit pouze Bob, protože pouzeon má přístup k soukromému klíči nutnému k rozlomení pevné vnější skořápky. Poté, co rozluštil vnější skořápku, rozluští Bob snadno i vnitřní vrstvu prostřednictvím Alicina veřejného klíče -vnitřní skořápka neslouží k ochraně zprávy, ale dokazuje, že zpráva pochází od Alice, a nikoli od podvodníka.

V této fázi se odesílání zpráv zašifrovaných pomocí PGP poněkud komplikuje. K šifrování vlastní zprávy se používá šifra IDEA, šifra RSA je pak zapotřebí pro zašifrování klíče k IDEA. Dalším stadiem šifrování musí být vložení digitálního podpisu, pokud jej chceme zařadit. Zimmermann vyvinul svůj produkt tak, že se vše děje automaticky, takže Alice a Bob si nebudou muset dělat starosti s matematikou. Aby Alice poslala zprávu Bobovi, jednoduše napíše svůj e-mail a vybere volbu PGP z menu na obrazovce svého počítače. Jakmile uvede Bobovo jméno, PGP vyhledá jeho veřejný klíč a automaticky provede veškeré šifrování. Současně provede PGP všechny manipulace nezbytné k digitálnímu podpisu zprávy. Po obdržení zprávy Bob vybere volbu PGP, program dešifruje zprávu a ověří autora. Nic v PGP nebylo původní - už Diffie a Hellman uvažovali o digitálních podpisech, další kryptografové použili kombinaci symetrické a asymetrické šifry k urychlení šifrování - ale Zimmermann byl první, kdo vše složil dohromady v jednoduše ovladatelný šifrovací produkt, který byl dostatečně efektivní, aby fungoval na průměrném osobním počítači.

Do léta roku 1991 byl Zimmermann na dobré cestě udělat z PGP skvělý produkt. Zůstávaly pouze dva problémy a ani jeden z nich nebyl technický. Dlouhodobý problém představovala skutečnost, že RSA, tvořící jádro PGP, je patentovaný produkt. Patentový zákon vyžadoval, aby Zimmermann obdržel licenci od RSA Data Security, Inc., než PGP uvede na trh. Zimmermann se rozhodl tento problém dočasně ignorovat. PGP nebyl zamýšlen jako produkt pro podniky, ale pro jednotlivce. Zimmermann měl za to, že by přímo nekonkuroval RSA Data Security, Inc., a doufal, že společnost mu dá povolení zadarmo.

Vážnější a bezodkladný problém představoval senátní návrh nového Trestního zákona z roku 1991, který obsahoval následující klauzuli: „Kongres je přesvědčen, že poskytovatelé služeb elektronické komunikace a výrobci vybavení pro takové služby mají zaručit, aby jejich komunikační systémy umožnily vládním úřadům obdržet otevřený text hlasových, datových a jiných komunikací, bude-li to

odpovídajícím způsobem upraveno zákonem." Senát se obával, že rozvoj digitálních technologií, jako například mobilních telefonů, může zabránit orgánům

činným v trestním řízení provádět odposlech. *Zákon* tedy nutil firmy, aby zajistily možnost odposlechu, a zdál se ohrožovat všechny formy bezpečného šifrování.

Spojené úsilí RSA Data Security, Inc., telekomunikačního průmyslu a občanských aktivistů vedlo k vynechání této klauzule, převládl však názor, že jde pouze o dočasný odklad. Zimmermann se obával, že dříve či později vláda znovu zkusí přijít se zákonem, který prohlásí šifrování typu PGP za nezákonné. Původně měl v úmyslu PGP prodávat, ale nyní to znovu zvážil. Než čekat a riskovat, že bude PGP *zakázán*, rozhodl se, že je důležitější, aby byl jeho produkt dostupný zadarmo všem, než bude pozdě. V červnu 1991 podnikl drastický krok a požádal přítele, aby PGP umístil na vývěsku (bulletin board) Usenetu*. PGP není nic jiného než software, tedy informace, a tak si jej mohl kdokoli z vývěsky stáhnout. PGP vstoupil na internet.

Napřed způsobil PGP rozruch pouze mezi fanoušky kryptografie. Později si jej začala stahovat širší vrstva internetových nadšenců. Počítačové časopisy otiskly krátké zprávy a pak celostránkové články. Postupně se PGP šířil i do nejvzdálenějších koutů digitální komunity. Například skupiny obhájců základních lidských práv na celém světě začaly používat PGP k šifrování svých dokumentů, aby zabránily tomu, že se informace dostanou do rukou represivních režimů. Zimmermann začal dostávat nadšené e-maily. „Odbojové skupiny v Barmě," říká Zimmermann, „jej používají ve výcvikových táborech v džungli. Řekli mi, že to napomáhá morálce, protože než začali PGP používat, zabavené dokumenty mohly vést k zatčení, mučení a popravám celých rodin." V roce 1991, v den, kdy Boris Jelcin dal střílet na budovu moskevské státní dumy, obdržel Zimmermann z Lotyšska následující mail: „Phile, měl bys vědět tohle: ať se to nikdy nestane, ale kdyby přece v Rusku zavládla diktatura, tvůj PGP je teď rozšířen od Baltu po Dálný východ, a pokud to bude nutné, bude pomáhat demokraticky smýšlejícím lidem. Díky."

Zatímco Zimmermann získával uznání po celém světě, doma v Americe byl terčem kritiky. RSA Data Security, Inc., se rozhodla

*Jde o tehdy běžnou internetovou technologii, předchůdce webových stránek.

nedat Zimmermannovi licenci zdarma a zuřila kvůli porušení svých patentových práv. Přestože Zimmermann dal PGP k dispozici jako freeware, tedy k volnému šíření, byl v něm zahrnut systém kryptografie s veřejným klíčem RSA; následkem toho RSA Data Security, Inc., přezdila PGP jako „banditware". Zimmermann volně rozdal něco, co patřilo někomu jinému. Tahanice o patent trvala několik let a během té doby potkaly Zimmermanna ještě větší problémy.

V únoru 1993 navštívili Zimmermanna dva vládní vyšetřovatelé. Po úvodních dotazech na porušení patentu vytáhli vážnější obvinění - z nelegálního exportu zbraní. Protože vláda Spojených států zahrnula šifrovací software do své definice zbraní - vedle raketových střel, minometů a kulometů - PGP se nesmělo exportovat bez povolení ministerstva zahraničí. Jinými slovy, Zimmermann byl obviněn, že je nelegálním obchodníkem se zbraněmi, protože exportoval PGP přes internet. Na další tři roky se Zimmermann stal předmětem vyšetřování velké poroty a byl

pronásledován FBI.

Šifrování pro masy... Nebo ne?

Vyšetřování Phila Zimmermanna a PGP podnítilo debatu o pozitivních a negativních dopadech šifrování v informačním věku. Rozšíření PGP přimělo kryptografy, politiky, bojovníky za občanská práva i policisty a soudce, aby přemýšleli, kam vede všeobecně rozšířené šifrování. Někteří lidé jako Zimmermann se domnívali, že neomezené používání bezpečného šifrování bude pro společnost dobrodiním, neboť poskytne jednotlivcům soukromí pro jejich digitální komunikaci. Jejich odpůrci byli ale toho názoru, že šifrování je společenskou hrozbou, protože zločinci a teroristi budou schopni komunikovat tajně, v bezpečí před policejním odposlechem.

Debata pokračovala po celá devadesátá léta a dosud není uzavřena. Základní otázka zní, zda vláda má nebo nemá vydávat zákony proti neomezené kryptografii. Kryptografická svoboda by dala všem lidem včetně zločinců jistotu, že jejich e-maily jsou bezpečné. Omezené použití kryptografie by na druhou stranu sice umožnilo policii sledovat zločince, policie i kdokoli jiný by však také mohl sledovat průměrného občana. Nakonec to budeme my všichni, kdo prostřednictvím demokratického procesu rozhodne o budoucí roli kryptografie. Tento oddíl je věnován načrtnutí hlavních rysů obou stran debaty. Velká část diskuse se bude týkat politiky a amerických zákonodárců, částečně proto, že Amerika je domovem PGP, okolo něhož se debata točila, a částečně proto, že jakákoliv politika směřující do oblasti kryptografie v USA bude mít nakonec dopad na politiku na celém světě.

Hledisko, které odmítá všeobecnou dostupnost šifrování a jež zastávají orgány činné v trestním řízení, vychází ze snahy zachovat status quo. Policie na celém světě po desetiletí prováděla legální odposlechy, aby dopadla zločince. Například v Americe se v roce 1918 pomocí odposlechů bojovalo s válečnými špiony, ve 20. letech 20. století sloužily odposlechy během prohibice k usvědčování nelegálních výrobců alkoholu. Stanovisko, které považuje odposlechy za nezbytný nástroj vymáhání práva, nabylo na důrazu koncem let šedesátých, kdy si FBI uvědomila rostoucí hrozbu organizovaného zločinu . Policisté a další úředníci měli velké problémy s usvědčováním podezřelých osob, protože gangsteři vyhrožovali každému, kdo by proti nim svědčil, a sami se řídili zákonem *omerta,* tedy zákonem mlčení. Policie usoudila, že její jediná naděje spočívá ve sběru důkazů prostřednictvím odposlechů, a i Nejvyšší soud byl tomuto argumentu nakloněn. V roce 1967 rozhodl, že policie smí používat odposlech, pokud disponuje soudním povolením.

O dvacet let později FBI stále hájila názor, že „soudem nařízený odposlech je jedinou efektivní vyšetřovací technikou používanou orgány činnými v trestním řízení v boji proti ilegálním drogám, terorismu, násilnému zločinu, špionáži a organizovanému zločinu". Policejní odposlechy by však byly k ničemu, kdyby měli zločinci přístup k šifrování. Telefonní hovor přes digitální linku není nic jiného než proud čísel a lze jej zašifrovat pomocí stejných technik, jaké se používají k šifrování e-mailů. Například tzv. PGPfone je jen jedním z několika produktů umožňujících šifrovat hlasovou komunikaci probíhající přes internet.

Orgány činné v trestním řízení tvrdí, že účinné odposlechy jsou nezbytné pro zachování práva a pořádku a že šifrování je třeba omezit tak, aby v nich bylo možno pokračovat. Policie už narazila na zločince, kteří měli k dispozici silné kryptografické prostředky. Nejmenovaný německý právní expert řekl, že „horké obchody se zbraněmi a drogami se již nedělají přes telefon, ale stále častěji v zašifrovanéformě na celosvětové datové síti". Bílý dům oficiálně připouští stejný varovný trend v Americe; prohlašuje, že „členové organizovaného zločinu patří k nejpokročilejším uživatelům počítačových systémů a silného šifrování". Například kartel Cali zařizuje své drogové kontrakty pomocí šifrované komunikace. Orgány činné v trestním řízení se obávají, že internet spojený s kryptografií pomůže zločincům komunikovat a koordinovat své úsilí. Znepokojeny jsou obzvláště takovými skupinami jako Čtyři jezdci Infokalypsy- což jsou drogoví dealeři, organizovaní zločinci, teroristi a pedofilové - tedy skupinami, jež budou mít z šifrování největší prospěch.

Kromě komunikace šifrují zločinci a teroristé také své plány a záznamy, čímž brání získání důkazů. Například sekta Óm šinrikjó, odpovědná za plynové útoky v tokijském metru v roce 1995, šifrovala některé své dokumenty pomocí RSA. Ramsey Yousef, jeden z teroristů zapletených do přípravy bombového útoku na World Trade Center*, uchovával zašifrované plány teroristických činů ve svém laptopu. Vedle mezinárodních teroristických organizací využívá šifrování také stále více řadových zločinců. Nelegální syndikát hazardních her v Americe šifroval své zprávy po čtyři roky. Studie Dorothy Denningové a Williama Baugha, vypracovaná roku 1997 z pověření pracovní skupiny pro organizovaný zločin National Stratégy Information Center's U.S. Working Group on Organized Crime, odhaduje, že tou dobou se na světě vyskytovalo kolem pěti set případů zločinů, které zahrnovaly šifrování, a předpovídá, že toto číslo se každým rokem zhruba zdvojnásobí.

Kromě domácí politiky je třeba vzít v úvahu i otázky národní bezpečnosti. Americká National Security Agency je odpovědná za shromažďování zpravodajských informací o nepřátelích USA dešifrováním jejich komunikace. NSA provozuje celosvětovou síť odposlouchávacích stanic ve spolupráci s Británií, Austrálií, Kanadou a Novým Zélandem; všechny tyto země shromažďují a sdílí informace. Síť zahrnuje místa jako Menwith Hill Signals Intelligence Base v hrabství Yorkshire, což je největší výzvědná stanice na světě. Část práce Menwith Hillu představuje systém Echelon, který je schopen prohledávat e-maily, faxy, telexy a telefonní hovory se zaměřením na určitá slova. Echelon funguje podle slovníku podezřelých slov (například „Hizballáh", „vrah" a „Clinton") a systém je natolik účinný,

* Zde je míněn neúspěšný pokus v roce 1993.

že tato slova rozezná v reálném čase. Echelon může označit podezřelé zprávy pro další prozkoumání, umožňuje monitorovat zprávy určitých politických skupin nebo teroristických organizací. Nebyl by však k ničemu, kdyby všechny zprávy

byly účinně šifrovány. Země podílející se na Echelonu by tak ztratily hodnotné zpravodajské informace o politických spiknutích a teroristických útocích.

Na druhé straně debaty jsou zastánci občanských práv včetně skupin jako Center for Democracy and Technology a Electronic Frontier Fo«ndation. Argumenty pro šifrování jsou založeny na přesvědčení, že soukromí je základním lidským právem, jak to vyjadřuje článek 12 *Všeobecné deklarace lidských práv*. „Nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům."

Zastánci občanských svobod argumentují, že všeobecná dostupnost šifrování je nepostradatelná pro zajištění práva na soukromí. Jinak se obávají, že nástup digitální technologie, jenž usnadňuje monitorování, bude počátkem nové éry odposlechů a zneužívání moci, která nevyhnutelně následuje. V minulosti vlády často zneužívaly svou moc, aby odposlouchávaly nevinné občany. Prezidenti Lyndon Johnson a Richard Nixon se provinili nezákonnými odposlechy, prezident John F. Kennedy vedl podezřelé odposlechy během prvních měsíců v úřadu. Ve snaze prosadit zákon týkající se dovozu cukru z Dominikánské republiky Kennedy požádal, aby byli odposlouchávání někteří kongresmani. Zdůvodnil to podezřením, že berou úplatky, což byl zdánlivě legitimní zájem národní bezpečnosti. Žádný důkaz o uplácení však nebyl objeven a odposlechy pouze poskytly Kennedymu významné politické informace, na jejichž základě pak vláda prosadila svou verzi zákona.

Jeden z dobře známých případů neustálého neodůvodněného odposlechu se týká Martina Luthera Kingajr., jehož telefonní hovory byly monitorovány po několik let. Například v roce 1963 FBI obdržela informace o Kingovi prostřednictvím odposlechu a dodala je senátorovi Jamesi Eastlandovi, aby mu pomohla v diskusi týkající se zákona o lidských právech. FBI všeobecně shromažďovala informace o Kingově osobním životě, jež pak byly použity k jeho diskreditaci. Nahrávky, v nichž King vypráví nemravné historky, byly zaslány jeho manželce a přehrány před prezidentem Johnsonem. Poté, coKing obdržel Nobelovu cenu, dostala zásilku kompromitujících informací o Kingově životě každá organizace, která uvažovala, že by mu udělila nějakou poctu.

I další vlády jsou vinny zneužíváním odposlechů. Francouzská státní organizace Commission Nationale de Contróle des Intercep-tions de Securité odhaduje, že se každý rok ve Francii provádí zhruba 100 000 nezákonných odposlechů. Pravděpodobně největším narušitelem soukromí každého z nás je mezinárodní program Eche-lon. Ten nemusí své odposlechy nijak ospravedlňovat a není zaměřen jen na určité osoby. Místo toho sbírá informace bez rozlišení. Jeho přijímače zachycují satelitní komunikaci. Pokud Alice pošle neškodnou zprávu Bobovi přes Atlantský oceán, bude jistě zachycena Echelonem, a pokud se stane, že obsahuje pár slov, která jsou ve slovníku Echelonu, bude odložena stranou pro další zkoumání spolu se zprávami od extrémních politických skupin a gangů teroristů. Zatímco orgány činné v trestním řízení argumentují, že šifrování má být zakázáno, protože Echelon by se tak stal neúčinným, zastánci občanských práv

tvrdí, že šifrování je nezbytné - právě proto, aby Echelon neúčinným byl.

Zatímco orgány činné v trestním řízení dokazují, že silné šifrování sníží počet usvědčených zločinců, zastánci občanských práv odpovídají, že otázka soukromí je daleko důležitější. V každém případě zastánci občanských práv trvají na tom, že šifrování by nemělo být velkou překážkou v prosazování práva, protože odposlechy nejsou rozhodující součástí většiny případů. Například v Americe v roce 1994 proběhlo tisíc soudem schválených odposlechů z celkového počtu čtvrt milionu federálních kriminálních případů.

Asi nás nepřekvapí, že mezi obhájci kryptografické svobody jsou někteří z objevitelů kryptografie s veřejným klíčem. Whitfield Diffie prohlašuje, že lidé se těšili plné ochraně soukromí po většinu historie:

„Kolem roku 1790, když byla ratifikována *Listina svobod*, mohl soukromě mluvit kdokoli s kýmkoli - s jistotou, jakou dnes už nemá nikdo -prostě tak, že popošel po cestě kousek od ostatních a podíval se, jestli se někdo neskrývá v keřích. Nebyla žádná nahrávací zařízení, parabolické mikrofony nebo laserové interferometry měřící odraz od jeho brýlí. Dnes se nejeden člověk dívá na toto období jako na zlatý věk americké politické kultury."

Ron Rivest, jeden z vynálezců RSA, se domnívá, že by omezení kryptografie bylo nerozumné:

Je to špatná politika - nekriticky *zakázat* technologii jen proto, že někteří zločinci ji mohou používat ke svému prospěchu. Například každý občan Spojených států může volně koupit pár rukavic, přestože je může lupič použít k vyplenění domu bez zanechání otisků. Kryptografie je technologií ochrany dat stejně jako rukavice jsou technologií ochrany rukou. Kryptografie chrání data před hackery, průmyslovou špionáží a podvodníky, zatímco rukavice chrání ruce před pořezáním, odřeninami, horkem, chladem a infekcí. Kryptografie může zmařit FBI odposlech, rukavice jí mohou překazit analýzu otisků prstů. Jak kryptografie, tak rukavice jsou směšně laciné a široce dostupné. Dobrý kryptografic-ký software můžete stáhnout z internetu za cenu nižší, než je cena kvalitního páru rukavic."

Možná největšími spojenci zastánců občanských práv jsou velké korporace. Internetový obchod je dosud v plenkách, ale prodej roste rychle, zavedli jej maloobchodní prodejci knih, hudebních CD a počítačového softwaru, následují je supermarkety, cestovní kanceláře a další obchody. V roce 1998 použilo internet milion Britů k nákupu zboží v hodnotě 400 milionů liber, v roce 1999 se očekává čtyřnásobek této částky. Během několika málo let může internetový obchod dominovat trhu, ale jen za podmínky, že podniky zvládnou problematiku bezpečnosti a důvěry. Podnik musí být schopen zaručit soukromí a bezpečnost finančních transakcí. Jediný způsob, jak to udělat, je použít silné šifrování.

V dnešní době lze nákup na internetu zabezpečit kryptografií s veřejným klíčem. Alice navštíví webovou stránku firmy a vybere si položku. Potom vyplní objednací formulář, který se jí zeptá na jméno, adresu a údaje o kreditní kartě. Alice pak použije veřejný klíč společnosti k zašifrování objednacího formuláře. Zašifrovaná objednávka se předá společnosti, která jako jediná je schopná ji dešifrovat, protože pouze její pracovníci mají soukromý klíč nezbytný pro dešifrování.

To vše se může provést automaticky Aliciným we-bovým prohlížečem (např. Netscape nebo Explorer), který spolupracuje s počítačem obchodní firmy.

Bezpečnost šifrování závisí jako vždy na délce klíče. V Americe neplatí žádné omezení délky klíče, ale americké softwarové společnosti nemají povoleno exportovat webové produkty, jež poskytujísilné šifrování.* Browsery exportované mimo USA proto mohou pracovat jen s krátkými klíči, a tudíž poskytovat jen poměrně nízkou bezpečnost. Pokud je Alice v Londýně a kupuje knížku od firmy v Chicagu, její internetová transakce je miliard miliard miliard-krát méně bezpečná než transakce Boba, který v New Yorku kupuje knížku od téže firmy. Bobova transakce je naprosto bezpečná, protože jeho prohlížeč podporuje šifrování s delšími klíči, zatímco Ali-cina transakce může být šikovným a dobře vybaveným zločincem zachycena a rozluštěna. Náklady na vybavení nezbytné k rozluštění údajů o Alicině kreditní kartě jsou naštěstí daleko větší než obvyklý limit kreditní karty, takže takový útok není rentabilní. Nicméně, jak se množství peněz tekoucích internetem zvětšuje, může se nakonec rozluštění údajů o kreditních kartách stát pro zločince výhodné. Pokud má internetový obchod prospívat, zákazníci na celém světě musí disponovat kvalitními bezpečnostními mechanismy a firmy nesmí tolerovat uměle omezené šifrování.

Podniky si přejí silné šifrování i z jiného důvodu. Shromažďují rozsáhlé množství informací v počítačových databázích včetně popisu produktů, detailů o zákaznících a obchodních transakcích. Takové informace samozřejmě chtějí chránit před hackery, kteří by mohli proniknout do počítačů a data ukrást. Této ochrany lze dosáhnout zašifrováním uložených informací, takže jsou přístupné pouze zaměstnancům, kteří mají dešifrovací klíč.

Shrňme si situaci: je zřejmé, že debata probíhá mezi dvěma tábory, zastánci občanských práv a firmy podporují silné šifrování, zatímco orgány činné v trestním řízení jsou zastánci přísných omezení. Obecně se zdá, že veřejné mínění spíše podporuje prošifrovací alianci, které pomohla sympatizující média a několik hollywoodských filmů. Počátkem roku 1998 se v kinech promítal film *Mercury Rising*, příběh nové, údajně nerozlomitelné šifry NSA, kterou neúmyslně dešifruje devítiletý autistický chlapec. Agent NSA Alec Baldwin vyrazí zabít hocha, kterého pokládají za hrozbu národní bezpečnosti. Naštěstí má hoch po ruce Bruce Willise, který jej ochrání. Rovněž v roce 1998 uvedl Hollywood film *Nepřítel státu*, který pojednával o spiknutí NSA směřujícím k zavraždění politika, který

* Od doby napsání knihy proběhlo v této oblasti v USA mnoho změn směrem k velkému zmírnění vývozních omezení. V současné době je už do většiny zemí možné z USA vyvážet silné šifry. (Pozn. odborného lektora.)

podporuje silné šifrování. Politika skutečně zavraždí, ale právník ztělesněný Willem Smithem a rebel z NSA v podání Gena Hackma-na nakonec předají vrahy z NSA do rukou spravedlnosti. Oba filmy vykreslují NSA jako ještě hrozivější instituci než CIA; v mnoha ohledech převzala NSA roli strašáka ze strany establishmentu.

Zatímco lobby za šifrování hájí kryptografickou svobodu a lobby proti šifrování obhajuje kryptografická omezení, existuje třetí možnost, která by mohla vést ke kompromisu. Během posledního desetiletí kryptografové a zákonodárci zkoumali klady a zápory schématu známého jako *depozice klíčů* (key escrow). Pojem „depozice" se v právním smyslu obvykle vztahuje k dohodě, podle níž někdo svěří určitou sumu peněz třetí straně, která ji za daných podmínek doručí straně druhé. Například nájemce může uložit zálohu u advokáta, který ji odevzdá majiteli pronajímané nemovitosti v případě, že dojde k poškození majetku. V kryptografických pojmech znamená „depozice" toto: Alice dá kopii svého soukromého klíče depozitáři - nezávislému, spolehlivému prostředníkovi, který je zplnomocněn doručit soukromý klíč policii, pokud by někdy byly dostatečné důkazy o tom, že je Alice zapletena do zločinu.

Nejznámějším experimentem s depozicí kryptografických klíčů byl American Escrowed Encryption Standard, přijatý roku 1994. Jeho cílem bylo podpořit přijetí dvou šifrovacích systémů nazvaných Clipper a Capstone, které se měly používat pro telefonickou, resp. počítačovou komunikaci. Chce-li Alice použít Clipper, zakoupí telefon s předem nainstalovaným čipem obsahujícím informace o jejím tajném soukromém klíči. Jakmile si Alice takový telefon koupí, kopie jejího soukromého klíče v čipu se rozdělí na dvě poloviny. Pak se obě části odešlou dvěma různým federálním úřadům k uschování. Vláda Spojených států zastávala názor, že Alice bude mít takto přístup k bezpečnému šifrování a její soukromí by bylo narušeno jen tehdy, kdyby orgány činné v trestním *řízení* přesvědčily oba federální úřady, že mají důvod obdržet její deponovaný soukromý klíč.

Vláda Spojených států používala Clipper a Capstone pro svou vlastní komunikaci. American Escrowed Encryption Standard zavedla jako povinný pro podniky, které se účastní jejích aktivit a obchodují s ní. Ostatní podniky a jedinci takový závazek neměli, ale vláda doufala, že Clipper a Capstone se postupně stanou nejoblíbenější formou šifrování v USA. Tato politika se však neosvědčila. Myšlenka depozice klíčů nezískala mimo vládní kruhy mnoho příz-nivců. Zastáncům občanských práv se nelíbila myšlenka, že by úřady měly všechny klíče - přirovnali situaci ke skutečnými klíčům a ptali se, jak by se lidé cítili, kdyby vláda vlastnila klíče ke všem domům v zemi. Kryptografičtí experti zase upozorňovali, že jeden nepoctivý zaměstnanec může zničit celý systém, kdyby deponované klíče například prodával oproti nejvyšší nabídce. A podniky se bály o důvěrnost svých informací. Evropské firmy v Americe by se například mohly obávat, že jejich zprávy zachytí američtí komerční úředníci ve snaze získat tajemství, které by domácím rivalům poskytlo konkurenční výhodu.

