edice aliter

Simon **Singh**

Kniha kódů a šifer

Tajná komunikace od starého Egypta po kvantovou kryptografii

DOKOŘÁN
ARGO

edice aliter

edice aliter – svazek 9

Simon **Singh**

Kniha kódů a šifer

Tajná komunikace od starého Egypta po kvantovou kryptografii

Přeložili Petr Koubský a Dita Eckhardtová

Nakladatelství Dokořán a Argo
Praha 2017

Simon **Singh**

Kniha kódů a šifer

Tajná komunikace od starého Egypta po kvantovou kryptografii

The moral rights of the author have been asserted.
Copyright © 1999 Simon Singh
First published in the United Kingdom by Fourth Estate Limited
Translation © Petr Koubský, Dita Eckhardtová, 2003, 2009, 2017

Všechna práva vyhrazena. Žádná část této publikace nesmí být rozmnožována a rozšiřována jakýmkoli způsobem bez předchozího písemného svolení nakladatele.

Třetí vydání v českém jazyce (první elektronické).
Z anglického originálu ***The Code Book*** přeložili Petr Koubský a Dita Eckhardtová.
Odborný lektor a konzultace k terminologii Vlastimil Klíma.
Odpovědná redaktorka Michaela Tichá (Redigo).
Korektura Lucie Navrátilová (Redigo).
Obálka a grafická úprava Martin Radimecký, sazba Miloš Jirsa.
Konverze do elektronické verze Michal Puhač.
V roce 2017 vydalo nakladatelství Dokořán, s. r. o.,
Holečkova 9, 150 00 Praha 5,
dokoran@dokoran.cz, www.dokoran.cz,
jako svou 901. publikaci (267. elektronická).

ISBN 978-80-7363-850-4

Pro moji matku a otce
Sawaran Kaur a Mehnga Singh

„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 možností,
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 kryptografická 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 příslušná

česká 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 autentizace „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 64bitový 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 kryptoanalytiků se nezastavil. Už už se zdálo, že kryptografové vyhráli, neboť AES bude dost silná, ale luštitelé přišli s novým objevem, který do-

stal 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 kryptografů. 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 stanovisko

zástupci 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 Security 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-

Obrázek 1: Marie Stuartovna.

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. l. Chápal je jako konfrontaci svobody a otroctví, jako boj mezi nezávislými řeckými státy a perskými utlačovateli. Podle Herodota to bylo právě umění tajných zpráv, co zachránilo 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. l. 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 Leonida) 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 závadného. 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 (*Tithymalus 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 mikrotečku 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

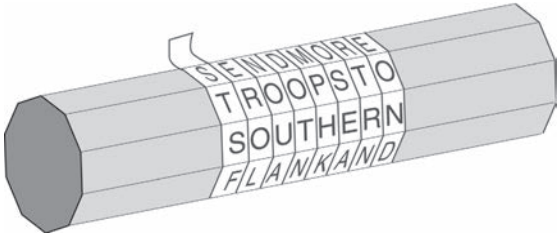
příliš bezpečný u velmi krátkých zpráv, například takových, jež sestávají z jednoho slova, protože dostupných kombinací písmen je příliš málo. Tři písmena lze například uspořádat jen šesti různými způsoby: `bok`, `bko`, `kbo`, `obk`, `okb`, `kob`. S rostoucím počtem písmen však počet variací prudce roste, 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 000krát 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:

```
BYL POZDNI VECER, PRVNI MAJ, VECERNI MAJ, BYL LASKY CAS, HRDLICCIN ZVAL
BYLPOZDNIVECERPRVNIMAJVECERNIMAJBYLLASKYCASHRDLICCINZVAL
B L O D I E E P V I A V C R I A B L A K C S R L C I Z A
Y P Z N V C R R N M J E E N M J Y L S Y A H D I C N V L
BLODIEEPVIAVCRIABLAKCSRLCIZAYPZNVCRRNMJEENMJYLSYAHDICNVL
```

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-



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. l. 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 Lysandros 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. l. 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:

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

Namísto `schuzka o pulnoci` pak odesilatel napíše `NMBETJV Q YERSQMG`. 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. Caesar 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. l. 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.

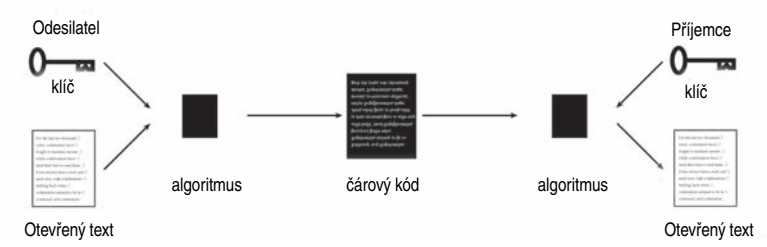
Suetonius se zmiňuje pouze o posunu o tři písmena, je však jasné, že lze použít posun o jakýkoli počet znaků od 1 do 25 a vytvořit tak 25 odlišných šifer. Kromě toho se nemusíme omezovat jen na posun abecedy. Její znaky můžeme seřadit libovolným způsobem, čímž se počet možných šifer významně zvýší. Existuje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

Otevřená abeceda	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
Šifrová abeceda	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
Otevřený text	v e n i, v i d i, v i c i
Šifrový text	Y H Q L, Y L G L, Y L F L

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. Podobně 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	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
Šifrová abeceda	J L P A W I Q B C T R Z Y D S K E G F X H U O N V M
Otevřený text	e t t u, b r u t e ?
Šifrový text	W X X H, L G H X W ?

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	**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**
Šifrová abeceda	**J U L I S C A E R T V W X Y Z B D F G H K M N O P Q**

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 nerozluštitelná, 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 posel

Boží. 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 chalífát. 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 chalífové 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-Kuttáb* (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 *monoalfabetická 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 monoalfabetickou 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. *ilm*. 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.