Přes neúspěch systémů Clipper a Capstone se mnoho vlád stále domnívá, že depozici klíčů lze využít za předpokladu, že klíče budou dostatečně spolehlivě chráněny před zločinci, a za předpokladu, že budou k dispozici záruky, jež veřejnost uklidní a přesvědčí ji, že systém nepřipouští vládní zneužití. Bývalý ředitel FBI Louis J. Freeh v roce 1996 řekl: „Komunita ochránců zákona plně podporuje vyváženou politiku šifrování... Depozice klíčuje nejen jediným možným řešením, je to navíc velmi dobré řešení, protože účinně vyvažuje základní

společenské zájmy včetně ochrany soukromí, bezpečnosti informací, požadavků elektronického obchodu, veřejné a národní bezpečnosti." Přestože vláda Spojených států od svého návrhu ustoupila, mnozí lidé se domnívají, že se někdy v budoucnosti znovu vynasnaží zavést jinou formu depozice klíčů. Po neúspěchu dobrovolné depozice může dokonce uvažovat o povinné depozici klíčů. Lobby za šifrování i nadále vznáší námitky proti tomuto schématu. Novinář Kenneth Neil Cukier, který se zabývá novými technologiemi, napsal: „Lidé zapojení dó~ debaty o šifrování jsou vesměs inteligentní, čestní a jsou pro depozici klíčů, ale nikdy nemají více než dvě tyto vlastnosti najednou."

Vláda by mohla hledat i jiná řešení, aby se pokusila uvést do rovnováhy hlediska občanských práv, byznysu a vymahatelnosti práva. Není zdaleka jasné, která možnost bude preferována, protože v současnosti je kryptografická politika ve stavu neustálé změny. Stálý proud událostí na celém světě ovlivňuje rozhovory o šifrování. V listopadu 1998 oznámila britská královna ve svém proslovu chystanou legislativu týkající se digitálního obchodování. V prosinci 1998 po-depsalo 33 států Wassenaarskou dohodu limitující vývoz zbraní, která mimo jiné pokrývá silné kryptografické technologie. V lednu 1999 zrušila Francie své antikryptografické zákony, jež byly do té

doby nejvíce restriktivní v celé západní Evropě, a to pravděpodobně jako výsledek tlaku obchodní komunity. V březnu 1999 vydala britská vláda předběžný dokument týkající se navrhovaného zákona o elektronickém obchodu.

Než budete číst tuto knihu, odehrají se zřejmě další zvraty v diskusi o kryptografické politice. Jeden aspekt budoucí šifrovací politiky se však zdá být jistý, a tím je nutnost *certifikačníautority*. Pokud chce Alice poslat bezpečný e-mail svému novému příteli Zakovi, potřebuje Zakuv veřejný klíč. Může požádat Zaka, aby jí ho poslal poštou. Je tu však riziko, že Eva zachytí Zakuv dopis Alici, zničí jej a podvrhne nový dopis, který bude obsahovat namísto Zakova její vlastní veřejný klíč. Alice potom zašle delikátní mail Zakovi a nic zlého netušíc jej zašifruje Eviným veřejným klíčem. Pokud Eva tento e-mail zachytí, může jej snadno dešifrovat a přečíst. Jinými slovy, mezi problémy kryptografie s veřejným klíčem patří *otázka*, jistoty, zda skutečně máte veřejný klíč právě té osoby, se kterou chcete komunikovat. Certifikační autorita je organizace, která ověřuje, zda veřejný klíč odpovídá určité osobě. Certifikační autorita si může vyžádat osobní setkání se Zakem jako jeden ze způsobů, jak zaručit, že správně katalogizovala jeho veřejný klíč. Pokud Alice organizaci věří, může od ní obdržet *Zakuv* veřejný klíč a mít jistotu, že klíč je platný.

Vysvětlil jsem, jak Alice bezpečně nakupuje zboží na internetu pomocí veřejného klíče podniku k zašifrování objednávkového formuláře. Ve skutečnosti by to udělala pouze tehdy, kdyby byl veřejný klíč potvrzen certifikační autoritou. Roku 1998 stál v čele certifi-kačního trhu VeriSign, který během pouhých čtyř let vyrostl z nuly na společnost s obratem přes 30 milionů dolarů. Stejně jako zajiš-tují certifikační autority spolehlivé šifrování certifikováním veřejných klíčů, mohou také zaručit platnost digitálních podpisů. V roce 1998 eertifikovala irská společnost Baltimore Technologies veřejné klíče amerického prezidenta Billa Clintona a

irského předsedy vlády Bertie Aherna. Díky tomu mohli oba státníci digitálně podepsat komuniké v Dublinu.

Certifikační autorita nepředstavuje žádné riziko pro bezpečnost. Pouze požádá Zaka, aby jí ukázal svůj veřejný klíč, takže jej může potvrdit pro ostatní zájemce, kteří si mu přejí zasílat šifrované zprávy- Nicméně existují jiné společnosti, známé jako tzv. *důvěryhodné třetí strany* (trusted third parties - TTPs), které poskytují kontroverz-nejsí služby, jímž se říká *obnova klíče* (key recovery).Představte si právní firmu, která všechny své důležité dokumenty chrání tak, že je zašifruje svým veřejným klíčem, takže je může dešifrovat pouze vlastním soukromým klíčem. Takový systém funguje jako účinné opatření proti hackerům a komukoliv, kdo by se pokusil ukrást informace. Co se však stane, když zaměstnanec, který má v péči soukromý klíč, tento klíč zapomene, uprchne s ním nebo ho porazí autobus? Vlády podporují vznik agentur TIP a jsou nakloněny tomu, aby takové firmy měly kopie všech klíčů. Firma, která ztratí svůj soukromý klíč, jej bude moci dostat zpět, když naváže kontakt se svou TTP.

Důvěryhodné třetí strany jsou však poněkud kontroverzní, protože by získaly přístup k soukromým klíčům lidí, což by jim umožnilo číst zprávy svých zákazníků. Systém musí být spolehlivý, jinak je snadno zneužitelný. Někteří oponenti namítají, že TPPs nejsou ničím jiným než návratem systému depozice klíčů a že by se orgány činné v trestním řízení snadno mohly dostat do pokušení nutit zastrašováním představitele TTPs, aby jim během policejního vyšetřování vydali klíče klientů. Jiní hájí názor, že TTPs jsou nezbytnou součástí každé rozumně navržené infrastruktury veřejných klíčů.

Nikdo nemůže předpovědět, jakou roli budou TTPs hrát v budoucnosti, a nikdo nemůže s jistotou předvídat podobu kryptogra-fické politiky za deset let. Domnívám se však, že v blízké budoucnosti nejprve vyhraje lobby za šifrování - především proto, že žádná země nebude chtít zákon o kryptografii, který by zakazoval elektronický obchod. Pokud se však tato politika ukáže jako chybná, bude stále možné zákony změnit. Kdyby například došlo k vzestupu terorismu, potom by orgány činné v trestním řízení rychle získaly souhlas pro politiku depozice klíčů. Všichni uživatelé silného šifrování by byli nuceni uložit své klíče k depozitářům a od té chvíle by porušoval zákon každý, kdo by odeslal šifrovanou zprávu s nedeponova-ným klíčem. Pokud by byly tresty dostatečně přísné, potom by stát znovu získal kontrolu. Naopak, pokud by se později ukázalo, že vláda zneužívá důvěru spojenou se systémem depozice klíčů, veřejnost by se dožadovala návratu ke kryptografické svobodě a kyvadlo by se zhouplo nazpět. Není žádný důvod, proč bychom nemohli měnit svou politiku tak, aby odpovídala politickému, ekonomickému a společenskému klimatu. Rozhodující je, koho se veřejnost bojí více -zda zločinců, nebo vlády.

Zimmermannova rehabilitace

Roku 1993 se Phil Zimmermann stal předmětem vyšetřování velké poroty. Podle FBI vyvezl zbraně, protože dodával nepřátelským státům a teroristům nástroje, které potřebovali k tomu, aby se vyhnuli pravomoci vlády Spojených států. Jak se vyšetřování protahovalo, více a více kryptografů a zastánců

občanských práv přispěchalo Zimmermanna podpořit. Zřídili dokonce mezinárodní fond na financování jeho obhajoby. Skutečnost, že autora vyšetřuje FBI, pozvedla reputaci PGP a Zimmermannův výtvor se po internetu rozšiřoval ještě rychleji - vždyť to byl tak silný šifrovací software, že vystrašil i federály.

Program Pretty Good Privacy byl původně vypuštěn ve spěchu, a proto nebyl dotažen do takové podoby, do jaké by se slušelo. Brzy vznikla poptávka po revidované verzi PGP, ale Zimmermann nebyl v situaci, v níž by mohl pokračovat v práci na produktu. Místo toho začali PGP předělávat evropští programátoři. Evropský postoj k šifrování byl - a stále je - liberálnější než americký, vývoz evropské verze PGP do celého světa by nebyl nijak omezen. Ani spor o patent RSA nebyl v Evropě problémem, protože patent se vztahoval jen na USA.

Ani tři roky vyšetřování velkou porotou nepřivedly Zimmermanna před soud. Případ byl komplikovaný kvůli povaze PGP a způsobu jeho distribuce. Pokud by Zimmermann nahrál PGP do počítače a potom jej poslal do ciziny, byla by obžaloba jednoduchá, protože by byl jasně vinen vývozem úplného fungujícího šifrovacího systému. Podobně, pokud by vyvezl disketu obsahující program PGP, potom by tento fyzický předmět mohl být interpretován jako kryptografické zařízení a obžaloba proti Zimmermannovi by rovněž byla docela solidní. Na druhou stranu, pokud by počítačový program vytiskl a vyvezl jako knihu, právo by se již přiklánělo na stranu Zimmermanna, protože by jej museli pokládat spíše za vývozce znalostí než kryptografického zařízení. Tištěné materiály však lze jednoduše elektronicky naskenovat a informace znovu vložit do počítače, což znamená, že kníhaje stejně nebezpečná jako disk. Co se ale skutečně stalo: Zimmermann dal kopii PGP „příteli", který ji jednoduše nainstaloval na americký počítač, který byl „náhodou" připojen k internetu. Nepřátelské režimy si program mohly, ale nemusely stáhnout. Byl Zimmermann skutečně vinen vývozem PGP? Ještědnes jsou podobné právní problémy týkající se internetu předmětem sporů a rozličných interpretací. Počátkem 90. let byla situace zcela nejasná.

V roce 1996, po třech letech vyšetřování, úřad amerického generálního prokurátora stáhl žalobu. FBI si uvědomila, že je příliš pozdě - PGP pronikl na internet a soudním stíháním Zimmermanna se už nedalo ničeho dosáhnout. Kromě toho Zimmermanna podporovaly důležité instituce jako vydavatelství Massachusetts Institute of Technology Press, které publikovalo PGP v 600stránkové knize. Kniha byla distribuována po celém světě, takže soudní stíhání Zimmermanna by znamenalo také stíhání MIT Press. FBI se zdráhala pokračovat ve stíhání i proto, že bylo velmi pravděpodobné, že by Zimmermann nebyl odsouzen. Soud by tedy nedosáhl ničeho jiného než zahanbující ústavní debaty o právu na soukromí, a tím by ještě více podpořil kladný postoj veřejnosti k silnému šifrování.

Vyřešil se i další Zimmermannův závažný problém. Zimmermann dosáhl dohody s RSA a získal povolení, které odstranilo problém s patentem. PGP se stal legitimním produktem a Zimmermann byl volný. Vyšetřování z něj udělalo kryptografického hrdinu a každý marketingový manažer na světě musel závidět proslulost a bezplatnou reklamu, kterou PGP získal. Koncem roku 1997 prodal

Zimmermann PGP firmě Network Associates a stal se jedním z jejích vedoucích spolupracovníků*. Pro obchodní účely je nyní PGP komerčním produktem, je však stále zadarmo pro jednotlivce, kteří jej hodlají používat jen pro soukromé účely. Tito zájemci si nadále mohou PGP stáhnout z internetu bez placení.

Pokud chcete získat kopii PGP, existuje mnoho internetových stránek, které ji nabízejí, a měli byste ji najít docela snadno. Pravděpodobně nejspolehlivější zdroj je na http://www.pgpi.com/, což je mezinárodní domovská stránka PGP, z níž si můžete stáhnout americkou a mezinárodní verzi PGP. V tomto bodě bych se rád zbavil jakékoliv odpovědnosti - pokud se rozhodnete instalovat PGP, je na vás samých ověřit si, že se hodí pro váš počítač, že software není nakažen virem a podobně. Také byste si měli zjistit, zda se *nacházíte* v zemi, která povoluje používání silného šifrování. Nakonec byste

* V době překladu knihy do češtiny je již situace trochu jiná. Zimmermann odešel od Network Associates a založil novou společnost PGP Corporation, která v srpnu 2002 odkoupila větší část produktů na bázi PGP. (Pozn. odborného lektora.)

se měli přesvědčit, že jste si stáhli správnou verzi PGP. Osoby žijící mimo USA by totiž neměly používat americkou verzi PGP, protože by tím byly porušeny americké exportní zákony. Mezinárodní verze PGP nemá exportní omezení.

Stále si pamatuji nedělní odpoledne, kdy jsem poprvé stáhl kopii PGP z internetu. Od té doby mohu zajistit své e-maily proti čtení neoprávněnou osobou, protože nyní dovedu zašifrovat každý delikátní materiál určený Alici, Bobovi a komukoli dalšímu, kdo má PGP. Můj přenosný počítač a jeho software PGP mi poskytují takovou úroveň bezpečnosti, která přesahuje spojené úsilí všech světových zařízení na lámání kódů.**8**

Kvantový skok do budoucnosti

Po dva tisíce let se kryptografové snažili uchránit nejrůznější tajemství, zatímco kryptoanalytici usilovali o jejich odhalení. Byl to vždy vyrovnaný souboj, analytici zesilovali úsilí, kdykoli kryptografové nabyli převahy, ti zase vymýšleli nové a silnější formy šifrování zejména tehdy, když došlo k znehodnocení šifer starých. Vynález kryptografie s veřejným klíčem a politická debata týkající se používání silné kryptografie je tématem dnešních dní. Je jasné, že v dnešní době mají převahu kryptografové.* Podle Phila Zimmermanna žijeme ve zlatém čase kryptografie: „Dnes je možné v moderní kryptografii vytvořit šifry, které jsou vskutku mimo dosah všech známých forem kryptoanalýzy. A myslím, že to tak zůstane." Zimmermannův postoj sdílí i William Crowell, zástupce ředitele NSA: „Pokud by se všechny osobní počítače na světě - přibližně 260 milionů počítačů - daly společně do práce na jediné zprávě zašifrované PGP, pak střední odhad doby potřebné k rozluštění činí známou dobu existence vesmíru násobenou dvanácti miliony."

Dosavadní zkušenost nám nicméně ukazuje, že každá takzvaná nerozlomitelná šifra dříve nebo později kryptoanalytikům podlehla. Vigeněrově šifře se říkalo „le chiffre indéchiffrable", Babbage ji však rozlomil; Enigma byla považovaná také za

neprolomitelnou, dokud Poláci neodhalili její slabiny. Jsou tedy kryptoanalytici na pokraji dalšího průlomu, nebo má Zimmermann pravdu? Předpovídání budoucího rozvoje v každé technologii je vždy svízelný úkol, ale u šifer je zvláště riskantní. Nejen že musíme uhodnout, jaké objevy nás čekají v budoucnosti, ale je třeba také odhadnout, k jakým

* V době psaní knihy tomu tak možná bylo, v době překladu do češtiny není věc tak jasná. Došlo totiž k revolučnímu objevu tzv. *postranních kanálů*, které ukazují nové cesty útoků i na ty nejdokonalejší šifry. Přitom se útočí nikoli na jejich nejsilnější stránku, tj. matematickou podstatu, ale na tu nejslabší, což je způsob implementace. Postranní kanály se nevyhnou ani kvantové kryptografii. (Pozn. odborného lektora.)

objevům už došlo. Příběh Jamese Ellise a GCHQ nás varuje, že pozoruhodný objev může být skryt za závojem státního tajemství.

Tato závěrečná kapitola zkoumá několik futuristických myšlenek, jež mohou zesílit nebo zničit soukromí ve 21. století. Bezprostředně následující úsek textu se *zabývá*, budoucností kryptoanalýzy a zvláště pak jednou konkrétní myšlenkou, která může umožnit kryptoanalytikům rozlomit všechny dnešní šifry. Naproti tomu poslední část knihy zkoumá nejvíce vzrušující kryptografickou perspektivu, systém, který má potenciál zaručit absolutní soukromí.

Budoucnost kryptoanalýzy

Navzdory obrovské síle RSA a dalších moderních šifer jsou kryptoanalytici stále schopni hrát důležitou roli ve zpravodajské činnosti. Důkazem jejich důležitosti je i skutečnost, že poptávka po nich je dnes větší než kdykoliv dříve - NSA je stále největším světovým zaměstnavatelem matematiků.

Pouze malý zlomek informací putujících po světě je bezpečně zašifrován, zbytek je zašifrován špatně nebo vůbec ne. To proto, že počet uživatelů internetu rychle narůstá a jen málokdo přijímá adekvátní bezpečnostní opatření. To má za důsledek, že státní bezpečnostní organizace, orgány činné v trestním řízení a všichni další zvědavci mohou získat více informací, než lze zpracovat.

Dokonce i kdyby uživatelé pracovali s šifrou RSA správně, analytici mohou stále ještě dělat hodně pro to, aby získali informace ze zachycených zpráv. Kryptoanalytici dosud používají staromódní techniky, jako je analýza provozu, a i když se nemohou dostat na kloub obsahu zprávy, dovedou přinejmenším zjistit, kdo a komu ji poslal, což samo o sobě může mít velkou vypovídací hodnotu. K nejnovějším trendům patří elektromagnetický odposlech, jehož cílem je objevit elektromagnetické signály vyzařované elektronikou v obrazovce počítače. Pokud Eva zaparkuje dodávku před Aliciným domem, může použít citlivé vybavení, aby rozpoznala každý jednotlivý úder na klávesu Alicina počítače. To Evě umožní zachytit zprávu již [v] okamžiku, kdy se zapisuje do počítače, tedy předtím, než se zašifruje. Aby se tomu mohli uživatelé bránit, dodávají některé firmy stínící materiály, jimiž lze obložit stěny místnosti, aby nedošlo k úniku elektromagnetického signálu. V Americe je nezbytné před náku-pem takového stínícího materiálu dostat povolení od vlády, což svědčí o tom, že organizace jako

FBI se na popsaný typ odposlechu spoléhají.

Další typ útoku zahrnuje použití virů a trojských koní. Eva může vytvořit virus, který nakazí software PGP a tiše se usadí uvnitř Alici-na počítače. Když Alice použije svůj soukromý klíč k zašifrování zprávy, virus se vzbudí a zaznamená jej. Když se příště Alice připojí na internet, virus tajně odešle soukromý klíč Evě, a tak jí umožní dešifrovat všechny další zprávy adresované Alici. Trojský kůň, další softwarový trik, vyžaduje, aby Eva napsala program, který vypadá jako skutečný kryptografický produkt, ale ve skutečnosti uživatele zrazuje. Alice je například přesvědčena, že si z internetu kopíruje autentickou verzi PGP, zatímco ve skutečnosti stahuje trojského koně. Tato upravená verze vypadá přesně jako skutečný program PGP, ale obsahuje instrukce k zasílání původních textů veškeré Ali-ciny korespondence Evě. Jak říká Phil Zimmermann: „Kdokoli může změnit zdrojový kód a vytvořit imitaci PGP - lobotomizovanou zombii, která vypadá jako živá, přitom však plní záměry svého záludného pána. Tato trojská verze PGP se pak může široce rozšířit, protože vypadá, jako by pocházela ode mě. Jak záludné! Musíte se co nejvíce snažit, abyste svou kopii PGP získali ze spolehlivého zdroje, ať už to znamená cokoliv."

Obměnou trojského koně je regulérní šifrovací software, který se zdá být bezpečný, ale ve skutečnosti obsahuje zadní vrátka, tedy něco, co umožní jeho tvůrcům dešifrovat všechny zprávy. V roce 1998 odhalil Wayne Madsen, že švýcarská kryptografická společnost Crypto AG zabudovala zadní vrátka do některých svých produktů a poskytla americké vládě informace, jak tato zadní vrátka využívat. V důsledku toho mohli v USA číst komunikaci několika zemí. Útočníci, kteří v roce 1991 zavraždili Šachpúra Bachtiara, bývalého íránského předsedu vlády žijícího v exilu, byli dopadeni díky zachycení íránských zpráv, které byly zašifrovány produkty Crypto AG a následně dešifrovány pomocí zadních vrátek.

Přestože jsou analýza provozu, elektromagnetický odposlech, viry a trojští koně užitečné techniky sběru informací, kryptoanaly-tici si uvědomují, že jejich skutečným cílem je nalézt způsob, jak rozlomit RSA, základní kámen moderního šifrování. Šifra RSA se používá k ochraně nejdůležitějších vojenských, diplomatických, obchodních a zločineckých komunikací - přesně těch zpráv, které

zpravodajské služby chtějí dešifrovat. Mají-li kryptoanalytici zvládnout silné šifrování RSA, musí dojít k zásadnímu teoretickému nebo technickému průlomu.

Teoretickým průlomem by byla zásadně nová cesta nalezení Ali-cina soukromého klíče. Alicin soukromý klíč sestává z p a q, výsledků faktorizace jejího veřejného klíče N. Standardní přístup je prověřit každé prvočíslo, zda dělí N, ale víme, že tento postup zabere extrémní množství času. Kryptoanalytici se pokoušeli najít jakousi zkratku, metodu, která by drasticky snížila počet kroků potřebných pro nalezení p a q, dosud však všechny pokusy vyvinout návod k rychlé faktorizaci skončily neúspěchem. Matematici studovali faktorizaci po staletí, přesto nejsou moderní techniky faktorizace významně lepší než ty staré. Je možné, že matematické zákony neumožňují existenci významnější zkratky vedoucí k faktorizaci.

Protože naděje na teoretický průlom je malá, kryptoanalytici se museli soustředit na hledání technologické inovace. Pokud neexistuje způsob, jak snížit počet kroků nutných pro faktorizaci, potom kryptoanalytici potřebují technologii, která by tyto kroky zvládla rychleji. Křemíkové čipy budou i nadále zdvojnásobovat svou rychlost zhruba každých 18 měsíců, to ale není růst dostatečně velký na to, aby mohl mít skutečný dopad na rychlost faktorizace - kryptoanalytici vyžadují technologii, která je miliardkrát rychlejší než běžné počítače. Proto hledí s nadějí k radikálně novému typu počítače - ke *kvantovému počítači*. Kdyby jej vědci dokázali sestavit, byl by schopen provádět výpočty tak obrovskou rychlostí, že by vedle něj vypadal moderní superpočítač jako polámané kuličkové počitadlo.

Zbývající část této kapitoly se bude zabývat konceptem kvantového počítače, a proto představí některé principy kvantové fyziky, někdy nazývané kvantovou mechanikou. Než se vydáme dál, dbejte prosím varování, které původně vyslovil Niels Bohr, jeden z otců kvantové mechaniky: „Každý, kdo přemýšlí o kvantové mechanice, aniž by se mu zatočila hlava, jí nerozumí." Jinými slovy, připravte se, že se setkáte s některými poměrně šílenými myšlenkami.

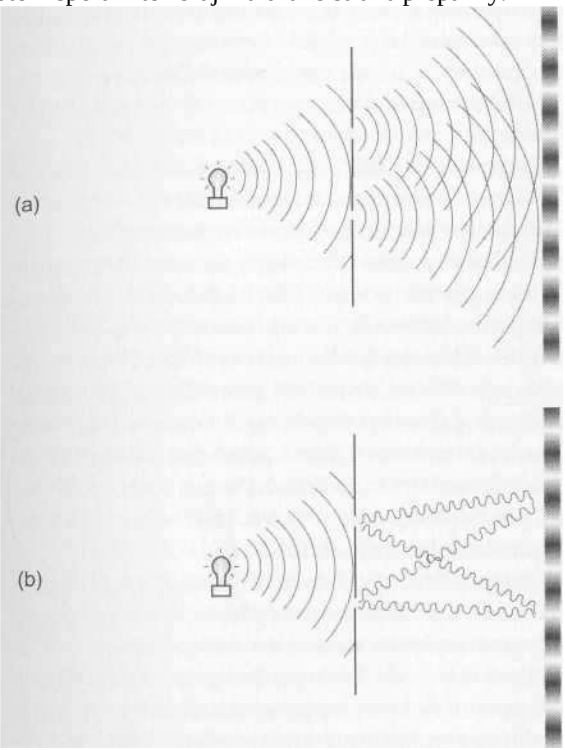
Pro vysvětlení principů kvantové mechaniky se nejprve vrátíme na konec 18. století k práci anglického polyhistora Thomase Youn-ga, který učinil první pokrok v rozluštění egyptských hieroglyfů. Young jako člen Emmanuel College v Cambridgi často trávil odpoledne odpočinkem poblíž školního rybníka s kachnami. Jednoho dne, jak se traduje, si všiml dvou kachen šťastně plovoucích bok po boku. Zpozoroval, že za sebou zanechávají dvojici zvlněných stop, jež se prolínají a vytvářejí zvláštní vzor z klidných a vlnících se míst. Když se hřeben vlny, kterou za sebou zanechala jedna kachna, setkal s poklesem hladiny po kachně druhé, bylo výsledkem drobné místo klidné vody - hřeben a pokles se navzájem zrušily. Naopak, pokud dorazily dva hřebeny na stejné místo zároveň, výsledkem byl ještě vyšší hřeben vlny. Podobně, když se setkaly dva poklesy, došlo k poklesu ještě hlubšímu. Younga to fascinovalo, protože mu kachny připomněly jeho vlastní pokus z roku 1799, kterým zkoumal povahu světla.

Young ve svém pokusu svítil na přepážku, ve které byly dvě úzké svislé štěrbiny, jak ukazuje schéma 71(a). Očekával, že na stěně za přepážkou uvidí dva světlé pruhy, projekce světla. Místo toho pozoroval, že světlo vycházející ze dvou štěrbin vytvořilo na stěně vzor několika světlých a tmavých pruhů. S pruhovaným světelným vzorem na stěně si Young dlouho nevěděl rady, náhle však pochopil, že jej může vysvětlit pomocí úkazu, který spatřil na rybníku.

Vyšel z předpokladu, že světlo má podobu vlny. Pokud se světlo vyzařující ze dvou štěrbin chová jako vlna, pak pro něj platí stejný princip jako pro dvě kachní stopy na hladině rybníka. Světlé a tmavé pruhy na stěně byly způsobeny stejným vzájemným působením, jež zapříčinilo, že vodní vlny tvořily vysoké vrcholy, hluboké prolák-liny a klidná místa. Young si představil místo na stěně, kde se pokles setkal s vrcholem, takže došlo ke zrušení světelného obrazu a výsledkem byl tmavý pruh, a naopak jiné místo na stěně, kde se setkaly dva vrcholy (nebo dva poklesy), bylo ozářeno ještě intenzivnějším světlým pruhem, jak ukazuje schéma

71(b). Kachny poskytly Youngovi hlubší pochopení skutečné podstaty světla. Své závěry nakonec publikoval jako „vlnovou teorii světla", což je jedna z nejklasičtějších fyzikálních statí všech dob.

Dnes víme, že se světlo opravdu chová jako vlna, ale rovněž víme, že se také může chovat jako částice. Zda vnímáme světlo jako vlnu nebo jako částici, *záleží* na okolnostech. Tato dvojznačnost světlaje známá jako vlnově korpuskulární dualita. Myji nepotřebujeme rozebírat podrobněji, pouze si řekneme, že moderní fyzika vychází z představy světelného paprsku, který je tvořen nesčetnými jednotlivými částicemi, známými jako fotony, jež mají vlnové vlastností. Z tohoto pohledu můžeme Youngův pokus interpretovat pomocí fotonů, jež zaplaví štěrbiny a potom spolu interferují na druhé straně přepážky.



Obrázek 71: Youngův experiment se štěrbinami, pohled shora. Diagram (a) ukazuje světlo přicházejíc! ze dvou štěrbin v přepážce a tvořící pruhovaný vzor na stěně. Diagram (b) ukazuje, jak interagují jednotlivé vlny. Pokud se setká na stěně proláklina s vrcholem, výsledkem je tmavý pruh. Pokud se na stěně setkají dvě prolákliny (nebo dva vrcholy), výsledkem je světlý pruh.

Až dosud nebylo na Youngově experimentu nic skutečně neobvyklého. Moderní technologie však umožňuje fyzikům pokus opakovat s využitím světelného zdroje tak slabého, že vysílá pouze jediný foton. Řekněme, že každou minutu se vytvoří jeden foton, který letí sám k přepážce. Někdy foton projde jednou ze dvou štěrbin a narazí na stěnu. Přestože naše oči nejsou tak citlivé, aby spatřily jednotlivé fotony, lze je pozorovat pomocí speciálních detektorů. Za

nějakou dobu, řekněme za hodinu, můžeme získat celkový obrázek. Protože v každém konkrétním okamžiku prochází přepážkou pou-ze jeden foton, neměli bychom očekávat, že uvidíme pruhovaný vzor pozorovaný Youngenr, protože ten je zřejmě vytvořen přinejmenším dvěma fotony, jež současně prolétnou různými štěrbinami a navzájem se střetnou na druhé straně. V našem pokusu s jedním fotonem očekáváme, že uvidíme jen dva světlé pruhy, jednoduchý průmět štěrbin v přepážce. Je tomu však jinak - z nějaké neobyčejné příčiny je i s jednotlivými fotony výsledný obraz na stěně stále týž - vzor světlých a tmavých pruhů, stejně jako když fotony interagovaly.

Tento zvláštní výsledek se vzpírá zdravému rozumu. Neexistuje způsob, jak takový úkaz vysvětlit pomocí klasických fyzikálních zákonů, kterými popisujeme a zdůvodňujeme chování předmětů v našem každodenním životě. Klasická fyzika může vysvětlit oběžné dráhy planet nebo trajektorii dělové koule, ale nemůže úplně popsat svět velmi malých měřítek, jako například trajektorii fotonu. Proto se fyzikové uchylují ke kvantové teorii, která popisuje, jak se objekty chovají v mikroskopickém měřítku. Avšak ani kvantoví teoretikové se neshodují na tom, jak popsaný pokus vysvětlit. Dělí se na dva tábory, z nichž každý má vlastní interpretaci.

První tábor postuluje myšlenku známou jako *superpozice*. Super-pozicionisté začínají tvrzením, že v tomto pokusu víme s jistotou jen dvě věci - foton opustí zdroj a narazí do stěny. Vše ostatní je naprosté tajemství včetně toho, zda foton proletí pravou nebo levou štěrbinou. Protože přesná dráha fotonu je neznámá, superpozicio-nisté zastávají výstřední *názor,* že foton nějak proletí oběma štěrbi-nami najednou, což mu pak umožňuje interferovat se sebou samým a vytvořit pruhovaný vzor pozorovaný na stěně. Ale jak je možné, že jeden foton proletí oběma štěrbinami?

Superpozicionisté argumentují následujícím způsobem: pokud nevíme, co částice dělá, potom může dělat cokoliv. V případě fotonu nevíme, zda proletěl levou nebo pravou štěrbinou, takže předpokládáme, že prošel oběma štěrbinami najednou. Každé z možností se říká *stav,* a protože foton naplní obě možnosti, říkáme, že je v *superpozici stavů.* Víme, že zdroj opustil jeden foton, a víme, že jeden foton narazil na stěnu na druhé straně příčky. Mezi tím se však rozdělil ve dva „fotony-duchy", které proletěly oběma štěrbinami. Superpozice se může zdát potrhlá, ale přinejmenším vysvětluje pruhovaný vzor, který je výsledkem Youngova pokusu prováděného s jednotlivými fotony. Pro porovnání - staromódní klasický názor říká, že foton musel proletět jednou ze dvou štěrbin, a my jednoduše nevíme, kterou - to se zdá daleko rozumnější než kvantový pohled, ale bohužel to nemůže vysvětlit pozorovaný výsledek.

Erwin Schródinger, který získal Nobelovu cenu za fyziku v roce 1933, vymyslel podobenství známé jako „Schródingerova kočka", které se často používá, aby pomohlo vysvětlit koncept superpozice. Představte si kočku v krabici. Existují dva možné stavy kočky: smrt nebo život. Na počátku víme, že kočka je určitě v jednom konkrétním stavu, protože vidíme, zeje živá. V tomto momentu kočka není v superpozici stavů. Potom do krabice s kočkou vložíme ampulku s kyanidem a

zavřeme víko. Nyní vstupujeme do období nevědomosti, protože kočku nevidíme ani nemůžeme její stav zjistit. Je stále naživu, nebo rozbila ampulku kyanidu a zemřela? Normálně bychom řekli, zeje kočka buď živá, nebo mrtvá, jen nevíme, co z toho platí. Kvantová teorie namísto toho říká, že kočka je v superpozici stavů - je zároveň živá i mrtvá, vyhovuje oběma možnostem. Superpozice nastává, pouze když nějaký předmět spustíme z očí - je to způsob, jak popsat jeho stav během období nejasnosti. Když nakonec otevřeme krabici, vidíme, zda je kočka živá nebo mrtvá. To, že se na kočku podíváme, ji donutí být v jednom určitém stavu a přesně v tento moment superpozice zmizí.

Pro čtenáře, kteří nejsou ze superpozice zrovna moudří, je tu další kvantový tábor, který dává přednost jinému výkladu Youngova pokusu. Tento alternativní pohled je bohužel neméně podivný. Tzv. *interpretace mnoha světů* tvrdí, že poté, co foton opustí zdroj, má dvě možnosti - buď proletět levou, nebo pravou štěrbinou - a v tomto bodě se vesmír dělí na dva vesmíry, v jednom vesmíru foton proletí levou štěrbinou, v druhém vesmíru proletí pravou. Tyto dva světy nějak interferují navzájem, což vysvětluje pruhovaný vzor. Přívrženci interpretace mnoha světů se domnívají, že kdykoliv má předmět možnost vstoupit do několika možných stavů, rozdělí se vesmír do mnoha vesmírů, aby byla každá možnost naplněna v jiném vesmíru. O tomto rozrůstání počtu vesmírů se mluví jako o *multiversu*, mnohovesmíru.

Ať přijmeme superpozici nebo interpretaci mnoha světů, je kvantová teorie filosofií, nad níž se nám zatočí hlava. Ukázala se však jako nejúspěšnější a nejpraktičtější vědecká teorie, která byla kdy vymyšlena. Mimo své jedinečné schopnosti vysvětlit výsledek Youngova pokusu kvantová teorie úspěšně objasňuje mnohé další fenomény. Jen kvantová teorie umožňuje fyzikům vypočítat násled-ky jaderné reakce v elektrárně; jen kvantová teorie dokáže vysvětlit zázrak DNA; jen kvantová teorie objasňuje, jak slunce září; jen pomocí kvantové teorie lze sestavit laser, který čte zápis na CD ve vašem přehrávači. Ať se vám to tedy líbí nebo ne, žijeme v kvantovém světě.

Ze všech důsledků kvantové teorie je možná technologicky nejvýznamnější právě kvantový počítač. Nejenže by zničil bezpečnost všech moderních šifer, zahájil by také zcela novou éru výpočetní techniky. Jedním z průkopníků kvantového počítání je britský fyzik David Deutsch, který na tomto konceptu začal pracovat roku 1984, kdy se zúčastnil konference o teorii počítání. Všiml si přitom něčeho, co předtím přehlédl. Nevyřčeným předpokladem bylo, že všechny počítače v podstatě fungují podle zákonů klasické fyziky, ale Deutsch došel k názoru, že by se měly místo toho řídit zákony fyziky kvantové, protože ty jsou hlubší.

Obyčejné počítače operují víceméně na makroskopické úrovni, na níž jsou kvantové a klasické zákony téměř nerozlišitelné. Proto nehrálo žádnou roli, že vědci obvykle uvažovali o počítačích v pojmech klasické fyziky. Ale na mikroskopické úrovni se tyto dva soubory zákonů odchylují a klasické fyzikální zákony přestávají platit. Na mikroskopické úrovni odhalují kvantové zákony svou neobvyklost; počítače sestrojené tak, aby jich využívaly, se budou chovat naprosto odlišně. Po konferenci se Deutsch vrátil domů a začal přepracovávat teorii počítačů

ve světle kvantové fyziky. V článku publikovaném roku 1985 popsal svou vizi kvantového počítače, který pracuje podle zákonů kvantové fyziky. Především pak popsal, jak se jeho kvantový počítač liší od počítače běžného.

Představte si, že máte dvě verze otázky. Abyste odpověděli na obě otázky pomocí obyčejného počítače, musíte nejdříve vložit první verzi a čekat na odpověď, potom vložit druhou verzi a zase čekat na odpověď. Jinými slovy, obyčejný počítač dokáže řešit najednou pouze jednu otázku, pokud je otázek více, je nutné je zpracovat jednu po druhé. S kvantovým počítačem však lze dvě otázky kombinovat jako superpozici dvou stavů a vložit je zároveň - sám přístroj potom vstoupí do superpozice stavů, z nichž každý bude odpovídat jedné otázce. Nebo - podle interpretace mnoha světů - přístroj vstoupí do dvou různých vesmírů a zodpoví každou verzi otázky v jiném vesmíru. Bez ohledu na interpretaci dokáže kvantový počítač zodpovědět dvě otázky najednou tím, že využívá zákonů kvantové fyziky.

Abychom měli představu o síle kvantových počítačů, můžeme porovnat jejich výkon s výkonem tradičních počítačů. Oba počítače by se například mohly pustit do problému nalezení čísla, jehož druhá a třetí mocnina dohromady obsahují všechny číslice od 0 do 9, každou pouze jednou. Pokud ověříme číslo 19, zjistíme, že $19^2 = 361$ a $19^3 = 6\,859$. Číslo 19 nesplňuje naše požadavky, protože jeho druhá a třetí mocnina obsahují pouze tyto číslice: 1, 3, 5, 6, 6, 8, 9, tj. číslice 0, 2, 4, 7 chybí a číslice 6 se opakuje.

Máme-li tento problém vyřešit pomocí tradičního počítače, bude třeba postupovat takto: operátor vloží číslo 1 a nechá jej otestovat. Jakmile počítač vykoná potřebné výpočty, sdělí, zda číslo 1 kritéria splňuje či nesplňuje. Pokud číslo 1 nesplňuje kritéria, operátor vloží číslo 2 a nechá proběhnout další test a tak dále, dokud není nakonec nalezeno vhodné číslo. Ukáže se, že odpovědí je číslo 69, protože $69^2 = 4\,761$ a $69^3 = 328\,509$, tato čísla vskutku zahrnují každou z deseti číslic jednou a pouze jednou. 69 je dokonce jediné číslo, které tyto podmínky splňuje. Je jasné, že tento proces je časově náročný, protože tradiční počítač může testovat najednou pouze jedno číslo. Pokud počítači zabere testování jednoho čísla jednu vteřinu, potom nalezení odpovědi trvá 69 vteřin. V porovnání s tím kvantový počítač nalezne odpověď v jedné vteřině.

Operátor začne tím, že čísla vyjádří speciálním způsobem tak, aby využil síly kvantového počítače. Jeden způsob, jak vyjádřit čísla,spočívá ve využití rotace neboli spinu částice - mnohé částice mají vlastní charakteristickou rotaci, mohou se točit ve směru hodinových ručiček či proti směru jako basketbalový míč, který se točí na špičce prstu. Když částice rotuje ve směru hodinových ručiček, znázorňuje číslo 1, pokud rotuje opačně, znázorňuje 0. Rada rotujících částic představuje řadu jedniček a nul neboli binární číslo. Například sedm částic, které rotují každá jednotlivě po směru, po směru, proti směru, po, proti, proti, proti, představuje společně binární číslo 1101000, které odpovídá číslu 104 v desítkové soustavě. Kombinace sedmi částic může představovat jakékoli číslo mezi 0 a 127.

S tradičním počítačem bychom pracovali tak, že by operátor vložil určitou sekvenci spinu, jako třeba proti, proti, proti, proti, proti, proti, po, což představuje

0000001 neboli decimální číslo 1. Operátor by pak čekal, až počítač číslo otestuje, aby zjistil, zda splňuje stanovená kritéria. Potom by vložil 0000010, což by byla sekvence částic představující číslo 2 a tak dále. Stejně jako předtím je třeba vkládat čísla po jednom, což je časově náročné. Když však máme co do činění s kvantovým počítačem, existuje alternativní způsob vkládání čísel, který je daleko rychlejší. Protože jde o elementární částice, řídí se zákony kvantové fyziky. Když není částice pozorována, může vstoupit do superpozice stavů, a tak reprezentovat najednou 0 i 1. Anebo můžeme o částicích uvažovat jako o složkách dvou různých vesmírů: v jednom vesmíru částice rotuje po směru hodinových ručiček a představuje 1, zatímco v druhém proti směru a představuje 0.

Superpozice se dosáhne následujícím způsobem: představte si, že pozorujeme jednu z částic, která rotuje proti směru. Abychom změnili její spin, vyšleme dostatečně silný energetický puls, aby převedl částici do opačného spinu. Kdybychom vyslali slabší záblesk, mohli bychom sice mít někdy štěstí a částice by skutečně spin změnila, jindy bychom však štěstí neměli a částice by pokračovala v původním spinu. Dosud byla částice stále na očích, a proto jsme byli schopni sledovat její vývoj. Když však částici, která rotuje například proti směru, ukryjeme před našimi zraky do krabice a zapůsobíme na ni slabým energetickým pulsem, potom nemáme představu, zda se spin změnil. Částice vejde do superpozice obou možných spinu, stejně jako kočka vkročila do superpozice života a smrti. Když vezmeme sedm částic rotujících proti směru, vložíme je do krabice a vyšleme na ně sedm slabých záblesků energie, pak všech sedm částic vejde do superpozice.

Všech sedm částic v superpozici ve skutečnosti představuje všechny možné kombinace kladného a záporného spinu. Sedm částic zároveň představuje 128 různých stavů nebo 128 různých čísel. Operátor vloží sedm částic, nacházejících se v superpozici stavů, do kvantového počítače, který potom vykoná své výpočty, jako by testoval najednou všech 128 čísel. Po jedné vteřině vydá počítač jako výstup číslo 69, které splňuje požadovaná kritéria. Operátor získá 128 výpočtů za cenu jednoho.

Kvantový počítač popírá zdravý rozum. Pokud na chvíli zapomeneme na detaily, můžeme o kvantovém počítači přemýšlet dvěma různými způsoby podle toho, které kvantové interpretaci dáváme přednost. Někteří fyzikové nahlížejí na kvantový počítač jako na jedinou entitu, která provádí stejný výpočet zároveň se 128 čísly. Jiní jej chápou jako 128 entit, z nichž každá se nachází v odlišném vesmíru a vykonává pouze jeden výpočet. Kvantové počítání je technologie jako ze sci-fi filmu.

V případě tradičních počítačů, které pracují s nulami a jedničkami, se těmto číslicím říká bity, což je zkratka pro „binary digits", binární číslice. Protože kvantový počítač pracuje s jedničkami a nulami, které jsou v kvantové superpozici, říká se jim kvantové bity neboli *qubity*. Výhoda qubitů je jasnější, když vezmeme v úvahu více částic. S 250 částicemi neboli 250 qubity je možné vyjádřit zhruba 10^{73} kombinací, což je více než počet atomů ve vesmíru. Pokud by bylo možné dosáhnout vhodné superpozice 250 částic, kvantový počítač by mohl vykonat 10^{7S} souběžných výpočtů, všechny dokončené během jediné vteřiny.

Využití těchto efektů může zapříčinit vznik nepředstavitelně výkonných kvantových počítačů. Když však Deutsch vytvořil v polovině 80. let svou vizi kvantového počítače, nikdo neměl ani tušení, jak sestrojit prakticky fungující zařízení založené na tomto principu. Vědci nebyli například ani schopni sestavit něco, co by dovedlo počítat s částicemi v superpozici stavů. Jednou z největších překážek bylo udržet superpozicí stavů v průběhu celého výpočtu. Superpozice existuje pouze tehdy, když ji nepozorujeme, ale pozorování v nejobecnějším smyslu zahrnuje jakoukoli interakci s čímkoliv, co vystupuje vůči superpozici jako vnější prvek. Pouhý zatoulaný atom interagující s jednou z částic by zapříčinil, že by se superpozice zřítila do jednotného stavu a zapříčinila tak neúspěch kvantového výpočtu.Další problém spočíval v tom, že nikdo nevěděl, jak kvantový počítač naprogramovat, a vědci si tedy nebyli jisti, k jakému druhu výpočtů by se hodil. Až v roce 1994 Peter Shoř z AT&T Bell Laboratories v New Jersey uspěl v definování užitečného programu pro kvantový počítač. Pozoruhodnou novinkou pro kryptografy bylo, že Shorův program definoval sérii kroků, které by mohl kvantový počítač použít k faktorizaci obrovského čísla - přesně to bylo zapotřebí pro rozlomení šifry RSA. Když Martin Gardner předložil svou výzvu v časopise *Scientific American,* zabrala faktorizace 129ci-ferného čísla šesti stovkám počítačů několik měsíců. Naproti tomu Shorův program mohl faktorizovat miliónkrát větší číslo jen za zlomek tohoto času. Shoř však bohužel nemohl předvést svůj program v praxi, protože stále ještě nic takového jako kvantový počítač neexistovalo.

Lov Grover, který také působil v Bell Labs, sestavil roku 1996 další výkonný program. Groverův program řeší úlohu, jak prohledat jakýkoli seznam neuvěřitelně vysokou rychlostí, což nemusí vypadat zvlášť zajímavě, dokud si neuvědomíme, že se právě tato schopnost vyžaduje pro rozlomení šifry DES. K tomu je třeba prohledat seznam všech možných klíčů, aby se našel ten správný. Jestliže konvenční počítač prohledá milion klíčů za vteřinu, prolomení šifry DES by mu zabralo více než tisíc let, zatímco kvantový počítač s Groverovým programem by mohl najít klíč dříve než za čtyři minuty.

Je čistě náhodné, že první dva programy pro kvantové počítače, které vědci vymysleli, byly přesně tím, co by kryptoanalytici ve svém seznamu priorit dali na první místo. Přestože Shorův a Groverův program vyvolal mezi kryptoanalytiky obrovský optimismus, byly oba programy také zdrojem nesmírné frustrace, protože fungující kvantový počítač nebyl k dispozici. Jistě nás nepřekvapí, že možnost objevu konečné zbraně v dešifrovací technologii povzbudil apetit takových organizací jako například americké Defense Advanced Research Projects Agency (DARPA) a Los Alamos National Labora-tory, které se ze všech sil snaží vybudovat zařízení, jež dokáže zacházet s qubity stejným způsobem, jako *zachází* křemíkové čipy s bity. Ačkoliv některé nedávné objevy zvýšily optimismus výzkumníků, je poctivé říci, že celá technologie je teprve v plenkách. Serge Haroche z pařížské univerzity uvedl roku 1998 do správné souvislosti tvrzení, že vznik skutečného kvantového počítače je na dosah. Řekl, že je

to *totéž,* jako bychom s vypětím sil sestavili první řadu domečku z karet a pak se vychloubali, že dalších 15 000 řad už představuje pouhou formalitu.

Pouze čas ukáže, zda a kdy bude problém konstrukce kvantového počítače zdolán. Mezitím můžeme pouze spekulovat o tom, jaký dopad by to mělo na svět kryptografie. Od 70. let 20. století tvůrci kódů jasně vedou v souboji s kryptoanalytiky, a to díky šifrám jako DES a RSA (posléze Triple DES, resp. AES). Tyto druhy šifer jsou důležitým výdobytkem, protože jim důvěřujeme do té míry, že pomocí nich šifrujeme své e-maily a chráníme své soukromí. Postupem času bude stále více a více obchodních aktivit provozováno přes internet a elektronický trh se bude spoléhat na silné šifry, které by chránily a ověřovaly finanční transakce. Úměrně tomu, jak se informace stávají nejcennějším zbožím na světě, závisí také ekonomický, politický a vojenský osud států stále ve větší míře na síle šifer.

Následkem toho by rozvoj plně provozuschopných kvantových počítačů ohrozil naše soukromí, zastavil elektronický obchod a zničil koncept národní bezpečnosti. Kvantový počítač by ohrozil stabilitu světa. Kterákoliv země, která takového objevu dosáhne jako první, bude mít schopnost monitorovat komunikaci občanů, číst myšlenky svých obchodních rivalů a naslouchat plánům svých nepřátel. Přestože je kvantové počítání teprve na počátku, představuje potenciální hrozbu jednotlivcům, mezinárodnímu obchodu a globální bezpečnosti.

Kvantová kryptografie

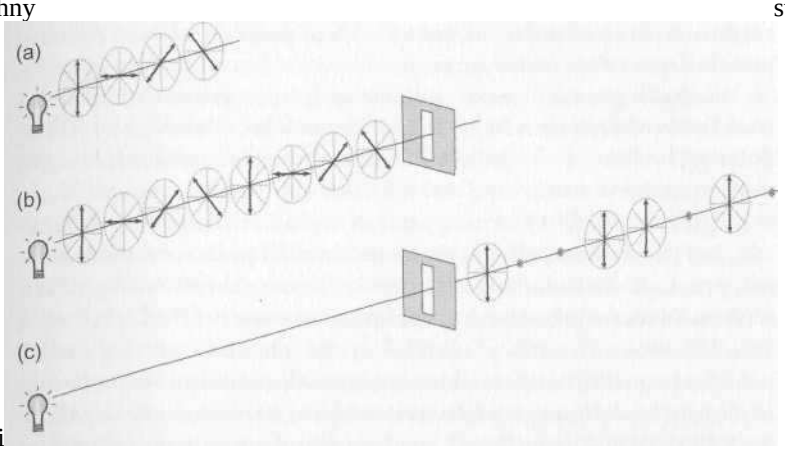
Zatímco kryptoanalytici předvídají příchod kvantových počítačů, kryptografové pracují na vlastním technologickém *zázraku* - šifrovacím systému, který znovu nastolí soukromí, dokonce i když bude čelit plné síle kvantového počítače. Tato nová forma šifrování je zásadně odlišná od kterékoli jiné šifry, na niž jsme dosud *narazili,* protože nabízí naději na dokonalé soukromí. Jinými slovy, tento systém bude bezchybný a zaručí na věky naprostou bezpečnost. Navíc je založen na kvantové teorii, stejné teorii, která je základem kvantového počítače. Takže zatímco kvantová teorie je inspirací pro počítače, které mohou rozlomit všechny současné šifry, je také zároveň jádrem nové, nerozlomitelné šifry zvané *kvantová kryptografie.*Příběh kvantové kryptografie začal neobvyklou myšlenkou, kterou koncem 60. let rozvinul Stephen Wiesner, v té době postgraduální student na Kolumbijské univerzitě. Wiesner měl smůlu, svou dobu totiž předběhl natolik, že ho nikdo nebral vážně. Stále si vybavuje reakci svých nadřízených: „Můj profesor mě vůbec nepodpořil - neprojevil absolutně žádný zájem. Ukázal jsem to několika dalším lidem a všichni nasadili divné obličeje a vrátili se hned k tomu, co zrovna dělali." Wiesner navrhl podivný koncept kvantových peněz, které měly tu výhodu, že se nedaly padělat.

Wiesnerovy kvantové peníze vycházely z fyziky fotonů. Když foton cestuje prostorem, vibruje - viz schéma 73 (a). Všechny čtyři fotony na schématu letí ve stejném směru, ale úhel vibrace je u každého z nich jiný. Uhlu vibrace se říká polarizace fotonu. Žárovka vytváří fotony všech polarizací, což znamená, že některé z nich kmitají nahoru a dolů, některé ze strany na stranu a některé ve všech ostatních úhlech. Abychom problém zjednodušili, budeme předpokládat, že fotony mají pouze čtyři možné polarizace, které označíme I, *-», \a/.

Tím, že fotonům umístíme do cesty tzv. polarizační filtr, je možné zajistit, aby

se paprsek světla skládal z fotonů, které kmitají v jednom určitém směru; jinými slovy, všechny fotony mají stejnou polarizaci. Do určité míry si můžeme polarizační filtr představit jako mřížku a fotony jako zápalky, které jsou na mřížce náhodně rozházené. Zápalky mříží propadnou pouze tehdy, pokud jsou ve správném úhlu. Každý foton, který je polarizovaný ve stejném směru jako polarizační filtr, automaticky projde beze změny, zatímco fotony, které jsou polarizovány kolmo na filtr, budou zablokovány.

Analogie se zápalkami bohužel končí, pokud uvažujeme o úh-lopříčně polarizovaných fotonech, které se přibližují ke svisle polarizovanému polarizačnímu filtru. Přestože zápalky orientované úhlopříčně jsou blokovány svisle orientovanou mřížkou, tento princip nutně neplatí pro úhlopříčně polarizované fotony, které se přibližují ke svislému polarizačnímu filtru. Úhlopříčně polarizované fotony jsou před svislým polarizačním filtrem v kvantovém dilematu. Co se stane? Náhodně vybraná polovina fotonů bude zablokována, zatímco druhá polovina projde, ty fotony, které projdou, nabudou svislé polarizace. Schéma 73 (b) ukazuje osm fotonů, které se blíží ke svislému polarizačnímu filtru, a schéma 73 (c) znázorňuje čtyři fotony, jež úspěšně prošly. Všechny svisle polari



Obrázek 73: (a) Přestože fotony světla kmitají ve všech směrech, pro jednoduchost předpokládejme, že existují pouze čtyři různé směry, jak ukazuje tento diagram.

(b) Lampa vyslala osm fotonů, které kmitají v různých směrech. Říkáme, že každý foton má polarizaci. Fotony směřují ke svislému polarizačnímu filtru.

(c) Na druhou stranu filtru prošla pouze polovina fotonů. Svisle polarizované fotony prošly, vodorovně polarizované fotony nikoli. Polovina úhlopříčně polarizovaných fotonů prošla přes filtr a získala tak svislou polarizaci.

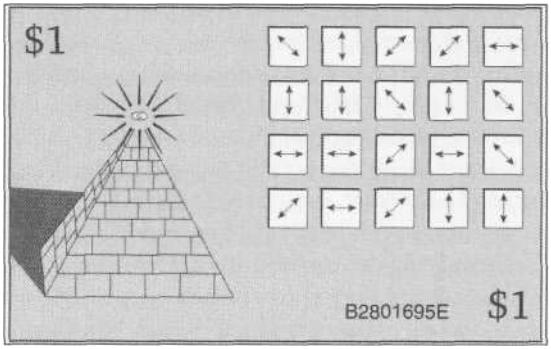
zované fotony prošly skrz, všechny vodorovně polarizované fotony byly zablokovány a polovina úhlopříčně polarizovaných fotonů prošla filtrem.

Právě schopnost blokovat určité fotony vysvětluje, jak fungují polarizační brýle. S nimi si můžete účinek polarizačních filtrů vyzkoušet. Nejdříve z brýlí odstraňte jedno sklíčko a zavřete příslušné oko, takže se díváte pouze druhým

okem přes zbývající sklo. Asi vás nepřekvapí, že svět vypadá poměrně tmavě, protože čočka blokuje hodně fotonů, které by jinak dorazily do vašeho oka. Všechny fotony, které dopadají na sítnici, mají v této situaci stejnou polarizaci. Pak přidržte druhou čočku před tou, kterou se díváte, a pomalu jí otáčejte. V určitém bodě otáčení nebude mít volná čočka žádný vliv na množství světla, které dorazí do vašeho oka, protože její orientace bude stejná jako orientace upevněné čočky. Pokud nyní otočíte volnou čočku o 90°, obraz úplně zčerná. V této konfiguraci je polarizace volné čočky kolmá na polarizaci upevněné čočky, takže každý foton, který se dostane skrz volnou čočku, je zablokován upevněnou čočkou. Pokud nyní otáčíte volnou čočkou o 45°, dosáhnete mezi-stupně, v němž se polovině fotonů, které projdou volnou čočkou, podaří dostat skrz čočku upevněnou.

Wiesnera napadlo použít polarizaci fotonů pro vytvoření dolarové bankovky, kterou by nešlo nikdy padělat. Navrhl, aby každá dolarová bankovka obsahovala 20 světelných pastí, malá zařízení, jež mohou zachytit a uchovat foton. Bankám doporučil, aby používaly čtyři polarizační filtry orientované ve čtyřech směrech I, <->, \, *d'* tak, že vyplní 20 světelných pastí sekvencí 20 polarizovaných fotonů, pro každou dolarovou bankovku jinou sekvencí. Například schéma 74 ukazuje bankovku s polarizační sekvencí *(\ $ i/*[1] *tf* <-> *$ $ \ $%*<-*+-> *S* *->■ \ *S* <-> *u? t* I). Na schématu jsou jednotlivé polarizace znázorněny, ve skutečnosti však nebudou vidět. Každá bankovka také ponese tradiční sériové číslo, které je v našem příkladu B2801695E. Banka, která bankovku vydává, rozpozná každou dolarovou bankovku podle její polarizační sekvence a natištěného sériového čísla, přičemž si povede seznam sériových čísel a odpovídajících polarizačních sekvencí.

Padělatel nyní musí čelit problému - nemůže pouze padělat dolarovou bankovku, která nese libovolné sériové číslo a náhodnou polarizační sekvenci ve světelných pastích, protože tyto páry se neobjeví na seznamu banky, takže vyjde najevo, že dolarová bankovka je falešná. Aby padělatel vytvořil účinný falzifikát, musí použít pravou bankovku jako vzorek, nějak změřit jejích 20 polarizací a potom



Obrázek 74: Kvantové peníze Stephena Wiesnera. Každá bankovka je unikátní díky svému sériovému číslu, které je vidět, a díky 20 světelným pastem, jejichž obsah je tajný. Světelné pasti obsahují fotony s různou polarizací. Banka ví, které sekvence polarizace odpovídají každému sériovému číslu, ale padělatel to neví.

vytvořit kopii dolarové bankovky tak, že okopíruje sériové číslo a naplní

světelné pasti odpovídajícím způsobem. Měření polarizace fotonu je však nechvalně proslulé jako komplikovaný úkol; pokud padělatel nedokáže na vzorové bankovce přesně změřit polarizace, potom nemůže doufat, že bankovku zfalšuje.

Abychom pochopili složitost měření polarizace fotonu, musíme vzít v úvahu, jak by se takové měření provádělo. Jediný způsob, jak se něco dozvědět o polarizaci fotonu, je použít polarizační filtr. Aby padělatel změřil polarizaci fotonu v konkrétní světelné pasti, vybere polarizační filtr a orientuje jej určitým směrem, řekněme svisle *t*-Pokud je foton, který vylétne ze světelné pasti, náhodou skutečně polarizovaný svisle, projde svislým polarizačním filtrem a padělatel správně usoudí, že jde o svisle polarizovaný foton. Pokud je příslušný foton polarizovaný vodorovně, svislým filtrem neprojde a padělatel správně usoudí, že jde o vodorovně polarizovaný foton. Ale pokud je foton náhodou polarizován úhlopříčně (\ nebo i/[1]), potom filtrem projít může a nemusí. V obou těchto případech padělatel v určení jeho pravé podstaty neuspěje. Foton \ může svislým polarizačním filtrem projít a padělatel bude mylně předpokládat, že jde o svisle polarizovaný foton. Anebo týž foton projít nemusí a v tomto případě se bude padělatel mylně domnívat, že to je foton polarizovaný vodorovně. Opačně platí, že pokud se padělatel rozhodne změřit fotony v další světelné pasti tím, že filtr nastaví úhlopříčně, řekněme \, potom správně určí povahu úhlopříčně polarizovaných fotonů, ale selže při přesném určení svisle nebo vodorovně polarizovaných fotonů.

Padělatelův problém spočívá v tom, že musí použít správně orientovaný polarizační filtr, aby určil polarizaci fotonu, ale neví, kterou orientaci použít, protože polarizaci fotonu nezná. Tato situace typu Hlava 22 je neodmyslitelnou součástí fyziky fotonů. Představte si, že padělatel vybere filtr s orientací \, aby změřil fotony v druhé světelné pasti, a foton filtrem neprojde. Padělatel si může být jist, že foton nebyl polarizován \, protože tento typ fotonu by filtrem prošel. Ale nemůže říci, zda byl foton polarizován *if, takže* filtrem určitě neprošel, nebo zda byl polarizován í či <-►, každý z nich by totiž měl šanci 50 : 50, že projde.

Nesnáze při měření fotonů jsou jedním aspektem principu neurčitosti, rozpracovaného ve 20. letech 20. století německým fyzikem Wernerem Heisenbergem, který přeložil svou vysoce odbornouformulaci do jednoduchého tvrzení: „Z principu nemůžeme poznat současnost ve všech jejích detailech." To neznamená, že nemůžeme vědět vše, protože nemáme dost měřicích zařízení nebo je naše zařízení špatně navrženo. Místo toho Heisenberg tvrdí, že je logicky nemožné změřit každý aspekt určitého předmětu s dokonalou přesností. V tomto konkrétním případě nemůžeme změřit každou vlastnost fotonu ve světelných pastích s dokonalou přesností. Princip neurčitosti je dalším těžko představitelným důsledkem kvantové teorie.

Princip Wiesnerových kvantových peněz vycházel ze skutečnosti, že padělání je dvoustupňový proces: padělatel nejdříve musí přesně změřit původní bankovku a potom ji replikovat. Tím, že Wiesner začlenil do dolarové bankovky fotony, zařídil, že bankovku není možné přesně změřit, a tudíž postavil padělatelům do cesty nepřekonatelnou překážku.

Naivní padělatel si může myslet, že pokud není schopen polarizaci fotonů ve

světelných pastech změřit on, nemůže to udělat ani banka. Třeba se pokusí vyrobit dolarovou bankovku s náhodnou sekvencí polarizací. Banka však dovede ověřit, která bankovka je pravá. Její pracovník se podívá na sériové číslo, potom nahlédne do tajného seznamu, aby zjistil, jaké fotony jsou obsaženy ve světelných pastech. Protože banka ví, které polarizace má očekávat v každé světelné pasti, může pro každou past správně nastavit polarizační filtr a provést přesné měření. Pokud je bankovka padělaná, padělatelova náhodná polarizace povede ke špatnému měření a bankovka bude vyřazena jako falzifikát. Jestliže chce banka například změřit foton s očekávanou polarizací I, použije stejně polarizovaný filtr. Zjistili však, že filtr foton blokuje, potom ví, že padělatel vyplnil past špatným fotonem. Ale pokud se bankovka ukáže být pravou, banka znovu vyplní světelné pasti odpovídajícími fotony a dá ji zpět do oběhu.

Krátce řečeno, padělatel nemůže změřit polarizaci v pravé bankovce, protože neví, jaký typ fotonu je v každé světelné pasti, a nemůže tedy vědět, jak orientovat polarizační filtr, aby foton správně změřil. Na druhou stranu je banka schopna ověřit polarizaci pravé bankovky, protože typ polarizace sama vybrala a ví tedy, jak polarizační filtr orientovat pro každou světelnou past.

Kvantové peníze jsou vynikající myšlenkou. Jsou také naprosto nerealizovatelné. Za prvé, inženýři *zatím* nevyvinuli technologii umožňující zachytit fotony v určitém polarizovaném stavu na dostatečně dlouhou dobu. I kdyby taková technologie existovala, bylo by příliš drahé ji implementovat. Ochrana jedné dolarové bankovky by přišla možná na milion dolarů. Přestože jsou kvantové peníze nepraktické, aplikují kvantovou teorii fascinujícím a vynalézavým způsobem, takže i přes nedostatek podpory svého profesora předložil Wiesner svou stať vědeckému časopisu. Byla odmítnuta. Nabídl ji dalším třem časopisům a byla třikrát odmítnuta. Wiesner tvrdí, že jeho fyzice jednoduše nebylo porozuměno.

Zdálo se, že existuje pouze jediná osoba, jež sdílí Wiesnerovo nadšení pro koncept kvantových peněz. Byl to jeho starý přítel Charles Bennett, který s ním kdysi studoval na Brandeis University. Ben-nettův zájem o všechno, co nějak souviselo s vědou, je jedním z nejpozoruhodnějších rysů jeho osobnosti. Sám říká, že již ve věku tří let věděl, že chce být vědcem, a jeho dětské nadšení pro věc nebylo lhostejné ani jeho matce. Jednoho dne se vrátila domů a našla na plotně bublající pánev s podivnou hmotou. Naštěstí ji nic nelákalo tu věc ochutnat - jak se později ukázalo, šlo o pozůstatky želvy, kterou malý Bennett vařil v louhu, aby oddělil maso od kostí a dostal tak dokonalý vzorek želví kostry. Během dospívání Bennettova zvědavost přešla od biologie k biochemii, a když se dostal na Brandeisovu univerzitu, rozhodl se specializovat se na fyzikální chemii. Potom pokračoval ve výzkumech ve fyzice, matematice, logice a nakonec v počítačové vědě.Wiesner doufal, že by díky svému širokému okruhu zájmů mohl právě Bennett ocenit kvantové peníze, a dal mu kopii svého zavrženého rukopisu. Bennett byl konceptem ihned fascinován a považoval jej za jednu z nejkrásnějších myšlenek, kterou kdy viděl. Během následujícího desetiletí občas rukopis pročítal a uvažoval, zda existuje způsob, jak změnit tak důmyslný nápad v něco, co by bylo uskutečnitelné. O Wiesnerově nápadu nepřestal přemýšlet ani jako výzkumník v

laboratořích Thomase J. Watsona společnosti IBM, kde v 80. letech pracoval. Časopisy nadále nechtěly příspěvek otisknout, ale Bennett jím byl jako posedlý.

Jednoho dne Bennett vysvětloval koncept kvantových peněz Gil-lesi Brassardovi, počítačovému vědci z montrealské univerzity. Bennett a Brassard, kteří spolupracovali na různých výzkumných projektech, začali do detailů rozebírat spletitosti Wiesnerovy stati. Postupně začali chápat, že Wiesnerovu myšlenku lze aplikovat v kryptografii. Aby Eva rozluštila zašifrovanou zprávu mezi Alicí a Bobem, musí ji nejdříve zachytit, což znamená, že musí nějakým způsobem přesně rozpoznat obsah vysílání. Wiesnerovy kvantové peníze byly bezpečné, protože bylo nemožné přesně zachytit polarizaci fotonů uvězněných v dolarové bankovce. Bennett a Brassard uvažovali, co by se stalo, kdyby zašifrovaná zpráva byla zastupována a přenášena sledem polarizovaných fotonů. Zdálo se jim, že Eva by nebyla schopna přesně číst zašifrovanou zprávu, a pokud by ji nemohla přečíst, nemohla by ji dešifrovat.

Bennett a Brassard začali vymýšlet systém založený na následujícím principu: představte si, že Alice chce Bobovi poslat zašifrovanou zprávu, která se skládá ze sledu jedniček a nul. Nahradí 1 a 0 emisí fotonů s určitou polarizací. Alice má dvě možná schémata pro spojení polarizace fotonů s 1 nebo 0. V prvním schématu, nazvaném *rovnoběžné* neboli plus-schéma, posílá foton s polarizací I jako zástupce 1 a foton s polarizací «-> jako zástupce 0. V druhém schématu, nazvaném *diagonální neboli* x-schéma, posílá *if* jako reprezentaci 1 a \ místo 0. Při odesílání binární zprávy přepíná Alice mezi těmito dvěma schématy nepředvídatelným způsobem. Binární zpráva 1101101001 může být vyslána následujícím způsobem:

Zpráva	1	1	0	1	1	0	1	0	0	1
Schéma	+	×	+	×	×	×	+	+	×	×
Přenos	↕	↗	↔	↗	↗	↘	↕	↔	↘	↗

Alice vyšle první 1 pomocí plus-schématu, druhou 1 pomocí x-schématu. Jednička je pak pokaždé představována různě polarizovanými fotony.

Když chce Eva tuto zprávu zachytit, potřebuje rozpoznat polarizaci každého fotonu, stejně jako padělatel potřebuje rozpoznat polarizaci každého fotonu ve světelných pastech dolarové bankovky. Chce-li změřit polarizaci každého fotonu, musí se Eva pokaždé rozhodnout, jak orientovat svůj polarizační filtr. Nemůže vědět, které schéma Alice použila pro jednotlivé fotony, takže její volba polarizačního filtru bude náhodná a v polovině případů mylná. Proto nemůže zachytit celou zprávu.

Jednodušší způsob, jak přemýšlet o Evině dilematu, je předpokládat, že má k dispozici dva typy polarizačních detektorů. Plus-detektor dovede měřit vodorovně a svisle polarizované fotony s dokonalou přesností, ale není schopen měřit fotony úhlopříčně polarizované, navíc je nesprávně interpretuje jako svisle nebo vodorovně polarizované. Naopak x-detektor přesně změří úhlopříčně polarizované fotony, nikoli však fotony polarizované vodorovně a svisle, ty mylně interpretuje jako částice polarizované úhlopříčně. Pokud Eva například použije x-detektor pro měření prvního fotonu, který je *t*, bude jej mylně interpretovat jako *if* nebo \. Pokud jej mylně interpretuje jako $i^{/1}$, pak vlastně nemá problém, protože tato polarizace

také představuje jedničku, pokud jej však mylně interpretuje jako N, potom má smůlu, protože symbol představuje 0. Aby to Eva měla ještě horší, má pouze jednu příležitost k měření. Foton je nedělitelný, nemůže jej rozdělit ve dva fotony a změřit jej podle obou schémat.

Tento systém má zřetelné výhody. Eva si nemůže být jista, že zachytila zašifrovanou zprávu přesně, takže nemá naději na její dešifrování. Systém však také trpí vážnými a na první pohled nepřekonatelnými problémy - Bob je ve stejné situaci jako Eva, protože nerozezná, které polarizační schéma Alice používá pro jednotlivý foton, takže zprávu špatně interpretuje i on. Evidentní řešení problému spočívá v tom, že se Alice a Bob domluví, jaké polarizační schéma pro jednotlivé fotony zavedou. V předchozím příkladě by Alice a Bob sdíleli seznam nebo klíč, který obsahuje + x + xxx + + xx. To jsme však zpět u starého problému distribuce klíčů - Alice musí nějakým bezpečným způsobem dopravit seznam polarizačních schémat k Bobovi.Samozřejmě by Alice mohla zašifrovat seznam schémat pomocí šifry veřejného klíče jako třeba RSA a potom jej poslat Bobovi. Ale představte si, že již žijeme v době, kdy je RSA prolomena, patrně díky rozvoji kvantových počítačů. Bennettův a Brassardův systém musí být soběstačný a nesmí se spoléhat na RSA. Po měsíce se Ben-nett a Brassard snažili vymyslet způsob, jak obejít problém distribuce klíčů. Potom v roce 1984 stáli na nástupišti stanice Croton-Harmon, blízko výzkumného střediska společnosti IBM. Cekali na vlak, který odveze Brassarda zpět do Montrealu, a krátili si čas povídáním o potížích Alice, Boba a Evy. Kdyby vlak přijel o několik minut dříve, zamávali by si na rozloučenou a s problémem distribuce klíčů by se nedostali ani o krok dále. Namísto toho vytvořili v náhlém okamžiku osvícení kvantovou kryptografii, nejbezpečnější formu komunikace, která kdy byla navržena.

Návod na kvantovou kryptografii vyžaduje tři přípravné etapy. Přestože tato stadia nezahrnují zaslání šifrované zprávy, umožňují bezpečnou výměnu klíče, který může být později použit k zašifrování zprávy.

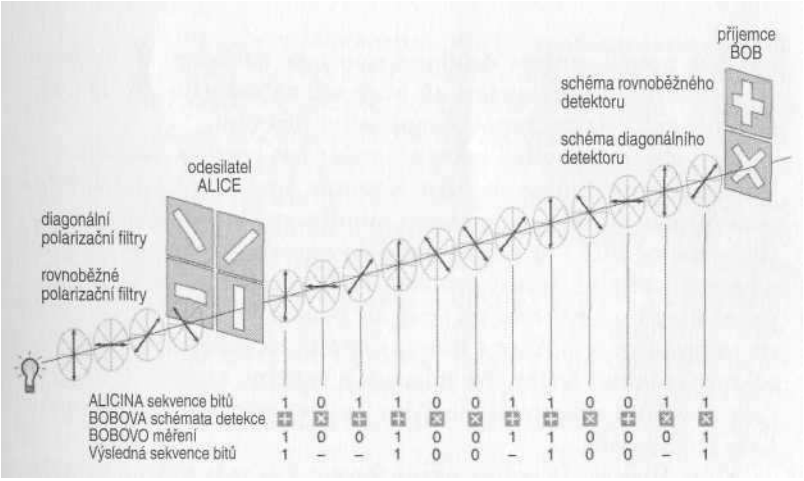
Etapa 1. Alice začne vysíláním náhodné sekvence jedniček a nul (bitů), přičemž používá náhodný výběr rovnoběžných (tj. vodorovných a svislých) a úhlopříčných polarizačních schémat. Obrázek 76 ukazuje takovou sekvenci fotonů, která míří k Bobovi.

Etapa 2. Bob změří polarizaci těchto fotonů. Vzhledem k tomu, že nemá představu, jaká polarizační schémata Alice pro každý foton použila, náhodně střídá svůj plus-detektor a x-detektor. Někdy Bob vybere správný detektor, jindy špatný. Pokud Bob sáhne po špatném detektoru, může Alicin foton interpretovat mylně. Tabulka 27 pokrývá všechny možnosti. Například v prvním řádku použila Alice rovnoběžné schéma k zaslání jedničky, a vyslala tedy *t,* potom použil Bob správný detektor, zjistil I, a proto správně zapíše 1 jako první bit sekvence. V dalším řádku Alice udělá totéž, ale Bob použije nesprávný detektor, takže zaznamená i/[1] nebo S, což znamená, že buď zapíše správně 1, nebo špatně 0.

Etapa 3. Dosud jsme si řekli, že Alice poslala sérii 1 a 0, Bob některé z nich identifikoval správně a některé špatně. Aby se situace vyjasnila, Alice zatelefonuje Bobovi běžnou nezabezpečenou

linkou a řekne mu, která polarizační schémata použila pro který foton - ne však, jak jednotlivé fotony polarizovala. Takže Bobovi například sdělí, že první vyslaný foton obsahuje rovnoběžné schéma, ale neprozradí, zda zvolila í nebo <->. Bob potom Alici řekne, u kterých fotonů uhodl správné polarizační schéma. V těchto případech totiž s jistotou změřil správnou polarizaci a správně zapsal 1 nebo 0. Alice a Bob nadále neberou na vědomí ty fotony, pro něž Bob použil nesprávné schéma, a soustředí se pouze na ty, které určil správně. Tím vytvoří novou, kratší sekvenci bitů, skládající se pouze z Bobových správných měření. Tato etapa je ilustrována tabulkou v dolní části obrázku 76.

Tyto tři etapy umožnily Alici a Bobovi vytvořit společnou sadu číslic, jako je třeba sekvence 11001001 dohodnutá na obrázku 76. *Zásadní* vlastností této sekvence je její nahodilost, protože je odvozena z Aliciny původní sekvence, která byla také náhodná. Případy,



Obrázek 76: Alice vysílá sérii jedniček a nul Bobovi. Každou 1 a každou 0 reprezentuje polarizovaný foton, a to buď podle rovnoběžného, nebo úhlopříčného polarizačního schématu. Bob změří každý foton pomocí jednoho ze svých polarizačních detektorů, a to bud rovnoběžného, nebo úhlopříčného. Zvolí správný detektor pro foton, který stojí první zleva, a správně jej interpretuje jako 1, Pro další foton vybere nesprávný detektor. Náhodou jej určí správně jako 0, ale tento bit je přesto později odložen, protože si Bob nemůže být jist, zda jej změřil

Alicino schéma	Aliciny bity	Alice posílá	Bobův detektor	Správný detektor?	Bob detekuje	Bobovy bity	Má Bob pravdu?
Rovnoběžné	1	↕	+	ano	↕	1	ano
			×	ne	↙	1	ano
					↘	0	ne
	0	↔	+	ano	↔	0	ano
			×	ne	↙	1	ne
					↘	0	ano
Diagonální	1	↙	+	ne	↕	1	ano
					↔	0	ne
			×	ano	↙	1	ano
	0	↘	+	ne	↕	1	ne
					↔	0	ano
			×	ano	↘	0	ano

správně.

Tabulka 27: Různé možnosti v 2. etapě výměny fotonů mezi Alicí a Bobem.

kdy Bob použil správný detektor, jsou také náhodné. Dohodnutá sekvence tedy netvoří zprávu, ale hraje roli náhodného klíče. Konečně může začít vlastní proces bezpečného šifrování.

Dohodnutá náhodná sekvence může být použita jako klíč pro jednorázovou tabulkovou šifru. Kapitola 3 popisuje, jak náhodná série písmen a čísel - jednorázová tabulka, může dát vzniknout ne-rozluštitelné šifře - ne pouze prakticky nerozluštitelné, ale absolutně nerozluštitelné. Jediný problém s takovou šifrou spočíval v bezpečné distribuci náhodných sérií, ale Bennettův a Brassardův plán tento problém řeší. Alice a Bob se dohodli na jednorázové tabulce, zákony kvantové fyziky Evě zakazují ji úspěšně zachytit. Teď je na čase, abychom se postavili do Eviny pozice a podívali se, proč nedokáže klíč zachytit.

Když Alice vysílá polarizované fotony, Eva se je pokouší změřit, ale neví, zda použít plus-detektor nebo x-detektor. V polovině případů zvolí špatný detektor. To je stejná pozice, ve které je Bob, protože také on v polovině případů vybere špatný detektor. Avšak po vysílání řekne Alice Bobovi, které schéma odpovídá jednotlivým fotonům, a dohodnou se, že použijí pouze fotony, které Bob změřil správným detektorem. To Evě nepomůže, protože polovinu těchto

fotonů změřila nesprávným detektorem, a tedy mylně interpretovala některé z fotonů, které tvoří konečný klíč.

Jiný způsob, jak přemýšlet o kvantové kryptografii, spočívá v přirovnání k balíčku karet. Každá hrací karta má hodnotu a barvu, jako třeba srdcový spodek nebo křížová šestka. Obvykle se na kartu podíváme a vidíme hodnotu i barvu zároveň. Představte si však, že je možné zjistit pouze hodnotu nebo barvu, ale ne oboje najednou. Alice vybere kartu z balíčku a musí se rozhodnout, zda změří hodnotu nebo barvu. Předpokládejme, že si vybere barvu, což jsou piky. Karta je piková čtyřka, ale Alice ví pouze to, že to jsou piky. Potom vyšle kartu telefonní

linkou Bobovi. Zatímco se toto odehrává, Eva se snaží určit kartu, ale zvolí její hodnotu, což je čtyřka. Když se karta dostane k Bobovi, rozhodne se, že změří její barvu, což jsou stále piky, a zapíše ji. Potom Alice Bobovi zavolá a zeptá se, zda změřil barvu, což opravdu udělal, takže Alice a Bob nyní vědí, že sdílejí společnou vědomost - ve svých blocích mají oba napsáno „piky". Ale Eva má zapsáno „čtyřka", což jí k ničemu není.

Potom Alice vybere další kartu z balíčku, řekněme kárového krále, ale znovu může správně změřit pouze jednu vlastnost. Tentokrát se rozhodne zjistit její hodnotu, což je král, a vyšle kartu telefonní linkou k Bobovi. Eva se snaží kartu odkrýt a také zvolí její hodnotu, tedy „krále". Když se karta dostane k Bobovi, rozhodne se změřit její barvu, což jsou kára. Potom Alice zavolá Bobovi a *zemitá*, se, zda zjistil hodnotu karty. Bob musí přiznat, že hádal špatně a změřil její barvu. Alici a Boba to netrápí, protože mohou tuto kartu naprosto ignorovat a znovu vyzkoušet další náhodně vybranou kartu z balíčku. V druhém případě Eva hádala správně a změřila totéž co Alice, tedy „krále", ale karta byla odložena, protože ji Bob nezměřil správně. Takže se Bob nemusí znepokojovat svými chybami, protože se s Alicí dohodli, že je budou ignorovat, ale Eva se svých chyb chtě nechtě drží. Alice a Bob se zasláním několika karet dohodnou na sekvenci barev a hodnot, které potom použijí jako základ pro nějaký druh klíče.

Kvantová kryptografie umožňuje Alici a Bobovi dohodu o klíči, který Eva nemůže zachytit bez chyb. Navíc má kvantová kryptografie dodatečnou výhodu: poskytuje Alici a Bobovi způsob, jak zjistit, zda Eva naslouchá. Evina přítomnost na lince se stává zjevnou, protože pokaždé, když změří foton, riskuje, že jej změní, a tak se prozradí.Představte si, že Alice pošle ** a Eva jej změří špatným detektorem - plus-detektorem. Ten donutí přicházející ** foton, aby se změnil na *t* nebo *-* foton, protože jen v této podobě se foton může dostat přes Evin detektor. Když Bob změří transformovaný foton svým x-detektorem, identifikuje buď ** (což je varianta, kterou Alice poslala), nebo může zjistit i/[1]. To je pro Alici a Boba problém, protože Alice poslala úhlopříčně polarizovaný foton a Bob použil správný detektor, ale přesto změřil foton špatně. Krátce řečeno, když Eva zvolí špatný detektor, „otočí" některé fotony a to zapříčiní, že se na Bobově straně projeví chyby, i když užije správný detektor. Tyto chyby lze odhalit, pokud Alice a Bob provedou speciální kontrolní

proceduru.

Zjišťování chyb se provede po úvodních etapách, tedy ve chvíli, kdy Alice a Bob mají mít k dispozici shodnou sekvenci jedniček a nul. Představte si, že získali sekvenci, která má na délku 1 075 binárních čísel. Jeden ze způsobů, jak Alice a Bob zjistí, zda si jejich sekvence odpovídají, může být ten, že Alice Bobovi zavolá a přečte mu celou svou sekvenci. Pokud však Eva poslouchá, zachytí celý klíč. Prověření celé sekvence je očividně nerozumné, a navíc není ani nezbytné. Místo toho Alice pouze náhodně vybere 75 číslic, které ověří. Pokud Bob těchto 75 číslic odsouhlasí, je velmi nepravděpodobné, že by Eva tajně naslouchala během původního vysílání fotonů. Pravděpodobnost toho, že Eva byla na lince a nezměnila Bobovo měření žádné z těchto 75 číslic, je menší než jedna k milionu.

Protože o těchto 75 číslicích Bob a Alice otevřeně mluvili, je třeba je odložit, jednorázová tabulka se tedy redukuje z 1 075 na 1 000 binárních číslic. Pokud však Alice a Bob naleznou v těchto 75 číslicích rozpor, poznají, že Eva naslouchala. Pak nezbývá, než opustit celou jednorázovou tabulku, přepnout se na jinou linku

a začít znovu.

Stručně shrnuto, kvantová kryptografie je systém, který zaručuje bezpečnost zpráv tím, že maximálně ztěžuje Evě správné čtení komunikace mezi Alicí a Bobem. Navíc, pokud se Eva pokouší naslouchat, mohou Alice a Bob zjistit její přítomnost. Kvantová kryptografie tudíž umožňuje Alici a Bobovi dohodnout se na jednorázové tabulce v naprostém soukromí, takže ji pak mohou používat jako klíč pro šifrování zpráv. Postup má pět základních kroků:

(1) Alice pošle Bobovi sérii fotonů a Bob je změří.

(2) Alice řekne Bobovi, které z nich změřil správně. (Přestože Alice říká Bobovi, kdy provedl správné měření, nesdělí mu, jaký je správný výsledek, takže tato konverzace může být odposlouchávána bez snížení bezpečnosti postupu.)

(3) Alice a Bob ignorují měření, která Bob provedl nesprávně, a soustředí se na správná měření, aby vytvořili shodnou dvojici jednorázových tabulek.

(4) Alice a Bob ověří shodu svých jednorázových tabulek tak, že otestují několik číslic.

(5) Pokud je ověřovací procedura uspokojivá, použijí jednorázovou tabulku k zašifrování zprávy; pokud ověření odhalí chyby, potom vědí, že Eva fotony zachytila, a musí začít vše od začátku.

Čtrnáct let poté, co vědecké časopisy odmítly Wiesnerovu stať, inspirovala naprosto bezpečný komunikační systém. Wiesner, který nyní žije v Izraeli, je rád, že byla jeho práce nakonec uznána: „Když se dívám nazpět, přemýšlím, zda jsem nemohl dokázat více. Někteří lidé mi řekli, že jsem předčasně hodil flintu do žita, protože jsem se více nesnažil, aby moje myšlenka byla publikována - myslím, že svým způsobem mají pravdu, ale já jsem byl tehdy mladý absolvent a neměl jsem tolik sebevědomí. V každém případě, o kvantové peníze nikdo nejevil zájem."

Kryptografové uvítali Bennettovu a Brassardovu kvantovou kryptografii s nadšením. Ale mnoho experimentátorů okamžitě došlo k závěru, že tento systém funguje sice dobře teoreticky, ale neuspěje v praxi. Domnívali se, že obtíže v práci s jednotlivými fotony znemožní implementaci systému. I přes tuto kritiku byli Bennett a Brassard přesvědčeni, že kvantová kryptografie fungovat může. Měli ve svůj systém takovou důvěru, že se ani neobtěžovali s konstrukcí přístroje. Jak jednou Bennett řekl: „Nemá smysl chodit na severní pól, když víte, že tam je."

Růst všeobecné skepse však nakonec Bennetta přiměl k tomu, aby dokázal, že systém může skutečně pracovat. V roce 1988 začal shromažďovat součástky, které potřeboval pro systém kvantové kryptografie, a zaměstnal postgraduálního studenta Johna Smolina, aby mu pomohl přístroj sestavit. Po roce úsilí byli připraveni pokusit se o přenos vůbec první zprávy chráněné kvantovou kryptografií. Pozdě večer se zavřeli ve světlotěsné laboratoři, v prostředíčerném jako noc, zajištěném proti zatoulaným fotonům, které by mohly experiment ovlivnit. Po chutné večeři byli dobře připraveni na dlouhou noc zápolení s

přístrojem. Vytyčili si úkol poslat polarizované fotony přes místnost a potom je změřit pomocí plus-de-tektoru a x-detektoru. Počítač jménem Alice řídil vysílání fotonů a počítač jménem Bob rozhodoval, který detektor změří každý jednotlivý foton.

Po hodinách vylepšování, kolem třetí hodiny ranní, se Bennett stal svědkem první výměny zpráv v kvantové kryptografii. Alice a Bob dokázali poslat a přijmout fotony, potom projednat polarizační schémata, která Alice zvolila, vyřadit fotony, které Bob změřil špatným detektorem, a dohodnout se na jednorázové tabulce, jež sestávala ze zbývajících fotonů. „Nikdy nebylo pochyb, že bude fungovat," vzpomíná Bennett, „nevěděli jsme pouze, zda naše prsty budou dost obratné, aby to dokázaly." Bennettův pokus prokázal, že dva počítače - Alice a Bob - mohou komunikovat v naprostém bezpečí. Byl to historický pokus, navzdory faktu, že oba počítače byly od sebe vzdáleny pouhých 30 cm.

Po Bennettově pokusu bylo úkolem sestavit systém kvantové kryptografie, který by fungoval i na skutečně významnou vzdálenost. To není banální úkol, protože fotonům nedělá cestování dobře. Pokud Alice vysílá vzduchem foton s určitou polarizací, molekuly vzduchu s ním budou interagovat, měnit jeho polarizaci, což nelze připustit. Výkonnějším médiem pro přenášení fotonů je optické vlákno. Vědci nedávno úspěšně využili této techniky k sestavení systému kvantové kryptografie, který pracuje na významnou vzdálenost. V roce 1995 implementovali výzkumníci ženevské univerzity kvantovou kryptografii do optického vlákna spojujícího na vzdálenost 23 km Zenevu s městem Nyon.

O něco později skupina vědců z Los Alamos National Laborato-ry v Novém Mexiku začala znovu experimentovat s kvantovou kryptografií ve vzduchu. Jejich konečným cílem je vytvořit systém kvantové kryptografie, který by mohl fungovat přes satelity. Pokud by toho dosáhli, systém by zajistil naprosto bezpečnou globální komunikaci. Dosud se skupině z Los Alamos podařilo přenést kvantový klíč vzduchem na vzdálenost 1 km.

Bezpečnostní experti nyní přemýšlejí nad tím, jak dlouho bude trvat, než se kvantová kryptografie stane praktickou technologií. Dnes nepředstavuje žádnou dodatečnou výhodu, protože RSA

nám již dává přístup k prakticky nerozlomitelnému šifrování. Pokud by se však kvantové počítače staly realitou, pak by RSA a všechny další moderní šifry byly nepoužitelné a kvantová kryptografie by se stala nezbytností. Takže závod pokračuje. Skutečně důležitá otázka zní, zda kvantová kryptografie dorazí včas, aby nás zachránila před hrozbou kvantových počítačů, nebo zda nastane absence soukromí, období mezi rozvojem kvantových počítačů a příchodem kvantové kryptografie. Zatím

je pokročilejší technologií kvantová kryptografie. Švýcarský pokus s optickým vláknem dokazuje, že by bylo proveditelné vybudovat systém, který by umožňoval bezpečnou komunikaci mezi finančními institucemi v jednom městě. V současnosti je již možné postavit pomocí kvantové kryptografie spojení mezi Bílým domem a Pentagonem. Možná už postaveno bylo.

Kvantová kryptografie by znamenala konec bitvy mezi tvůrci a luštiteli kódů, tvůrci kódů by z ní vyšli jako vítězové. Kvantová kryptografie je nerozlomitelný systém šifrování. Může to vypadat jako velmi přehnané tvrzení, zvláště ve světle předchozích podobných prohlášení. V různých dobách během posledních dvou tisíc let se kryptografové domnívali, že monoalfabetická šifra, polyalfa-betická šifra a šifrovací přístroje jako Enigma jsou nerozlomitel-né. V každém z těchto případů se nakonec prokázalo, že se kryptografové mýlili, protože jejich tvrzení byla založena pouze na faktu, že složitost šifer v určitém dějinném okamžiku předehnala vynalézavost a technologii kryptoanalytiků. Při zpětném pohledu vidíme, že kryptoanalytici nakonec nevyhnutelně dají dohromady způsob, jak prolomit každou šifru, nebo rozvinou technologii, která ji prolomí za ně.

Tvrzení, že kvantová kryptografie je bezpečná, je však kvalitativně odlišné od všech předchozích. Kvantová kryptografie není pouze prakticky nerozlomitelná, je nerozlomitelná naprosto. Kvantová teorie, nejúspěšnější teorie v historii fyziky, znamená, že Eva nemůže jednorázovou tabulku vytvořenou Alicí a Bobem správně zachytit. Eva se dokonce nemůže ani pokusit zachytit tabulku, aniž by Alice a Bob nebyli varováni. Pokud by se někdy podařilo dešifrovat zprávu chráněnou kvantovou kryptografií, znamenalo by to, že je kvantová teorie mylná, což by mělo pro fyziky drtivé důsledky; byli by nuceni znovu zvážit svůj pohled na fungování vesmíru na jeho nejzákladnější úrovni.Pokud se podaří sestrojit systémy kvantové kryptografie fungující na velké vzdálenosti, vývoj v jedné oblasti šifer bude završen. Hledání soukromí se přiblíží ke svému konci. Technologie by byla schopná zajistit bezpečnou komunikaci pro vlády, armády, obchodníky a veřejnost. Zůstává jediná otázka: Dovolily by nám vlády používat tuto technologii? Jak budou vlády regulovat kvantovou kryptografii, aby obohatily informační věk, a zároveň nechránily zločince?

Dešifrovací soutěž

Dešifrovací soutěž je soubor deseti šifrových zpráv, které jsem umístil na závěr této knihy, když byla poprvé vydána v roce 1999. Kromě intelektuální odměny byla za dešifrování všech deseti zpráv vypsána cena 10 000 liber pro první osobu, která soutěž vyřeší. *Výzva*, byla nakonec vyřešena 7. října 2000, po jednom roce a jednom měsíci namáhavého úsilí luštitelů kódů, amatérů i profesionálů z celého světa.

Dešifrovací soutěž přesto zůstává součástí i českého vydání. S vyřešením už není spojena cena, ale rád bych pobídl čtenáře, aby alespoň některé zprávy rozluštili. Deset stupňů by mělo mít rostoucí obtížnost, ačkoli mnoho luštitelů mělo pocit, že stupeň 3 je těžší než stupeň 4. Šifry se v jednotlivých stadiích liší a vyvíjejí dle vývoje šifrovacích technik v průběhu staletí, takže rané šifry jsou staré a snadné na rozlomení, zatímco pozdější stadia používají moderní šifry a vyžadují mnohem více úsilí. Krátce řečeno, úlohy 1 až 4 jsou pro amatéry, úlohy 5 až 8 pro skutečné nadšence a úloha 9 a 10 je určena opravdovým luštitelům kódů.

Pokud chcete o dešifrovací soutěži (Cipher Challenge) vědět více, můžete navštívit mou webovou stránku (www.simonsingh.net), jež *nabízí* pestrý výběr informací včetně odkazu na esej, který napsali výherci dešifrovací soutěže. Esej je vynikajícím čtením, buďte si však vědomi, že obsahuje - stejně jako další materiály na webové stránce - nápovědy, které možná ještě nechcete znát.

Hlavním cílem dešifrovací soutěže je nadchnout lidi, zaujmout je pro kryptografii a rozlamování kódů. Fakt, že tisíce lidí výzvu přijaly, je vysoce uspokojivý. Oficiálně dešifrovací soutěž skončila, ale doufám, že bude nadále vzbuzovat zájem mezi novými čtenáři, kteří si chtějí otestovat své schopnosti v rozlamování kódů.

Hodně štěstí.

Simon Singh

Úloha 1: Jednoduchá monoalfabetická substituční šifra

BT JPX RMLX PCUV AMLX ICVJP IBTWXVR CI M LMT' R PMTN, MTN YVCJX CDXV MWMBTRJ JPX AMTNGXRJBAH UQCT JPX QGMRJXV CI JPX YMGG CI JPX HBTWR QMGMAX; MTN JPX HBTW RMY JPX QMVJ CI JPX PMTN JPMJ YVCJX. JPXT JPX HBTWR ACUTJXTMTAX YMR APMTWXN, MTN PBR JPCUWPJR JVCUFGXN PBL, RC JPMJ JPX SCBTJR CI PBR GCBTR YXVX GCCRXN, MTN PBR HTXXR RLCJX CTX MWMBTRJ MTCJPXV. JPX HBTW AVBXN MGCUN JC FVBTW BT JPX MRJVCGCWXVR, JPX APMGNXMTR, MTN JPX RCCJPRMEXVR. MTN JPX HBTW RQMHX, MTN RMBN JC JPX YBRX LXT CI FMFEGCT, YPCRCXDXV RPMGG VXMN JPBR YVBJBTW, MTN RPCY LX JPX BTJXVQVXJMJBCT JPXVXCI, RPMGG FX AGCJPXN YBJP RAMVGXJ, MTN PMDX M APMBT CI WCGN MFCUJ PBR TXAH, MTN RPMGG FX JPX JPBVN VUGXV BT JPX HBTWNCL. JPXT AMLX BT MGG JPX HBTWR YBRX LXT; FUJ JPXE ACUGN TCJ VXMN JPX YVBJBTW, TCV LMHX HTCYT JC JPX HBTW JPX BTJXVQVXJMJBCT JPXVXCI. JPXT YMR HBTW FXGRPMOOMV WVXMJGE JVCUFGXN, MTN PBR ACUTJXTMTAX YMR APMTWXN BT PBL, MTN PBR GCVNR YXVX MRJCTBRPXN. TCY JPX KUXXT, FE VXMRCT CI JPX YCVNR CI JPX HBTW MTN PBR GCVNR, AMLX BTJC JPX FMTKUXJ PCURX; MTN JPX KUXXT RQMHX MTN RMBN, C HBTW, GBDX ICVXDXV; GXJ TCJ JPE JPCUWPJR JVCUFGX JPXX, TCV GXJ JPE ACUTJXTMTAX FX APMTWXN; JPXVX BR M LMT BT JPE HBTWNCL, BT YPCL BR JPX RQBVBJ CI JPX PCGE WCNR; MTN BT JPX NMER CI JPE IMJPXV GBWPJ MTN UTNXVRJMTNBTW MTN YBRNCL, GBHX JPX YBRNCL CI JPX WCNR, YMR ICUTN BT PBL; YPCL JPX HBTW TXFUAPMNTXOOMV JPE IMJPXV, JPX HBTW, B RME, JPE IMJPXV, LMNX LMRJXV CI JPX LMWBABMTR, MRJVCGCWXVR, APMGNXMTR, MTN RCCJPRMEXVR; ICVMRLUAP MR MT XZAXGGXTJ RQBVBJ, MTN HTCYGXNWX, MTN UTNXVRJMTNBTW, BTJXVQVXJBTW CI NVXMLR, MTN RPCYBTW CI PMVN RXTJXTAXR, MTN NBRRCGDBTW CI NCUFJR, YXVX ICUTN BT JPX RMLX NMTBXG, YPCL JPX HBTW TMLXN FXG JXRPMOOMV; TCY GXJ NMTBXG FX AMGGXN, MTN PX YBGG RPCY JPX BTJXVQVXJMJBCT. JPX IBVRJ ACNXYCVN BR CJPXGGC.

Úloha 2: Caesarova posunová šifra

MHILY LZA ZBHL XBPZXBL MVYABUHL HWWPBZ JSHBKPBZ JHLJBZ KPJABT HYJHUBT LZA ULBAYVU

Úloha 3: Monoalfabetická homofonní šifra

IXDVMUFXLFEEFXSOQXYQVXSQTUIXWF*FMXYQVFJ*FXEFQUQXJFPTUFX
MX*ISSFLQTUQXMXRPQEUMXUMTUIXYFSSFI*MXKFJF*FMXLQXTIEUVFX
EQTEFXSOQXLQ*XVFWMTQTUQXTITXKIJ*FMUQXTQJMVX*QEYQVFQTHMX
LFVQUVIXM*XEI*XLQ*XWITLIXEQTHGXJQTUQXSITEFLQVGUQX*GXKIE
UVGXEQWQTHGXDGUFXTITXDIEUQXGXKFKQVXSIWQXAVPUFXWGXYQVXEQ
JPFVXKFVUPUQXQXSGTIESQTHGX*FXWFQFXSIWYGJTFXDQSFIXEFXGJP
UFXSITXRPQEUGXIVGHFITXYFSSFI*CXC*XSCWWFTIXSOQXCXYQTCXYI
ESFCX*FXCKVQFXVFUQTPUFXQXKI*UCXTIEUVCXYIYYCXTQ*XWCUUFTI
XLQFXVQWFXDCSQWWIXC*FXC*XDI**QXKI*IXEQWYVQXCSRPFEUCTLIX
LC*X*CUIXWCTSFTIXUPUUQX*QXEUQ**QXJFCXLQX*C*UVIXYI*IXKQL
QCX*CXTIUUQXQX*XTIEUVIXUCTUIXACEEIXSOQXTITXEPVJQCXDPIVX
LQ*XWCVFTXEPI*IXSFTRPQXKI*UQXVCSSQEIXQXUCTUIXSCEEIX*IX*
PWQXQVZXLFXEIUUIXLZX*ZX*PTZXYIFXSOQXTUVZUFXQVZKZWXTQX*Z
*UIXYZEEIRPZTLIXTZYYZVKQXPTZXWITUZJTZXAVPTZXYQVX*ZXLFEU
ZTHZXQXYZVKQWFXZ*UZXUZTUIXRPZTUIXKQLPUZXTITXZKQZXZ*SPTZ
XTIFXSFXZ**QJVNWWIXQXUIEUIXUIVTIXFTXYFNTUIXSOQXLQX*NXTI
KNXUQVVNXPTXUPVAIXTNSRPQXQXYQVSIEEQXLQ*X*QJTIXF*XYVFWIX
SNTUIXUVQXKI*UQXF*XDQXJFVBVXSITXUPUUQX*BSRPQXBX*BXRPBVU
BX*QKBVX*BXYIYYBXFTXEPEIXQX*BXYVIVBXFVQXFTXJFPXSIWB*UVP
FXYFBSRPQFTDFTXSOQX*XWBVXDPXEIYVBXTIFXVFSOFPEIXX*BXYBVI
*BXFTXSILFSQXQXQRPBUIV**Úloha 4: Vigeněrova šifra**

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJB
GWRLFNFGHUDWUUMBSVLPSNCMUEKQCTESWR EEKOYSSIWCTUAXYOTAP X P
LWPNTCGOJBGFQ HTDWXIZAYGFFNSXCSEYNCTSSPNTUJNYTGG
WZGRWUUNEJUUQEAPYMEKQHUIDUXFPGUYTS MTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFB
DJQCUSWVBPNLGOYLSKMTEFVJJTWWMFMWPN MEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKC
PJRGPMURSKHFRSEIUEVGOYCWXIZAYGOSAA NYDOEOYJLWUNHAMEBFELXYVLWNOJNSIOFR
WUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUD EKQHCEUCPFCMPVSUDGAVEMNYMAMVLFMAOY
FNTQCUAFVFJNXKLNEIWCWODCCULWRIFTWG MUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNL
GFBTWOJFTWGNTEJKNEEDCLDHWTVBUVGFBI JGYYIDGMVRDGMPLSWGJLAGOEEKJOFEKNYN
OLRIVRWVUHEIWUURWGMUTJCDBNKGMBIDGM EEYGUOTDGGQEUJYOTVGGBRUJYS

Úloha 5

109 182 6 11 88 214 74 77 153 177 109 195 76 37 188
166 188 73 109 158 15 208 42 5 217 78 209 147 9 81 80 169 109
22 96 169 3 29 214 215 9 198 77 112 8 30 117 124 86 96 73 177
50 161

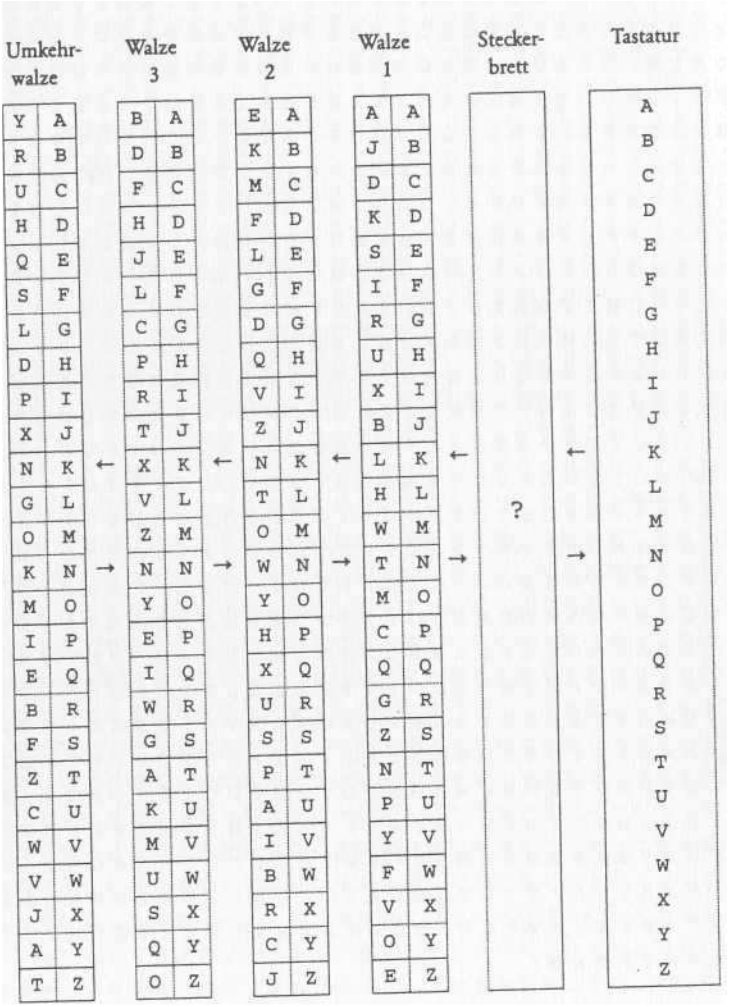
Úloha 6

OCOYFOLBVNPIASAKOPVYGESKOVMUFGUWMLNOOEDRNCFORSOCVMTUUTY
ERPFOLBVNPIASAKOPVIVKYEOCNKOCCARICVVLTSOCOYTRFDVCVOOUEG
KPVOOYN/KTHZSCVMBTWTRHPNKLRCUEGMSLNVLZSCANSCKOPORMZCKIZU
SLCCVFDLVORTHZSCLEGOXMIFOLBIMVIVKIUAYVUUFVWVCCBOVOVPFRH
CACSFGEOLCKMOCGEUMOHUEBRLXRHEMHPBMPLTVOEDRNCFORSGISTHOG
ILCVAIOAMVZIRRLNIIWUSGEWSRHCAUGIMFORSKVZMGCLBCGDRNKCVCP
YUXLOKFYFOLBVCCKDOKUUHAVOCOCLCIUSYCRGUFHBEVKROICSVPFTUQ
UMKIGPECEMGCGPGGMOQUSYEFVGFHRALAUQOLEVKROEOKMUQIRXCCBCV
MAODCLANOYNKBMVSMVCNVROEDRNCGESKYSYSLUUXNKGEGMZGRSONLCV
AGEBGLBIMORDPROCKINANKVCNFOLBCEUMNKPTVKTCGEFHOKPDULXSUE
OPCLANOYNKVKBUOYODORSNXLCKMGLVCVGRMNOPOYOFOCVKOCVKVWOFC
LANYEFVUAVNRPNCWMIPORDGLOSHIMOCNMLCCVGRMNOPOYHXAIFOOUEP
GCHK**Úloha 7**

MCCMMCTRUOUUUREPUCCTCTPCCCCUUPCMMP
RTCCRUPECCMUUPCMPEPPUPURUPPMEUPOCE UUCUCCCMEMTUPETPCMRCMCCUCCMPECRTMR
UPMPMRCPMMCRUMCUUEURPPCMOUUEUCCMUM TUCUCUTMUUUPMUUCTCUPMMCCRPPPPMMMME
EUMRCCCPUUEUPMUMMCCPECUCUPCTCUEPMP CUUEEUUUTPMMUCCTCCPPPCTPUCUCCCUREU
TUCMEPCCEMUUUPRMMTMUCMMMCCCCCCMEPU ECUMRERUUUUMURCCPMUURUUPMUPRPPUUUU
MRCCPCPEURMMMPUTCRUUEOUUUMCMUURUPU RUCMUCRUMMCUPUUMUCREUUUPCCURRCPRMC
TRCUUURCTPPMUUCCUUUUMUUEPCRMEPMPUU CCCUMMUUMCUCMCCCRTCCMEEUPTMUUMMMCC
PPTMCPTEOUUUMUUCRMCCCMCPRCRCEPMCMC PUUCMCCOMTPRCMCPCPMCPCERRECCRRECRU
PUEEPMUMTCUCEUUTPCEUMRCUOURRUCRUUC RPPTTCPCPCUCUMUMPECEERPMRMMURUMEPM
RMMCPRUCRCPEERPUUUURREPCCMMEPPPRCCU MPCCCMMEEUUPPERUECPUEMUCCUUCPUEPUC
MCMCUUCMMMCUPCCMMUUUCUOPUCUPMPUECC EUPMCEPRCTRMCCUUTECECCRMUCURUCMUCR
CMPCCUORUCTUCCMCUCMUMMTRUMCMMCP0UM UPCCMPCUUEPCTECTUUTCEEMTUCTEPPRUUM
UUECMUMRUEPCUMPPOURUCCUPUCUCUEPCMM ECCUCECPPCCCCOCRCRCRTUCPPTPUOCUORU
CCCEUCPPMRRCEUUURURCCMTPPURPPCTRRT RUUPMTMUUETRPROEMPTPTEPRERPTRUUUMT
RUMTPPPRUUPEOUTPTROMUUERMMEPOTTOTO OMTPRMPPTMREURRUPMTRPPREMUPRTRMMEO
UMMUPUUOUMEMOMECPEUUUUCRUTTTRTUPTT PEREMUUREEPETRMPTRUUUOTRUUOOTTTOTT
ETETOUPOMTUUOUTOEETPTEMUUTURCUOPTR POTEEMCOUUEPRMPTTTUPPRETTROEMUETPO
PMTERTEUUUPUPUUEMMOTOUMORRCMUUUETU
OTTEMTTCTMETEREUMUEETUMETPUTPUETTM
PEERTCPTOUUTRERETUTRETRTRUTCMTCUUT
POMTTPTPTOUMEOTTRPEPUTTTRTTOUMUUTP
EECTMPPMUECTRPUCTEUUETPTOTPMTMCPUE
ppUPRMTPCRURPREMERTUEEROROTOMMRCUU
EUTPTEPPEUUTPOTPPMEPEMTREEUTUUTOTP
REEROPORRMUUTMPRTTMEEETERUTMTOOCPE
PPMPMTPRRMEPREUMMPRTREEPUTTPECTURU
RCOPEEEOOUEMOMPTUECERMMMPPEPMUEMUR
TEUMRTTPOTCEROETMUUROTUTTRMUETETTR
PROUTUUPREUTTRTPMTUPEEMETEPTOETUUT
EPTMUUEEPPTPMUPTEPRMUTTPMUMMECRETE
PTRTURPMTOOUEEOTOURUURTUEUTPOMTPPU
REOTCMCPRPROOEERUUEERUMUUUCPPCPUET
ERORPORPTPCTPERERMUTTREUPRTMECUREP
POUTMOTCTMPTPOEUUTOTPTOREUETURMETR
EPEEPRUCPEMMPTMUUTTEOERMURUURUTPTT
ECETORTMTMETTUEMUUCTOPEMUUEPUMCMUC
MTPOUCECMTREMCPCMCTPMMPPCMUUUUCMCC
CPTMMUCREUUCTRREUCURECPMRCECUCEUCC
PMCTTPCREURMUTUPMPPMMCUTMCMCCEUUCT
UPUUUUURCUMEPOTUUUCTEPCCPMCCTPCPUM
ERUCUMEMMRMUPCMUUCUCRUUUUCPCUPCECM
CUUPOPCUUUUCUTTCPCMCUUCCEPUUPCMPUC
MMMPUUUEPMPPECRCMPRECRRUMCUECPUPUC
EMPMUCRTUTUCRCCUPUUCUMMPUUUUECUUCC
ECPPPRRMCMMECCRMMRCCECTURMCECCCPMM
MRPECUUUCPPMMECCMMRRCMUCMRCPCUCMUC
CCPCTRCUUEUCCMTEMCRCPECCUUCUUCPETP
CCPPTUMPCMPCMCEUCCCPCUCTCCCMTUMPTU
MEUCPPMUMPMMREMCUMMMERUCUCCMPUUEUC
PCEPPRUUCCUCTPUETERCMMMURUUPURPUEE
MUMUMRCUUCRMRCPTEMECMMUCUCUUPPETTT
MPCPMM0EMPPCUTPMCMUUPUCCPMPRCMCRPU
PMEMUUURCOCPCUEPMRCPTMMMMCCECUMCUU
CECPPUCPMRMEPCUURUCUCPRTUERMCCRPMUURUUPMEUPCECPTRUTUMCECEPCUTCUCPE
PC CUUETPPCPUUMCMMROUCCPUCPPEPMECRPCM
CUMPUCUUUEMMCUTMCUMCUEUCMUCCTPUREU PPCOPMPMUUMMMUUETPUUUUUPPPPMUECERU

RPURTPMPPPMEMCTUPCMECPPCCEMURMPTUU RCUEPCUECPUTCURUCPRUMTCOCCMPUCMEPE
MPRUPPECCPCUUCCCEUMRUUEUUEUCPCPMPU CUMPUCUMPPREUUUPEUPEUUCTPOTUPETUOE
COTTEMOTEUTEUMUPMUTPOUPETERPUTPRUU UPOTTEPTRRMTCETOROPMTRETRCOETPROEE
PTEPMMEUPEPEPUPUUREEPERTPEECEPORTU EMETTEPTERMMTTETTTPORUMPTTERPPUURM
TTOMTMUMMUUTUOEPEUUOTCPEPTMRERURPE TPPTTPCORPTTTMUTRUPPTERREURPRTRETT
RCPRCUUMUPRUUUMTPRTRETTUUUOCUMUUUU MOTTPEMETTERPCTOETUURMEPEEORCPETMP
PRUTTRUUETMOTMUUMTERUTOTCRPMURMUMR MPMOOMOUOTPOREMEMUPTORTRRPOOUTPPPE
PMTPEOCTRRMETORTPEMMPEEETRUURURPPU PURTROUMTMRCUOTETRCRPEECPTEEUUEMTT
PURUPEUOEUUMPEMUUTTEREUMERTTETTTME UTMRTORMECUCUEUEPRUMTUUERMUTREUUPE
EMEERCUUUTRMRTRMUUMMEPPTPRTEMTEMPE UETPOOOUUMOTOUTOOPEPRUUR T T
TMURTUTE TPCOTEMTUOETRMTETEMMTUMOEEOOUMOPTP
RUTMRMTRTPTUUEPUUPURROEUERUUOUPRTM ETPEPPOTRMCMRUTTPUUEURTTEETETUUEUE
ETURRMEEMREURCTPEMUUREPRUEORURUUPT UMPEMTTPTUEMUPMORTOOOUTPPMUUPUPERE
RUUOUEETUPETETPTTTEMRUURTTTUTTMUPR PRRURUUTMTURTCUEEOMRRTETTMUTPPRPEP
TREEOOTTETRETRUTPRUTMUUOTMUUCTUUPU ERUEEMMUEETTPETMUMETTETTPMREMRTPTE
TOURTPPOETTOMTPTETEUTPUCUMUCUOETUC PECUCMUPMUCUTTUCTUUMUCURPUCPMCUUMU
CCEPCMMUCPTPUMUPUCMECMPUMPPMUEMPPE
PUTEUMEPEPUPUURMTPEMRPMMPTPOPRCRUE
PCMPPMRCCCPUCUPTUMUUPCPEMPTUUMCCCU PCCUTUUURCEMPEUCMRPPEPCCMMMUMPECMT
RERPUMPCCPTUCMCOPCURUECMTECMMCCRPP EPUUCUTMUUUCCTMCMECPCDUUPUCUUUTCUC
CPTUUCCMMPPREMCUURUOMUEUUPPUCRPMRU PCMUUECUUCCUURCERRCUCPMPUOMTUURCMP
EMUUUUCTUMTTTCUMPUMCMRTUUUCPPMEPUC TOUPCMMCECUMCPECUPMTEPRUURURMPUPER
CRUUCCCMPCUCMRMPMPEEPTPEMCURCPCPUR UTEUUEUUUPTCUCCCEMMTUTREREMPRRMUCC
RCUMUEPUPUEUEPMUTRUCCMUUCMMUUPMECM MEMUUUCMRPCMCUUCCETPCPRRMURRCTECMC
MUUUUUUECUUCUUTEPMUURCCCUURCUCECPP UCMURCUUCRUCMCRCCCUCUMEMUUCPPPPRCR
URUCMCPPCRMPUEPUMPOMUMMCUUUPCCCECT MRPUPMPOCCTPCMUUMCMCCTUCECUUMCCMCU
ERTTRCMMUMTCPERUUMMTRUEUMCMCCMCUUP MUCCTPUMCUTPUMCUUUUCPPDCETUPERTRUU
UUMMCUMEEMCTCCPURRUURCPCUPCCUPMPMM URUUCCCEPRPUMMUTCMCMCCCUCPPCMEPCRE
MUURCTPEMCMCCPRUCCUUUCCUUPCUUPUTRU EEUUUEUCRPMRUUUOCPOCRPCMECRCPCECUU
ECPPUMPPEPCPRMPEUCPTUEMTUTTEOPRUEP EPMTPUPTTRRERPUEMMOPMUPRUUUMEMPPPU
TOUROPROPPMETPRMTUURPTPUUTOUUMTEPC OEMCUUTPUUPTOTUUTTUUURTPTRTTMOCTRU
TROTTROPTUMPPMURTEUMTPEUMCMPREPMRE EEEUTTTEUUTMTPURUEUUMTUPPUTTREMTPT
RRUTURTRUUTOTEROTMUUUTMUPTPUURTERU MMTMTTUPRPPPEMEPCMUMTRREMUCEUPPTTT
TTPRUUURTEEPUPUTMMTUPMRUOPEUEETMMP EMTPECRETMEOUTMEEPREUMEMRTOTEMTOTP
TECEPTUTREEEMPPTPEECPPTMUUTMUMPRME REUUPTOEOPUEPTRTTEPMOUMPEUTMTTMUUU
TTPTERMTRRUURUUEURTEEMUTTEPOUUEMEEPCRURMETMETOREUUOTRTPRTTEUMMTPMMRP
EUURERTEOTUTRROTOTETTEOTUEUUETUETP
MUOORTOUMCOTUECEUURUUMTTERUOTTMTE
TTEOTUTEPTRCTUUPPERUTOUUEORMUEMPRE
MUUPOPMOUOOTECUOETUCMTTPTTUURTTMMO
PTPUCMTUUOMUMTTTORTUPETETROMTRETTU
EUUTPPTMEUMURUUUURETUTRURRTTPPTTPO
ETEMUOTCOUEMTTMTUEUUPTUPUPTROTUEER
OEROUEMCPTERCPPTMUUMTOMCEMUTPTTTOU
TOEMTTPPCREPOTEPPERPOPPOTEUUUURPUU
CPRPRMTREUUERMUCTOPTTUUTPMCTRMETEM
MUOPTUUETPPMMRMTUPRMUPRMOUPRTEUUUR
MMCORTUMTOETMUPMUTTPUTTERMUUPCETMT
UPTPPETRUTTPOTMECURCPUOPMTPMCMPEPC
MMUORRMPCMMORCCUTCCOMCUUPRCPPPUCUU
EUPRUPMCECTMCCUURPPMUUEUUUUCETUURC
P U U RE UCECUCCUECUUURCPPMCCCUPRMUCMU
CPRUPPUOMPUUUCMUUCPMUCRCPMMTCMMUOM
CMCCMUUPCCTURUEUUUCUMT.UCCMMUCTCRRU
RUMRPRUCUCEMUCCUUUETUMCPCURPURCOUM
UPPCEMPPPUUMPPCCPRRCECCRMCPPRCCRPP

MUUURCMEPCPUCCCCUPRRUUPMCEMCUTMUCC
MEPMMPPMUUCCEMPREUUTCPCUCMCCUCMRTP
MPCUCPPMRCMPCPEMPPPMRUUCCUUPRCERTU
UPCUMUPUMPCRCCEPCUCCPMTRPCPCUUCRPP
RURCCMEUURUUMURPEMRUCCMMUCRMCTMRPR
CUCMCUUCUMMUUUEMCTMCCMUCTCMUCMPMUT
RURREOCUCRCUPUCMPCEUCCEUUEPUMPTCCE
URCUUCPURCTPEUUMMUUUCCMMTUCRCRMRPO
UCUCUPCMPCUCTPMMUPUCUMUMCUTPPMEUUU
PUPCUUUUCMPUEMCUPCCRPPRUUMCCUCUPCP
CPCCUUUCURCCPURCUTURECRUUCMTCCCMUC
CPPPCMUCCUUUUUMMPUCRCUECCTPCPMEECM
UUCCCUUMCPCCCUUCUPCUPUTCMMCUMMMUMM
PUMMPTRMMPPPMRUUUCUURETUCPECRPURUR
CCCTPPMTPUPMPPMRMURPUPUUUUUEPUCMPR
PPCCROUUECTUPCUPCCUUCPCPCMUECM0TUU
pCUUTPPPCMMUPCCRUCERTUCTECMCUUECRP UMCUTCUECCUPCUCCPURPMMTUTPPOCURCPC
PPMCMCCCPUPPMRUTERMOTUMUUEMRCUUŤPU pPTTTMUOTTERPRETTRMTEMTEUUTTRPTTCU
TMTUPMREUPMUEUUUUUPTETCPUCEECTERMM TMOTMPMETRPEROPEMEMMPRPTRUPTUOEUMP
PURMUUEMMMPUCPUMUTMPEUUOPPUOMPTOTR RMTPCPPPREPEERMREMUTPOUEMPPEERRMTR
TOMEPTEMUEPRTUROOTOMUPPEROTTPTTMPP TPCUUUMTTUREOPMTRETTMEEUUOPMERMPET
EERMUTTMMPEPOETMETERUUOORMEMMTRUUR UOPRUPRPPUUUEEETTTTPEURERRPUETRUUE
OOOUETEUUMUTUROTRUUTOPOTUPMURUUERU UUPUOOTTTPMEUERTMOUMTPPPEOMTTUUUOE
UOETUUETURPUMTMMERRUUETOTPTTTRPTMP
EEMTMEUUPOETTPPPRUTEECOUMEUOTTRTTT
RTTRTTMEPPTRTPOUTRTTOPECRTPUTTCEMP
TOMRETTTREUCOTOTRPRURPTUTEUUEPMEOT
MMUUURRETMOUMMPCPETPTPRMTUPUETETEE MCCTERUROEEPRRRRTPTUUMTPEEMCUOUORE
CTUPPRTPPMTMUMCTTTPRREOUTPERUTMPOR RUTUMOTTEETMTRMRTOMTRRRTOPTTERUOOM
UTPRMMPRPUETMEUTTMPPRTPTPTTUUMRTET TRROTURUTRUUCMRCMTOCRUTPOTTPTMTEOR
RMRUEURRTTOURUPTUECTEOTMTPRTPUMMRE EEPORPORPRUMEMOTTROPRUETTUETROMTOU
EOPUTMTURPTPRRTMORETCTMTMUETTMRTTE ORPCPPMMUMTTOUMTEUURTRTRMEMUUTMTUT
RETPMTPPMM**Úloha 8**


Umkehr-walze
Walze 3
Walze 2
Walze 1
Stecker-brett
Tastatur
?

```
K J Q P W C A I S R X W Q M A S E U P F O C Z O Q Z V G Z G W W
K Y E Z V T E M T P Z H V N O T K Z H R C C F Q L V R P C C W L
W P U Y O N F H O G D D M O J X G G B H W W U X N J E Z A X F U
M E Y S E C S M A Z F X N N A S S Z G W R B D D M A P G M R W T
G X X Z A X L B X C P H Z B O U Y V R R V F D K H X M Q O G Y L
Y Y C U W Q B T A D R L B O Z K Y X Q P W U U A F M I Z T C E A
X B C R E D H Z J D O P S Q T N L I H I Q H N M J Z U H S M V A
H H Q J L I J R R X Q Z N F K H U I I N Z P M P A F L H Y O N M
R M D A D F O X T Y O P E W E J G E C A H P Y F V M C I X A Q D
Y I A G Z X L D T F J W J Q Z M G B S N E R M I P C K P O V L T
H Z O T U X Q L R S R Z N Q L D H X H L G H Y D N Z K V B F D M
X R Z B R O M D P R U X H M F S H J
```

Schlüssel

```
0716150413020110
```

Schriftzeichen

```
begin 644 DEBUGGER.BIN
(-&>`_EU-_/$`
`
end
```

Úloha 9

```
begin 600 text.d
MM5P7)_8F_,H[JOF1C//L/W+)%QSK*Q37CJ-N 'W[_;CQSTW'UY0S2,\LQVG0
M@1&HY^1MHYI\>2P'F:6Y*E%X4A&$2'=L28$$..9["-ZIGA_VP(GIPK[CW3^L
M55+6OD^&=FS61(L96YG>  '59*1Q^)/C?$1/C&9PN35-HP;.>V8_/P(.:+R(
M61]'NG^UF:,#57MMQSKN[N7M>1NE;2(!RUA495Q16!;Q<*("[C*"A"@%A+=S
M8AR45+G$-#8A?29V_.6%7*6D$J_G4JX'JM^1? K@._#(B/N7-<YNU;/,JF8C
M6LD[90MVJ2'I*.G@>9U%!E(33!S^K# N7JH_Y5RYE&=J@S!>^<C3Y=PD%-RP
M9&++^"JLPOK%T)-5KI>IUA"W;7;&D(D-2/U'$3\C7 ?]B* 3*C/Y!%U >&V6
M%W85NJ:JPO(>#C1)CFEL&^H3YKR2.59XJVD??\MX+ [S?3X_F^/*1$NGH$B&
MI$L2-C'E/@OD*&5;6+P+G1S D49AO=#9\C!4D$/F;C(H#MX:\%G[K[OR+2RG
M@@SCSVG!A5%FEV!=$YD"V.2T06@>C-&)3H<:Y9BOR=V#S_>\:S8GZ.*A"$!T
MZOE=/4QWLLB<[:K8T TZ@C9_,( #D:/G4)P2>,S?%9: Q]MV0;?F9;F1VP'@
M=!XCI_M>2?F=' ;20):%Y61[.! -W8%7M3BJUX/&!-E@A7C\(>5SZXESA$LZ
MF\_U//JGV"KKHE259927962%P-9J!*J@ DPJF]M2/>DXHA?JT"^2C7;_-9B;
MBM'CFTYUR#DOA7.J4ZW8=+3(9O>#4A+^!=4IV_6A!(PNGZ:T$O)659KNGS=>
MN"?LQ3$6F*I43Q(3_U:64V/L9$<E%">*#A9P>@(66#XDS!)-'*\JZE.,=G29
MOJLH!9.Y#+=?]!"C?2/?H5O!A]<KW^H%J "&>+EXK;II6)N6JY$%UB'BN3'F
MMS[XKP#JY(:3@V);U2,5PG 6$!46;.B/K'E7$4'MKN1]* YX^R"Q?Q+;,"./
MPL((>]UF90L7[<]9^E0*:NMBI(Q+B'>-IHF+,J0&"G0F.5L8@"_)<Y$<ZRU=
M']&L9!WD1Y<V[D:/:4J(+#X(NIKKDFO@#:5O_3G%7]AG5H.? ,%;D)=7'HKE
M.(_E=(*(W5HO3RA5WP8<!ZM.K2T.:&#P\LV;!7W$ K3)/A7D&P8SVO3-?$U1
M2J10K3T>2)OVRA'Y;C<DZVV+'$VXI_ $JZ^)39,'.7MK,0*QOP9O6QRQ0F(*
M&8J9O!Z">N;S%MD%%A.SD?'^\K]"R_@XE6V# >&P.$L#$,%N"C[H:A_EPH$V
M\H)(;C0#3^C] T9Z0=,9UQ(3N^3D],9PVM<AJ.T:('(.=1FB;NBV_YS!\7ON
M?-T%5B;2J^TORBWA^Z$B'$K8LC;'A+>@87(6!8Q%FRS=^;Y*0$FC">;I!NI*
@#%0SNY_0_-EK1>;84QMT0/(KQQ2LL+R##K:I=NK7.OT

end
```

Úloha 10

Kratší zpráva

```
10052 30973 22295 13534 12990 66921 15454 81904 58209 26472 18119
11542 99190 01294 87266 20201 55809 80932 92390 96710 64341 91354
27685 27572 48495 78859 80627 33369 29356 36094 85523
```

Delší zpráva

```
begin 600 text.d
M.4#)>S I:R!!4)NA+\%T%V/(AW!7HHDPS$;T[\E!RWA?,J8:X#D[!:XF,A>K
MXT9$Q)37\IOMG6KL-$6?A!#FZ2Y)N+4%*.^2K!SP?Z2'8O7LZ]QP \T=QG-*
MAMJA;Q@3H[8^U/L<ILL%TA0J9M*F@8F?H:76%<33JOESAP=@3:(\:8NBGFM0
M,MP3B^CP%/D8DICZ$VO(7IS(DTJRZ&#Y- 7I\-#VI0">J@+O!CT.+6B9K$J%
4:EAB9%1#;(P+I>1!#<+2+;(7.W<

end
```

Dodatky

Dodatek A

Úvodní odstavec *La disparition* (Zmizení) od Georgese Perece (v anglickém překladu *A Void* Gilberta Adaira).

Today, by rádio, and also on giant hoardings, a rabbi, an admirál notorious for his links to masonry, a trio of cardinals, a trio, too, of insignificant politici-ans (bought and paid for by a rich and corrupt Anglo-Canadian banking Corporation), inform us all of how our country now risks dying of starvation. A rumor, that's my initial thought as I switch off my rádio, a rumor or possibly a hoax. Propaganda, I murmur anxiously - as though, just by saying so, I might allay my doubts-typical politicians' propaganda. But public opinion gradually absorbs it as a fact Individuals start strutting around with stout clubs. „Food, glorious food!" is a common cry (occasionally sung to Bart's music), with ordinary hardwor-king folk harassing officials, both local and national, and cursing capitalists and captains of industry. Cops shrink from going out on night shift In Mácon a mob storms a municipal building. In Rocadamour ruffians rob a hangár full of food-stuffs, pillaging tons of tuna fish, milk and cocoa, as also a vast quantity of corn-all of it, alas, totally unfit for human consumption. Without fuss or ado, and naturally without any sort of trial, an indignant crowd hangs 26 solicitors on a hastily built scaffold in front of Nancy^s law courts (this Nancy is a town, not a woman) and ransacks a local journal, a disgusting right-wing rag that is siding against it. Up and down this land of ours looting has brought docks, shops and farms to a virtual standstill.

[Od rána k nám promlouvá z rozhlasu i z billboardů jakýsi admirál (prý rabín, proslulý svými styky s tajnou lóží) s trojicí pohlavárů - málo významných politiků (zkorumpovaných bohatou a prohnilou anglo-kanadskou bankovní korporací) o tom, jak nyní hrozí občanům tohoto státu hladomor. Fáma - takový byl můj první pocit po vypnutí rádia. Pouhá fáma, snad i čísi hloupý vtip! Propaganda - mumlám si naštvaný, jako bych si tím do-dával odvahy - typická politická propaganda. Avšak zpráva padla na úrodnou půdu. Různá individua si začínají budovat silnou základnu. ‚Jídlo, pořádný kus masa!" křičí (s občasnou halasnou podporou místní kutálky) do úmoru pracující prostý lid, sužovaný byrokracií na lokální i státní úrovni - tou proklínanou kapitalistickou mocí svázanou s průmyslovými magnáty. Už

i strážci pořádku mají strach vystrčit v noci nos na ulici. V Máco-nu zaútočila lůza na správní budovu. V Rocadamouru rabují zoufalci sklady potravin s tunami tuňáků, sunaru a kakaa a s plnými pytli zrní -avšak hrůza, žrát by to mohla toliko zvířata! Aniž by zkoumal míru viny a komukoli poskytl právo na obhajobu, popravil zuřící dav, prostý skrupulí, 26 právních zástupců. Tito ubožáci skončili svůj život s oprátkou na krku na provizorním popravišti u soudního dvora blízko Nancy (tady mám na mysli sídlo, nikoli dívku). Masy zoufalců jdou po krku i místnímu plátku -protivný pravicový bulvární tisk totiž brojil proti vůli lidu. Drancování ničí krajinu od východu k západu - krachují přístavy, obchody i farmy.]

ha disparition bylo poprvé vydáno ve Francii v nakladatelství Editions Denóel v roce 1969, ve Velké Británii publikoval Harvill, 1994. Přetištěno se svolením Harvill Press. Český překlad ukázky Michaela Tichá.

Dodatek B

Některé základní tipy pro frekvenční analýzu

(1) Začněte tím, že sečtete frekvence všech písmen v šifrovém textu. Asi pět písmen by mělo mít frekvenci nižší než 1 % a ta pravděpodobně představují j, k, q, x a z. Jedno z písmen by mělo mít frekvenci větší než 10 % a to pravděpodobně představuje e. Pokud se šifrový text tímto frekvenčním rozdělením neřídí, vezměte v úvahu možnost, že původní zpráva nebyla napsána v angličtině. Jazyk zkuste určit tak, že analyzujete distribuci frekvencí v šifrovém textu. Například pro italštinu je typické, že má tři písmena s frekvencí větší než 10 % a devět písmen s frekvencí menší než 1 %. V němčině má písmeno e výjimečně vysokou frekvenci 19 %, takže jakýkoliv šifrový text obsahující jedno písmeno s tak značnou četností bude velmi pravděpodobně v němčině. Jakmile jste identifikovali jazyk, použijte pro svou frekvenční analýzu odpovídající tabulky frekvencí daného *jazyka.*. Často je možné dešifrovat text v neznámém jazyku, ovšem za předpokladu, že máte odpovídající tabulku frekvencí.

(2) Pokud korelace odpovídá angličtině, ale otevřený text se hned neodhalí, což se stává často, zaměřte se na dvojice opakovaných písmen. V angličtině se nejčastěji opakují písmena ss, ee, tt, ff, 11, mm a oo. Pokud šifrový text obsahuje jakoukoli dvojici stejných písmen, můžete předpokládat, že představuje jedno z nich.

(3) Pokud šifrový text obsahuje mezi slovy mezery, potom se pokuste identifikovat slova, která obsahují pouze jedno, dvě nebo tři písmena. Jediná jednopísmenná slova v angličtině jsou a a I. Nejčastější dvoupísmen-ná slova jsou of, to, 1n, 1t, 1s, be, as, at, so, we, he, by, oř, on, do, 1f, me, my, up, an, go, no, us a am. Nejčastější třípísmenná slova jsou the a and.

(4) Pokud je to možné, vytvořte tabulku frekvencí specifickou pro zprávu, kterou zkoušíte dešifrovat. Například vojenské zprávy mají sklon vynechávat zájmena a členy, ztráta slov jako I, he, a a the sníží frekvenci některých nejběžnějších písmen. Pokud víte, že pracujete s vojenskou zprávou, použijte frekvenční tabulku vytvořenou z jiných vojenských zpráv.(5) Jedna z nejužitečnějších dovedností pro kryptoanalytika je schopnost *-založená,* na zkušenosti nebo čirém dohadu - identifikovat slova nebo dokonce celé věty. Al-Khalil, raný arabský kryptoanalytik, předvedl tento talent, když rozlomil řecký šifrový text. Uhádl, že šifrový text bude začínat pozdravem „ve jménu Boha". Poté, co zjistil, že taio písmena odpovídají určité části šifrového textu, mohl je použít jako „páčidlo" k otevření zbytku šifrového textu. Tomu se říká tahák (crib).

(6) Může se stát, že nejčastějším písmenem v šifrovém textu je E, druhé nejčastější může být T a tak dále. Jinými slovy, frekvence písmen v šifrovém textu už odpovídá

frekvenční tabulce. Přestože šifrový text vypadá jako hatmatilka, zdá se, že E v šifrovém textu je skutečným e a totéž zřejmě platí pro všechna ostatní písmena. V tomto případě nemáte co do činění se substituční, ale transpoziční šifrou. Všechna písmena představují sebe sama, ale jsou na špatných místech.

Cryptanalysis od Helen Fouché Gainesové (Dover) je dobrý úvodní text. Poskytuje různé tipy a také obsahuje tabulku frekvence písmen v různých jazycích a seznam nejčastějších slov v angličtině.

Dodatek C

Takzvaný biblický kód

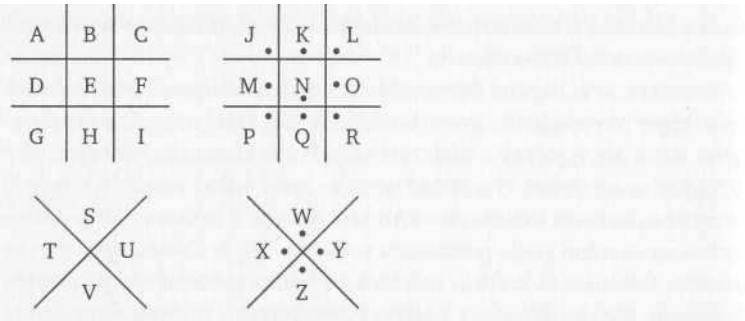
V roce 1997 se kniha *The Bible Code* (Biblický kód) od Michaela Drosni-na dostala do hlavních titulků zpráv po celém světě. Drosnin tvrdil, že *Bible* obsahuje skryté zprávy, které mohou být objeveny tak, že hledáte ekvi-distantní sekvence písmen (ESP). ESP najdete tak, že vezmete jakýkoli text, zvolíte určité začáteční písmeno a pak vždy přeskočíte dopředu o předem daný počet písmen. Takže například u tohoto odstavce začněte s M v Michaelovi a přeskočte, řekněme, pět míst najednou. Pokud zapíšete každé páté písmeno, vytvoříte ESP meoaahft...

Přestože tato konkrétní ESP neobsahuje žádné rozumné slovo, Drosnin popsal objev ohromujícího počtu biblických ESP, které nejenže tvoří smysluplná slova, ale vyplývají z nich celé věty. Podle Drosnina jsou tyto věty biblickými proroctvími. Například tvrdí, že našel odkaz na zabití Johna F. Kennedyho, Roberta Kennedyho a Anwara Sadata. V jednom ESP je jméno Newton zmiňováno vedle gravitace a v dalším ESP je Edison spojován se žárovkou. Drosninova kníhaje založena na článku uveřejněném Doronem Witzumem, Eliyahu Ripsem a Yoavem Rosenbergem, ve svých tvrzeních je však daleko ctižádostivější, a proto přitáhla mnoho kritiky. Hlavní příčinou nesouhlasu je fakt, že studovaný text je rozsáhlý: v každém dostatečně dlouhém textu je snadno proveditelné, abychom několika změnami počátečních písmen a různou velikostí skoku sestavili smysluplné věty.

Brendan McKay z Australian National University se pokusil prokázat nedostatky Drosninova přístupu tak, že hledal ESP v *Bílé velrybě* (Moby Dick), nakonec objevil třináct „zmínek" o vraždách slavných lidí včetně Trockého, Gándhího a Roberta Kennedyho. Navíc hebrejské texty jsou zákonitě obzvláště bohaté na ESP, protože z velké části postrádají samohlásky. To znamená, že interpreti mohou vsunout samohlásky, kam uznají za vhodné, což ulehčuje sestavení předpovědí.**Dodatek D**

Šifra prasečích chlívků

Monoalfabetická substituční šifra přetrvávala v různých formách po století. Například „šifru prasečích chlívků" používali svobodní zednáři na počátku 18. století pro uchovávání svých tajných záznamů. Ještě dnes se s ní baví školáci. Šifra nenahrazuje jedno písmeno druhým, ale každé písmeno textu nahradí symbolem podle následujícího vzoru:



Pro zašifrování určitého písmene je třeba najít jeho pozici v jedné ze čtyř mřížek a potom načrtnout část mřížky, která písmeno představuje:

a =

b =

:

:

z =

Pokud znáte klíč, je snadné šifru prasečích chlívků rozluštit. Pokud ne, je jednoduché ji rozlomit pomocí nápovědy:

Dodatek E

Playfairova šifra

Playfairovu šifru proslavil Lyon Playfair, první baron Playfair ze St. Andrews. Skutečným vynálezcem však byl jeden z průkopníků elektrického telegrafu sir Charles Wheatstone. Oba muži žili blízko sebe, každý na jedné straně Hammersmith Bridge, a často se scházeli, aby pohovořili o svých myšlenkách týkajících se kryptografie.

Playfairova šifra nahrazuje každou dvojici písmen v otevřeném textu jinou dvojicí písmen. Aby odesilatel a příjemce zašifrovali a poslali zprávu, musejí se nejdříve dohodnout na klíčovém slově. Například můžeme použít jako klíčové slovo Wheatstonovo křestní jméno CHARLES. Před zašifrováním dále sepíšeme písmena abecedy do čtverce o rozměrech 5x5, počínaje klíčovým slovem a dále spojením písmen I a J v jediný prvek.

C	H	A	R	L
E	S	B	D	F
G	I/J	K	M	N
O	P	Q	T	U
V	W	X	Y	Z

Zpráva je rozdělena na dvojice písmen neboli *digrafy*, které se skládají ze dvou různých písmen, čehož je v následujícím příkladu dosaženo vložením X mezi dvojité m ve slově hammersmi th. Písmeno x je navíc přidáno i na konec, aby vytvořilo digraf z posledního písmene.

Otevřený text meet me at hammersmi th bridge tonight

Otevřený text

vdigrafech me-et-me-at-ha-mx-me-rs-m1-th-br-1d-ge-to-n1-gh-tx

Šifrování může začít. Každý digraf spadá do jedné ze tří kategorií: obě písmena jsou v tomtéž řádku nebo v tomtéž sloupci, případně neplatí ani jedna možnost. Pokud jsou obě písmena ve stejném řádku, potom se nahradí nejbližším písmenem napravo od každého z nich - z m1 se tak stane NK. Pokud je jedno z písmen na konci řádku, je nahrazeno písmenem na začátku - z n1 se stane GK. Pokud jsou písmena ve stejném sloupci, nahradíse nejbližším písmenem pod každým z nich - z g e se stane 0 G. Pokud je jedno písmeno vespod sloupce, je nahrazeno písmenem z vrcholu - z v e se stane CG.

Pokud nejsou písmena digrafu ani ve stejném řádku, ani ve stejném sloupci, řídí se šifrování jiným pravidlem. Pro zašifrování prvního písmene se podíváte podél jeho řady, dokud nenarazíte na sloupec obsahující druhé písmeno. Písmeno *nalézající* se v tomto průsečíku potom nahradí první písmeno. Pro zašifrování druhého písmene se podíváte podél jeho řádku, dokud nenarazíte na sloupec obsahující první písmeno. Písmeno v tomto průsečíku nahradí druhé písmeno. Proto se z me stane GD a z et bude DO. Úplné zašifrování je následující:

Otevřený text

vdigrafech me et me at ha mx me rs m1 th br 1d ge to n1 gh tx Šifrovýtext GD DO GD RQ AR KY GD HD NK PR DA MS OG UP GK IC QY

Příjemce, který také zná klíčové slovo, může šifrovou zprávu dešifrovat tak, že jednoduše proces obrátí: například šifrová písmena ve stejném řádku jsou dešifrována nahrazením za písmena po jejich levici.

Playfair nebyl jenom vědcem, ale také význačnou veřejnou osobností (místopředseda Dolní sněmovny, generální ředitel poštovní služby a komisař pro veřejné zdraví, který pomáhal vytvářet moderní základy veřejné hygieny), a byl proto rozhodnut prosadit Wheatstonovu myšlenku mezi politickými špičkami. Poprvé se o ní zmínil v roce 1854 na večeři s princem Albertem a budoucím předsedou vlády lordem Palmerstonem. Později představil Wheatstona náměstkovi ministra zahraničí. Ten si však stěžoval, že celý systém je pro bojové podmínky příliš komplikovaný, načež Wheat-stone prohlásil, že naučí svou metodu chlapce z nejbližší základní školy během patnácti minut. „To je klidně možné," odvětil náměstek, „ale nedokážete ji vysvětlit diplomatům."

Playfair nakonec vytrval a britské ministerstvo války tajně přijalo tuto techniku, kterou pravděpodobně poprvé použilo v burské válce. Přestože se ukázala Playfairova šifra na čas jako účinná, nebyla zdaleka nedobytná. Mohla být napadena vyhledáním nejčastěji se vyskytujících digrafů v šifrovém textu za předpokladu, že představují nejčastější digrafy v angličtině: th, he. an, 1n, er. re. es.

Dodatek F

Šifra ADFGVX

Šifra ADFGVX zahrnuje substituci i transpozici. Šifrování začíná nakreslením mřížky 6x6 polí, kterér^plníme náhodným uspořádáním 26 písmen a 10 číslic. Každý řádek a sloupec mřížky je identifikován jedním z 6 písmen A, D, F, G, V nebo X. Uspořádání prvků v mřížce funguje jako část klíče. Aby příjemce mohl dešifrovat zprávy, musí znát o mřížce všechny podrobnosti.

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Prvním stadiem šifrování je pro každé písmeno zprávy nalezení jeho pozice v mřížce a nahrazení písmeny, která označují jeho řádek a sloupec. Například 8 bude nahrazeno za AA a p bude nahrazeno za AD. Uvedeme si krátkou zprávu zašifrovanou podle tohoto systému:

Zpráva	attack at 10 pm											
Otevřený text	a	t	t	a	c	k	a	t	1	0	p	m
1. stadium šifrového textu	DV	DD	DD	DV	FG	FD	DV	DD	AV	XG	AD	GX

Zatím je to jednoduchá monoalfabetická substituční šifra a k jejímu prolomení by stačila frekvenční *analýza*.. Druhým stadiem ADFGVX je transpozice, která činí kryptoanalýzu daleko těžší. Transpozice *záleží* na klíčovém slovu, které musí být sdíleno s příjemcem - v tomto případě je jím MARK. Transpozice se provede podle následujícího návodu: nejdříve napíšeme písmena klíčového slova do horního řádku nové mřížky. Potom pod něj napíšeme do několika řádků pod sebe šifrový text z 1. stadia, jak je vi-dět vlevo dole. Sloupce mřížky se pak znovu uspořádají tak, aby písmena klíčového slova byla v abecedním pořádku (vpravo dole). Konečný šifrový text se získá tak, že postupujeme dolů po každém sloupci a písmena zapíšeme v novém pořadí.

M	A	R	K
D	V	D	D
D	D	D	V
F	G	F	D
D	V	D	D
A	V	X	G
A	D	G	X

Znovu uspořádejte sloupce tak, aby písmena klíčového slova byla v abecedním pořadí.

A	K	M	R
V	D	D	D
D	V	D	D
G	D	F	F
V	D	D	D
V	G	A	X
D	X	A	G

Konečný šifrový text VDGVVDDVDDGXDDFDAADDFDXG

Konečný šifrový text se pak odešle morseovkou a příjemce šifrovací proces obrátí tak, aby dostal zpět původní text. Celý šifrový text je složen pouze z šesti písmen (tj. A, D, F, G, V, X), protože ty označují řádky a sloupce původní mřížky 6x6. Lidé se často ptají, proč byla za označení vybrána právě tato písmena, a nikoli třeba A, B, C, D, E, F. Odpověď zní, že A, D, F, G, V a X se navzájem výrazně liší v Morseově kódu, takže výběr písmen minimalizuje během přenosu riziko chyb.

Dodatek G

Slabina opakování jednorázové tabulky

Z důvodů vysvětlených v kapitole 3 jsou texty zašifrované jednorázovou tabulkovou šifrou nerozlomitelné. Bezpečí spočívá v tom, že každá jednorázová tabulka se použije jednou a pouze jednou. Pokud bychom mohli zachytit dva různé šifrové texty, jež byly zašifrovány stejnou jednorázovou tabulkou, můžeme je dešifrovat následujícím způsobem.

Pravděpodobně se nespleteme, že první šifrový text někde obsahuje slovo the, a proto vyjde naše kryptoanalýza z předpokladu, že se celá zpráva skládá z opakování slova the. Dále vytvoříme jednorázovou tabulku, která převede sérii the do prvního šifrového textu. Tato tabulka se stane naším prvním odhadem. Jak víme, které části první tabulky jsou správné?

Aplikujeme náš první odhad na druhý šifrový text a uvidíme, zda výsledný text dává smysl. Pokud máme štěstí, jsme schopni v druhém textu rozeznat několik fragmentů slov, které naznačí, že odpovídající části tabulky jsou správné. To nám zpětně ukáže, které části první zprávy mohou být slovem the.

Rozšířením zlomků slov, které jsme našli v druhém textu, můžeme dešifrovat další prvky tabulky a potom vyvodit v prvním otevřeném textu nové fragmenty. Rozšířením těchto fragmentů v prvním otevřeném textu se toho o tabulce dozvíme opět více. Potom jsme schopni vyvodit nové zlomky v druhém otevřeném textu. Tento postup lze opakovat, dokud nebudeme mít rozluštěné oba texty.

Postup je velmi podobný rozlomení zprávy zašifrované Vigeněrovou šifrou, která používá klíč sestávající ze série slov, jako například z kapitoly 3, vekterébylklíčCANADABRAZILEGYPTCUBA.**Dodatek H**

Řešení křížovky z *Daily Telegraph*

VODOROVNĚ	SVISLE
1. Troupe	1. Tipstaff
4. Short Cut	2. Olivě oil
9. Privet	3. Pseudonym
10. Aromatic	5. Hordě
12. Trend	6. Remit
13. Great deal	7. Cutter
15. Owe	8. Tackle
16. Feign	11. Agenda
17. Newark	14. Ada 22. Impale 18. Wreath 24. Guise 19. Right nail
27. Ash	20. Tinkling
28. Centre bit	21. Sennight
31. Token	23. Pie
32. Lamě dogs	25. Scales
33. Racing	26. Enamel
34. Silencer	29. Rodin
35. Alight	30. Bogie

Dodatek I

Cvičení pro čtenáře s hlubším zájmem

Některých největších dešifrovacích objevů v historii dosáhli amatéři. Například Georg Grotefend, který učinil první průlom ve vysvětlení klínového písma, byl učitelem. Pro ty čtenáře, kteří cítí pokušení jít v jeho stopách, předkládám několik druhů písma, které stále zůstávají tajemstvím. Lineární písmo A (minojské písmo) odolává všem pokusům o rozluštění, zčásti kvůli nedostatku materiálu. Etruština tímto problémem netrpí, k dispozici je více než 10 000 nápisů, přesto je záhadou i pro největší světové učence. Iberština, další pre-románské písmo, je stejně neproniknutelná.

Nejpodivnější staré evropské písmo se nachází na jedinečném Faistově disku, objeveném v roce 1908 v jižní Krétě. Jde o kulatou tabuli datovanou asi 1700 př. n. l., která obsahuje písmo ve formě dvou spirál, po jedné na každé straně. Znaky nejsou napsány

ručně, ale byly vytvořeny razidly, což znamená, že jde o nejstarší příklad psaní strojem na světě. Je pozoruhodné, že dosud nebyl žádný podobný dokument nalezen, takže rozluštění musí vycházet z velmi omezených informací - k dispozici je 242 znaků rozdělených do 61 skupin. Technologie razidel však naznačuje masovou produkci, takže existuje naděje, že archeologové nakonec objeví více podobných disků a vnesou světlo do problému písma, které se *zatím* vzpírá jakémukoli řešení.

Mimo Evropu je jednou z největších *výzev* rozluštění písma civilizace podél řeky Indu z doby bronzové. Písmo se *nalézá*, na tisících pečetí pocházejících ze třetího tisíciletí př. n. 1. Každá pečeť znázorňuje zvíře doprovázené krátkým nápisem, význam těchto nápisů však dosud všem expertům uniká. V jednom výjimečném příkladu bylo písmo nalezeno na velké dřevěné desce s obrovskými písmeny o výšce 37 cm. Mohlo by se jednat o nejstarší billboard na světě. Snad nám to naznačuje, že gramotnost nebyla omezená pouze na elitu. Nápis vyvolává zvědavost, co bylo na „billboardu" inzerováno. Nejpravděpodobnější odpovědí je, že nápis byl součástí královy propagační kampaně, a pokud by mohla být prokázána jeho totožnost, deska by mohl poskytnout nápovědu k odhalení tajemství tohoto písma.

Dodatek J

Matematika RSA

Zde uvádím jednoduchý matematický popis mechanismu šifrování a dešifrování pomocí RSA.

(1) Alice zvolí dvě obrovská prvočísla^? a *q*. Prvočísla musí být mimořádně velká, ale pro jednoduchost předpokládejme, že Alice vybere $p = 17$, $q = 11$. Tato čísla uchová v tajnosti.

(2) Čísla Alice vynásobí mezi sebou a dostane další číslo *N*. V tomto případě *N* - 187. Nyní zvolí další číslo *e*, v tomto případě $e = 7$. [Číslo *e* a $(p - 1) \times (q - 1)$ by neměly mít žádného společného dělitele, to je ale technický detail.]

(3) Alice nyní zveřejní *e* a *N* v něčem, co se podobá telefonnímu seznamu. Vzhledem k tomu, že jsou tato dvě čísla pro šifrování nezbytná, musí být k dispozici každému, kdo chce zašifrovat zprávu pro Alici. Dohromady se tato čísla nazývají veřejný klíč. (Stejně jako je *e* částí Alicina veřejného klíče, může být částí klíče kohokoli jiného. Každý ale musí mít jinou hodnotu *N*, která závisí na volbě *p* a *q.)*

(4) Pro zašifrování musí být zpráva nejdříve převedena do čísla M. Toho se dá dosáhnout například tak, že se slovo převede do ASCII binárních číslic, které lze pokládat za číslo v desítkové soustavě. M je potom zašifrováno tak, abý vytvořilo šifrový text C podle vzorce:

$C = M^e (mod N)$

(5) Představte si, že Bob chce zaslat Alici symbol polibku: pouhé písmeno *X*. Jeho ASCII reprezentace je 1011000, což v desítkové soustavě odpovídá číslu 88. Takže M = 88.

(6) Aby Bob tuto zprávu zašifroval, začne tím, že vyhledá Alicin veřejný klíč a zjistí, že $N = 187$ a $e = 7$. To mu poskytne k zašifrováni zprávy pro Alici potřebný šifrovací vzorec. Pro M = 88 vypadá vzorec nakonec takto:

$C = 88^7 (mod 187)$

(7) Kdybychom to chtěli počítat přímo na kalkulačce, nebylo by to tak jednoduché, protože displej tak velká čísla nezvládne. Existuje však elegantní trik,

jak počítat mocniny v modulární aritmetice. Vzhledem k tomu, že 7 = 4 + 2 +1,

88^7 (mod 187) = [?8^4 (mod 187) X 88^2 (mod 187) X 88^1 (mod 187)] (mod 187)

88^1 = 88-88 (mod 187)

88^2 = 7 744 = 77 (mod 187)

88" = 59 969 536 = 132 (mod 187)

88^7 = 88^1 x 88^2 X 88" = 88 x 77 X 132 = 894 432 - 11 (mod 187) Bob nyní může Alici poslat šifrový text C = 11.

(8) Víme, že mocniny v modulární matematice jsou jednosměrné funkce, takže je velmi těžké postupovat nazpět od C = 11 a získat originální zprávu *M.* Proto Eva nemůže zprávu rozšifrovat.

(9) Alici se to však podaří, protože má zvláštní informaci: zná hodnoty p a *q*. Vypočítá speciální číslo *d* - dešifrovací klíč neboli svůj soukromý klíč. Číslo *d* se počítá podle následujícího vzorce:

e X *d* - 1 (mod *(p* - 1) X *(q* - 1))

7 X *d* = 1 (mod 16 X 10)

7 X *d* = 1 (mod 160)

d = 23

(Výpočet hodnoty *d* není úplně samozřejmý, ale postup *známý* jako rozšířený Euklidův algoritmus umožní Alici nalézt *d* rychle a jednoduše.)

(10) Aby Alice rozluštila zprávu, jednoduše použije následující vzorec:

Aí = C(modl87)

Aí=ll^{23}(modl87)

M = [II^1 (mod 187) X II^2 (mod 187) X 11" (mod 187) X II^{16} (mod 187)] (mod 187)

M = 11 X 121 x 55 X 154 (mod 187)

M- 88 =*Xv* ASCII.

Rivest, Shamir a Adleman vytvořili speciální jednosměrnou funkci, kterou může invertovat pouze ten, kdo má přístup k důvěrným informacím, a to k hodnotě *p* a *q*. Funkce je určena výběrem *p* a *q*, které po vynásobení dají *N*. Funkce umožní odesilateli zašifrovat zprávu pro příjemce. Odesilatel zná jen *N*, zatímco zamýšlený příjemce je jedinou osobou, která zná *p* a *q* - tudíž je jedinou osobou, jež zná dešifrovací klíč *d.*

Slovníček

ASCII American Standard Code for Information Interchange (americký standardní kód pro výměnu informací), standard pro převod abecedy a dalších znaků do čísel.

Caesarova **posunová substituční šifra** (Caesar-shift substitution cipher) Původně šifra, ve které bylo každé písmeno zprávy nahrazeno písmenem o tři pozice dále v abecedě. Obecněji šifra, v níž je každé písmeno zprávy nahrazeno písmenem o *x* pozic dále v abecedě, kde *x* je číslo mezi 1 a 25.

Dekódovat (decode) Převést kódovanou zprávu zpět na originální text.

Délka klíče (key length) Počítačové šifrování pracuje s klíči v podobě čísel. Délka klíče se vztahuje k počtu číslic nebo bitů v klíči, určuje největší číslo, které může být použito jako klíč, a tím zároveň také počet možných klíčů. Čím větší délka klíče (neboli čím větší počet možných klíčů), tím déle bude kryptoanalytikům trvat otestování všech klíčů.

Depozice klíče (key escrow) Schéma, v němž uživatel uloží kopii svého taj-

ného klíče u důvěryhodné třetí strany, depozitního agenta, který předá klíč orgánům činným v trestním řízení pouze za určitých podmínek, například je-li vydán soudní příkaz.

DES (Data Ecryption Standard) Šifra vyvinutá společností IBM a přijatá v roce 1976 jako americký státní standard.

Dešifrovat (decipher) Převést šifrový text zpět do otevřeného textu. Formálně se pojem týká pouze zamýšleného příjemce, který zná klíč potřebný k získání původní zprávy, ale neoficiálně se vztahuje také na proces kryptoanalýzy, kdy dešifrování provádí nepřítel.

Digitální podpis (digital signatuře) Metoda, kterou se potvrzuje autorství elektronického dokumentu. Podpis je často generován autorem šifrujícího dokumentu, a to pomocí jeho soukromého klíče.

Distribuce klíčů (key distribution) Proces zajišťující, že odesilatel i příjemce mají k dispozici klíč nezbytný pro zašifrování a dešifrování zprávy, přičemž zároveň brání tomu, aby klíč padl do rukou nepříteli. Distribuce klíčů představovala závažný problém z hlediska logistiky a bezpečnosti až do vynálezu kryptografie s veřejným klíčem.**Homofonní substituční šifra** (homophonic substitution cipher) Šifra, v níž existuje pro každé písmeno otevřeného textu několik možných substitucí. Přitom je podstatné, že pokud existuje řekněme šest možných substitucí pro písmeno **a** v otevřeném textu, může těchto šest znaků představovat pouze písmeno **a** a žádné jiné. Jde o typ monoalfabe-tické substituční šifry.

Jednorázová tabulka (one-time pad) Jediná známá forma šifrování, která je nerozluštitelná. Spočívá v použití náhodného klíče, který má stejnou délku jako zpráva. Každý klíč smí být použit pouze jednou.

Klíč (key) Element, který změní obecný šifrovací algoritmus ve specifický postup šifrování. Nepřítel může šifrovací algoritmus použitý odesilatelem a příjemcem znát, ale nesmí znát klíč.

Kód (code) Systém pro ukrytí smyslu zprávy, který nahrazuje každé slovo nebo frázi v původní zprávě jiným znakem nebo skupinou znaků. Seznam nahrazení je definován kódovou knihou. (Alternativní definice kódu zní, že jde o jakoukoli formu šifrování, která nemá zabudovanou flexibilitu, tj. existuje pouze jeden klíč, jímž je kódová kniha.)

Kódová kniha (codebook) Seznam nahrazení pro slova nebo fráze v původní zprávě.

Kryptoanalýza (cryptanalysis) Věda o tom, jak bez znalosti klíče odvodit otevřený text ze šifrového textu.

Kryptografie (cryptography) Věda o šifrování zpráv, o zatajování smyslu zprávy. Někdy je pojem obecněji používán pro vědu o čemkoliv spojeném se šiframi a je alternativou k pojmu kryptologie.

Kryptografie s asymetrickým klíčem (asymmetric key cryptography) Forma kryptografie, ve které se k šifrování užívá jiný klíč než k dešifrování. Do této skupiny spadají systémy kryptografie s veřejným klíčem jako RSA.

Kryptografie s veřejným klíčem (public key cryptography) Systém kryptografie, který zvítězil nad problémem distribuce klíčů. Kryptografie s veřejným klíčem vyžaduje asymetrickou šifru, aby každý uživatel mohl vytvořit veřejný šifrovací klíč a soukromý dešifrovací klíč.

Kryptografie se symetrickým klíčem (symmetric key cryptography) Forma kryptografie, v níž je šifrovací a dešifrovací klíč týž. Pojem popisuje všechny tradiční formy šifrování, to jest ty, které byly objeveny do 70. let 20. století.

Kryptologie (cryptology) Věda o utajení zpráv ve všech formách zahrnující kryptografii a kryptoanalýzu.

Kvantová kryptografie (quantum cryptography) Nerozluštitelná forma kryptografie, která využívá kvantové teorie, zvláště principu neurčitosti, podle něhož je nemožné změřit všechny aspekty jevu s absolutní přesností. Kvantová kryptografie zaručuje bezpečnou výměnu série bitů, která se pak může použít jako základ pro jednorázovou tabulkovou šifru.

Kvantový počítač (quantum computer) Hypotetický, nesmírně výkonný počítač, který využívá kvantové teorie, zvláště pak teorie, že jeden předmět může být najednou v mnoha stavech (superpozice) nebo současně v mnoha vesmírech. Pokud by vědci dokázali reálně fungující kvantový počítač sestavit, mohlo by to ohrozit bezpečnost všech současných šifer s výjimkou jednorázové tabulky.

Monoalfabetická substituční šifra (monoalphabetic substitution cipher) Substituční šifra, v níž je šifrová abeceda pevně dána po celou dobu šifrování.

National Security Agency (NSA, Národní bezpečnostní úřad) Organizace podřízená americkému ministerstvu obrany, odpovědná za zajišťování bezpečnosti amerických komunikací a za luštění komunikací ostatních zemí.

Otevřený text (plaintext) Původní zpráva před zašifrováním.

Polyalfabetická substituční šifra (polyalphabetic substitution cipher) Substituční šifra, v níž se šifrová abeceda mění v průběhu šifrování, například šifra Vigeněrova. Tato změna je definována klíčem.

Pretty Good Privacy (PGP, Docela dobré soukromí) Počítačový šifrovací program vyvinutý Philem Zimmermannem, založený na RSA.

Rozluštit (decrypt) Dešifrovat nebo dekódovat.

RSA První prakticky použitelný systém, který splňoval požadavky kryptografie s veřejným klíčem, vynalezený Ronem Rivestem, Adi Shamirem a Leonardem Adlemanem v roce 1977.

Soukromý klíč (private key) Klíč používaný příjemcem k dešifrování zpráv v systému kryptografie s veřejným klíčem. Soukromý klíč musí být uchován v tajnosti.

Steganografie (steganography) Nauka o skrývání existence zprávy, na rozdíl od kryptografie, což je nauka o skrývání jejího obsahu.

Substituční šifra (substitution cipher) Systém šifrování, v němž je každé písmeno zprávy nahrazeno jiným znakem, ale ve zprávě zachovává svou pozici.

Šifra (cipher) Obecně jakýkoli systém pro ukrytí smyslu zprávy tak, že je každé písmeno v původní zprávě nahrazeno jiným písmenem. Systém by měl mít zabudovanou flexibilitu, známou jako klíč.**Šifrová abeceda** (cipher alphabet) Přeskupení normální (neboli otevřené) abecedy, které určuje, jak je každé písmeno v původní zprávě zašifrováno. Šifrová abeceda může také sestávat z čísel nebo jakýchkoli jiných znaků, ale ve všech případech určuje nahrazování písmen v původní zprávě.

Šifrovací algoritmus (encryption algorithm) Jakýkoli obecný proces šifrování, který může být přesně specifikován volbou klíče.

Šifrový text (ciphertext) Zpráva (neboli otevřený text) po zašifrování.

Transpoziční **šifra** (transposition cipher) Systém šifrování, v němž se každé písmeno zprávy přemístí ve zprávě na jiné místo, ale zachová si svou totožnost.

Veřejný klíč (public key) Klíč používaný odesilatelem k zašifrování zpráv v systému kryptografie s veřejným klíčem. Veřejný klíč jek dispozici veřejnosti.

Vigeněrova šifra (Vigeněre cipher) Polyalfabetická šifra vyvinutá okolo roku 1500. Vigeněrův čtverec obsahuje 26 samostatných šifrových abeced, z nichž každá je jednou z Caesarových posunutých abeced. Klíčové slovo určuje, která abeceda šifry bude použita pro

zašifrování konkrétního písmene ve zprávě.

Výměna klíčů Diffie-Hellman-Merkle (Diffie-Hellman-Merkle key ex-change) Proces, jehož pomocí mohou odesilatel a příjemce otevřeným kanálem ustavit tajný klíč. Jakmile k tomu dojde, odesilatel může použít k zašifrování například šifru DES.

Zakódovat (encode) Převést otevřený text v zakódovaný text.

Zašifrovat (encipher) Převést otevřený text v šifrový text.

Poděkování

Během psaní této knihy jsem měl tu čest setkat se s některými z největších žijících tvůrců i luštitelů kódů, počínaje těmi, kteří pracovali v Bletchey Park, až po ty, kteří vyvíjejí šifry, jež obohatí informační věk. Chtěl bych poděkovat Whitfieldu Diffiemu a Martinu Hellmanovi, kteří mi ve slunné Kalifornii věnovali čas a vysvětlili mi svou práci. Podobně mi byli Clifford Cocks, Malcolm Williamson a Richard Walton neobyčejně nápomocni během mé návštěvy pošmourného Cheltenhamu. Zvláště jsem vděčný organizaci Information Security Group na Royal Holloway College v Londýně, která mi umožnila zúčastnit se kurzu M.Sc. o informační bezpečnosti. Profesoři Fred Piper, Simon Blackburn, Jonathan Tuliani a Fauzan Mirza mi dali hodnotné lekce o kódech a šifrách.

Ve Virginii jsem se těšil společnosti experta na záhady Petera Viemeis-tera, který mě zasvěceně provedl po místech spojených s domnělým pokladem T. Beala. Bedford County Museum a Stephen Cowart z Beale Cypher and Treasure Association mi pomohli uskutečnit rešerši na toto téma. Rovněž jsem zavázán Davidu Deutschovi a Michele Moscové z Oxford Centre for Quantum Computation, Charlesů Bennettovi a jeho výzkumné skupině v Thomas J. Watson Laboratories ze společnosti IBM, Stephenu Wiesne-rovi, Leonardu Adlemanovi, Ronaldu Rivestovi, Paulu Rothemundovi, Jimovi Gilloglymu, Paulu Leylandovi a Neilu Barrettovi.

Derek Taunt, Alan Stripp a Donald Davies mi laskavě vysvětlili, jak Blet-chley Park rozlomil Enigmu. Pomohl mi také Bletchley Park Trust, jehož členové pravidelně přednášejí na rozmanitá témata. Dr. Mohammed Mra-yati a Dr. Ibrahim Kádi se podíleli na odhalování některých raných objevů arabských kryptoanalytiků a byli tak laskaví, že mi poslali příslušné dokumenty. Periodikum *Cryptologia* otisklo články o arabských kryptoanalytických, stejně jako o dalších kryptografických tématech; rád bych poděkoval Brianovi Winkelovi, který mi poslal starší čísla časopisu.

Rád bych doporučil čtenářům, aby navštívili National Cryptologic Museum ve Washingtonu, D. C. a Cabinet War Rooms v Londýně. Doufám, že budete stejně fascinováni, jako jsem byl během své návštěvy i já. Mé pode-kování patří kurátorům a knihovníkům těchto muzeí za pomoc s mým výzkumem. Když mě tlačil čas, James Howard, Bindu Mathur, Pretty Sagoo, Anna Singh a Nick Shearing mi pomáhali objevovat důležité a zajímavé články, knihy a dokumenty. Za jejich úsilí jsem jim vděčný. Mé díky také směřují k Anthonymu Buonomo z www.vertigo.co.uk, který mi pomohl vytvořit mou webovou stránku.

Stejně jako na rozhovorech s experty jsem byl závislý i na početných knihách a článcích. Seznam doporučené literatury obsahuje některé z těchto zdrojů, ale nejde ani o kompletní bibliografii, ani o úplný seznam referencí. Obsahuje pouze materiál, který by mohl být pro běžného čtenáře zajímavý. Ze všech knih, na které jsem během svého výzkumu narazil, bych rád vybral obzvláště jednu: *The Codebreakers* od Davida Kahna. Tato kniha dokumentuje téměř každou kryptografickou epizodu v historii a jako taková je neocenitelným zdrojem.

Různé knihovny, instituce a jedinci mi poskytli fotografie. Všechny zdroje jsou vyjmenovány v příslušném odstavci, ale zvláštní díky směřují k Sally McClainové za to, že

mi poslala fotografie navažských mluvčích kódu, k profesorce Evě Brannové za objev jediné známé fotografie Alice Ko-berové, k Joan Chadwickové za zaslání fotografie Johna Chadwicka a k Brendě Ellisové za to, že mi umožnila půjčit si fotografii Jamese Ellise. Díky také patří Hughovi Whitemorovi, který mi dovolil použít citát z jeho hry *Breaking the Code*, založené na knize Andrewa Hodgese *Alan Turing - The Enigma*.

Vřelým tónem bych chtěl poděkovat přátelům a rodině, kteří se mnou měli trpělivost po dva roky, kdy jsem psal tuto knihu. Neil Boynton, Dawn Dzedzy, Sonya Holbraad, Tim Johnson, Richard Singh a Andrew Thompson mi pomáhali udržet si dobrou duševní kondici, když jsem bojoval s komplikovanými kryptografickými koncepty. Zvláště Berna-dette Alvesová mi dodávala bohatou směs morální podpory a vnímavé kritiky. Když pohlížím zpět do minulosti, mé díky také směřují ke všem institucím a lidem, kteří formovali moji kariéru, včetně Wellington Scho-ol, Imperiál College a High Energy Physics Group v Cambridge University; včetně Dany Purvisové z BBC, která mi umožnila vstup do světa televize, a Rogera Highfielda z *Daily Telegraph*, který mě podporoval v psaní mých prvních článků.

Nakonec musím říci, že jsem měl to obrovské štěstí pracovat s některými nejlepšími lidmi ve vydavatelské branži. Patrick Walsh je literární agent s láskou k vědě, se zájmem o své autory a s bezmezným entuziasmem. Spojil mě s nejlaskavějšími a nejschopnějšími vydavateli, mezi nimiž musím

jmenovat především Fourth Estate, jejichž pracovníci vydrželi můj stálý proud dotazů s velkým elánem. Závěrečné a samozřejmé nikoli nejmenší poděkování patří mým editorům Christopheru Potterovi, Leo Hollisovi a Peternelle van Arsdale, kteří mi pomohli projít cestu tématem, jež pokrývá přes tři tisíce let. Jsem jim za to neskonale vděčný.

Doporučená literatura

Následuje seznam knih zaměřených na běžného čtenáře. Vyhýbal jsem se detailnějším technickým referencím, ale některé z uvedených textů obsahují podrobnější bibliografii. Pokud se například chcete dozvědět více o rozluštění lineárního písma B (kapitola 5), doporučil bych vám *The Deci-pberment ofLinear B* odjohna Chadwicka. Ale pokud by tato kniha nebyla pro vaše účely dostatečně podrobná, pak se prosím podívejte do seznamu referencí, který obsahuje.

Na Internetu je velké množství zajímavého materiálu, který se vztahuje ke kódům a šifrám. Kromě seznamu knih jsem proto vytvořil seznam několika webových stránek, jež se vyplatí navštívit.

Obecné publikace

Kahn, David. *The Codebreakers* (New York: Scribner 1996). Historie šifer na 1 200 stránkách. Úplný přehled kryptografie až do 50. let 20. století.

Newton, David E. *Encyclopedia ofCryptology* (Santa Barbara, CA: ABC-Clio, 1997). Užitečná příručka obsahující jasný a ucelený výklad většiny aspektů starověké a moderní kryptologie.

Smith, Lawrence Dwight. *Cryptography* (New York: Dover 1943). Vynikající úvod do kryptografie s více než 150 problémy k vyřešení. Vydavatelství Dover publikuje mnoho knih o kódech a šifrách.

Beutelspacher, Albrecht. *Cryptology* (Washington, D. C: Mathematical As-sociation of America, 1994). Vynikající přehled tematiky od Caesarovy šifry po kryptografii s veřejným klíčem, zaměřený spíše na matematiku než na historii. Zároveň jde o kryptografickou knihu s nejlepším známým podtitulem: *Úvod do vědy a*

*uměni šifrování, kódování, utajování, skrývání a střežení, napsaný beze všech tajemných švindlů, avšak nikoli bez mazaných žertíků pro potěšení a poučení široké veřejnosti.***Kapitola 1**

Gainesová, Helen Fouché. *Cryptanalysis* (New York: Dover 1956). Studie o šifrách a jejich řešeních. Vynikající úvod do kryptoanalýzy obsahuje v dodatku užitečné frekvenční tabulky.

Al-Kadi, Ibrahim A. The origins of cryptology: The Arab contributions. In *Cryptologia,* vol. 16, no. 2 (April 1992), pp. 97-126. Rozbor nedávno nalezených arabských rukopisů a práce al-Kindího.

Fraser, Lady Antonia. *Mary Queen ofScots* (London: Random House, 1989). Velmi dobře napsaný přehledný životopis Marie Stuartovny.

Smith, Alan Gordon. *The Babington Plot* (London: Macmillan, 1936). Kniha sestává ze dvou částí a zkoumá spiknutí jednak z hlediska Babingtona, jednak z pohledu Walsinghama.

Steuart, A. Francis (ed.). *Trial ofMary Queen ofScots* (London: William Hodge, 1951). Součást řady Slavné britské procesy.

Kapitola 2

Standage, Tom. *The Victorian Internet* (London: Weidenfeld & Nicolson,

1998). Příběh vynálezu a vývoje elektrického telegrafu. Franksen, Ole Immanuel. *MrBabbage's Secret* (London: Prentice-Hall, 1985).

Obsahuje rozbor Babbagovy práce na rozluštění Vigeněrovy šifry. Franksen, Ole Immanuel. Babbage and cryptography. Or, the mystery of Admirál Beauforťs cipher. In *Mathematics and Computer Simulation,* vol. 35, 1993, pp. 327-67. Detailně zaměřený článek popisující Babbagovu kryptografickou práci a jeho vazbu na kontraadmirála sira Francise Beauforta.

Rosenheim, Shawn. *The Cryptographic Imagination* (Baltimore, MD: Johns Hopkins University Press, 1997). Akademický rozbor kryptograficky zaměřených děl Edgara Allana Poea a jejich vliv na literaturu a kryptografii. Poe, Edgar Allan. *The Complete Tales and Poems of Edgar Allan Poe* (London:

Penguin, 1982). Obsahuje povídku Zlatý skarabeus.

Viemeister, Peter. *The Beale Treasure: History of a Mystery* (Bedford, VA: Hamilton's, 1997). Podrobný popis Bealových šifer napsaný uznávaným místním historikem. Obsahuje úplný text Bealovy brožury. Nejsnáze knihu získáte přímou objednávkou u vydavatele: Hamilton's, P.O.Box 932, Bedford, VA, 24523, USA.

Kapitola 3

Tuchmanová, Barbara W. *The Zimmermann Telegram* (New York: Ballantine, 1994). Čtivě napsaný přehled událostí kolem nejdůležitější šifry rozluštěné během první světové války.

Yardley, Herbert O. *The American Black Chamber* (Laguna Hills, CA: Aegean Park Press, 1931). Jadrně podaná historie kryptografie, v době svého prvního vydání kontroverzní bestseller.

Kapitola 4

Hinsley, F. H. *British Intelligence in the Second World War: Its Influence on Stratégy and Operations* (London: HMSO, 1975). Původní souhrn zpravodajských

operací během druhé světové války včetně popisu role zpráv Ultra.

Hodges, Andrew. *Alan Turing: The Enigma* (London: Vintage, 1992). Život a dílo Alana Turinga. Jedna z nejlepších biografií vědce, jež byly kdy napsány.

Kahn, David. *Seizing the Enigma* (London: Arrow, 1996). Kahnova historie bitvy o Atlantik a role kryptografie v ní. Obzvlášť dramaticky líčí krádeže kódových knih z německých ponorek, tzv. „čórky", jež pomáhaly kryptoanalytikům v Bletchley Parku.

Hinsley, F. H. a Stripp, Alan (eds). *The Codebreakers: The Inside Story of Bletchley Park* (Oxford: Oxford University Press, 1992). Sbírka zasvěcených esejů napsaných muži a ženami, kteří byli součástí největšího kryptoa-nalytického výkonu v dějinách.

Smith, Michael. *Station X* (London: Channel 4 Books, 1999). Kniha vycházející ze stejnojmenného televizního seriálu britské stanice Channel 4 obsahuje různé historky ze života v Bletchley Parku, místa známého také jako Station 9.

Harris, Robert. *Enigma* (London: Arrow, 1996). Román ze života kryptoanalytiků v Bletchley Parku.

Kapitola 5

Paulová, Doris A. *The Navajo Code Talkers* (Pittsburgh, PA: Dorrance, 1973). Kniha zasvěcená památce navažských mluvčích kódu a jejich příspěvku ve válce.

McClainová, S. *The Navajo Weapon* (Boulder, CO: Books Beyond Borders, 1994). Poutavý souhrn celého příběhu napsaný ženou, která strávila mnoho času v rozhovorech s tvůrci projektu navažských mluvčích kódu.

Pope, Maurice. *The Story ofDecipherment* (London: Thames & Hudson, 1975).Popis nejrůznějších rozluštění od chetitských hieroglyfů po písmo z Ugaritu, napsaný pro laického čtenáře.

Davies, W. V. *Reading the Past: Egyptian Hieroglyphs* (London: British Museum Press, 1997). Součást řady vynikajících úvodních textů publikovaných Britským muzeem. Jiní autoři této řady vydali knihy o klínovém písmu, písmu Etrusků, o řeckých písmech, lineárním písmu B, o písmu Mayů a o runovém písmu.

Chadwick,John. *The Decipherment ofLinear B* (Cambridge: Cambridge University Press, 1987). Skvělý popis vyluštění písma.

Kapitola 6

Data Encryption Standard, FIPS Pub. 46-1 (Washington, D.C.: National Bureau of Standards, 1987). Oficiální norma DES.

Diffie, Whiďield a Hellman, Martin. New directions in Cryptography. In *IEEE Transactions on Information Theory,* vol. IT-22 (November 1976), pp. 644-654. Klasický článek, v němž Diffie a Hellman zveřejnili svůj objev výměny klíčů, a otevřeli tak dveře pro kryptografii s veřejným klíčem.

Gardner, Martin. A new kind of cipher that would také millions of years to **break. In** *Scientiftc American,* vol. 237 (August 1977), pp. **120-124.** Článek, který uvedl RSA do světa.

Hellman, M. E. The mathematics of public key cryptography. In *Scientific American,* vol. 241 (August 1979), pp. 130-139. Vynikající přehled různých forem kryptografie s veřejným klíčem.

Schneier, Bruče. *Applied Cryptography* (New York: John Wiley & Sons, 1996). Vynikající přehled moderní kryptografie. Úplný, jasný a vyčerpávající úvod do problematiky.

Kapitola 7

Zimmermann, Philip R. *The OfficialPGP User's Guide* (Cambridge, MA: MIT Press, 1996). Přívětivě napsaný přehled PGP z pera autora systému.

Garfinkel, Simson. *PGP: Pretty Good Privacy* (Sebastopol, CA: CReilly & Associates, 1995). Výborný úvod do PGP a problematiky moderní kryptografie.

Bamford, James. *The Puzzle Paláce* (London: Penguin, 1983). Pohled do **nitra** National Security Agency, nejtajnější zpravodajské služby v USA.

Koops, Bert-Jaap. *The Crypto Controversy* (Boston, MA: Kluwer, 1998). Vyni-kající studie dopadu kryptografie na soukromí, občanské svobody, vy-mahatelnost práva a na obchodní sféru.

Diffie, Whitfield a Landauová, Susan. *Privacy on the Line* (Cambridge, MA: MIT Press, 1998). Politika, odposlechy, šifrování.

Kapitola 8

Deutsch, David. *The Fabric of Reality* (London: Allen Lané, 1997). Jednu z kapitol věnoval Deutsch kvantovým počítačům. Kniha spojuje kvantovou fyziku s teorií znalostí, s počítačovou vědou a evoluční teorií.

Bennett, C. H., Brassard, C. a Ekert, A. Quantum Cryptography. In *Scientific American*, vol. 269 (October 1992), pp. 26-33. Jasný výklad vzniku pojmu kvantová kryptografie.

Deutsch, D. a Ekert, A. Quantum computation. In *Physics World*, vol. 11, no. 3 (March 1998), pp. 33-56. Jeden ze čtyř článků ve zvláštním čísle časopisu *Physics World*. *Zbylé* tři články se věnují kvantovému zpracování informací a kvantové kryptografii, jejich autory jsou vesměs špičkové autority v oboru. Články počítají se čtenářem na úrovni vysokoškolského absolventa fyzikálního oboru a poskytují vynikající přehled o současném stavu výzkumu v dané oblasti.

Internet

Některé odkazy byly oproti originálnímu vydání knihy aktualizovány podle stavu platného na podzim 2002 (pozn. překl.).

Tajemství Bealova pokladu

http://www.roanokeva.com/stories/beale.html Odkazy na stránky věnované Bealovým šifrám.

Bletchley Park

http://www.retrobeep.com/

http://www.bletchleypark.org.uk/

http://www.codesandciphers.org.uk/

Počítačové muzeum v Bletchley Park, oficiální stránky Bletchley Park

Trust a obsáhlý web věnovaný činnosti Bletchley Parku.

Stránka Alana Turinga

http://www.turing.org.uk/turing/

Emulátory Enigmy

http://www.xat.nl/enigma/

http://www.users.globalnet.co.uk/~andlaw/engindex.htm Vynikající emulátory (první z adres obsahuje seznam většího počtu emulátorů) ukazují, jak Enigma pracovala. Liší se stupněm historické věrnosti.Phil Zimmermann a PGP

http://www.pgp.com/ Electronic Frontier Foundation

http://www.eff.org

Organizace zabývající se ochranou práv a propagací svobody

na internetu. Centre for Quantum Computation

http://www.qubit.org/ Information Security Group, Royal Holloway College

http://isg.rhbnc.ac.uk/ National Cryptologic Museum

http://www.nsa.gov/museum/index.html American Cryptogram Association (ACA)

http://www.cryptogram.org/

Asociace zaměřená na vypisování soutěží v kryptologických hádankách. *Cryptologia*

http://www.dean.usma.edu/math/pubs/cryptologia/

Čtvrtletník zabývající se všemi aspekty kryptologie.

RSA Laboratories' Frequently Asked Questions About Today's Crypto-graphy

http://www.rsasecurity.com/rsalabs/faq/index.html Yahoo! Security and Encryption Page

http://dir.yahoo.com/Computers_and_Internet/Security_and_Encryption/ Crypto Links

http://www.murky.org/cryptography/index.shtml

Poděkování za obrázky

Schémata nakreslil Miles Smith-Morris.

Hieroglyfy reprodukovány s laskavým svolením vydavatelství British Museum Press.

Znaky písma Linear B reprodukovány s laskavým svolením vydavatelství Cambridge University Press.

Obrázek 1 Scottish National Portrait Gallery, Edinburgh; Obrázek 6 Ibra-him A. Al-Kadi a Mohammed Mrayati, King Saud University, Rijád; Obrázek 9 Public Record Office, Londýn; Obrázek 10 Scottish National Portrait Gallery, Edinburgh; Obrázek 11 Cliché Bibliothèque Nationale de France, Paříž; Obrázek 12 Science and Society Picture Library, Londýn; Obrázky 20 a 25 *The Beale Treasure - History ofa Mystery* od Petera Viemeistera; Obrázek

26 David Kahn Collection, New York; Obrázek 27 Bundesarchiv, Koblenz; Obrázek 28 National Archive, Washington DC; Obrázek 29 General Research Division, The New York Public Library, Astor, Lenox and Tilden Foundations; Obrázky 31 a 32 Luis Kruh Collection, New York; Obrázek 38 David Kahn Collection, New York; Obrázky 39 a 40 Science and Society Picture Library, Londýn; Obrázky 41 a 42 David Kahn Collection, New York; Obrázek 43 Imperiál War Museum, Londýn; Obrázky 44 a 45 Soukromá sbírka Barbary Eachusové; Obrázek 47 Godfrey Argent Agency, Londýn; Obrázek 50 Imperiál War Museum, Londýn; Obrázek 51 Telegraph Group Limited, Londýn; Obrázky 52 a 53 National Archive, Washington DC; Obrázky 54 a 55 British Museum Press, Londýn;

Obrázek 56 Louvre, Paříž © Photo RMN; Obrázek 58 Department of Classics, University of Cincin-nati; Obrázek 59 Soukromá sbírka Evy Brannové; Obrázek 60 Neznámý zdroj; Obrázek 61 Soukromá sbírka Joan Chadwickové; Obrázek 62 Sun Microsystems; Obrázek 63 Stanford, University of California; Obrázek 65 RSA Data Security, Inc.; Obrázek 66 Soukromá sbírka Brendy Ellisové; Obrázek 67 Soukromá sbírka Clifforda Cockse; Obrázky 68 a 69 Soukromá sbírka Malcolma Williamsona; Obrázek 70 Network Asociates, Inc.; Obrázek 72 Penguin Books, Londýn; Obrázek 73 Thomas J. Watson Laboratories, IBM.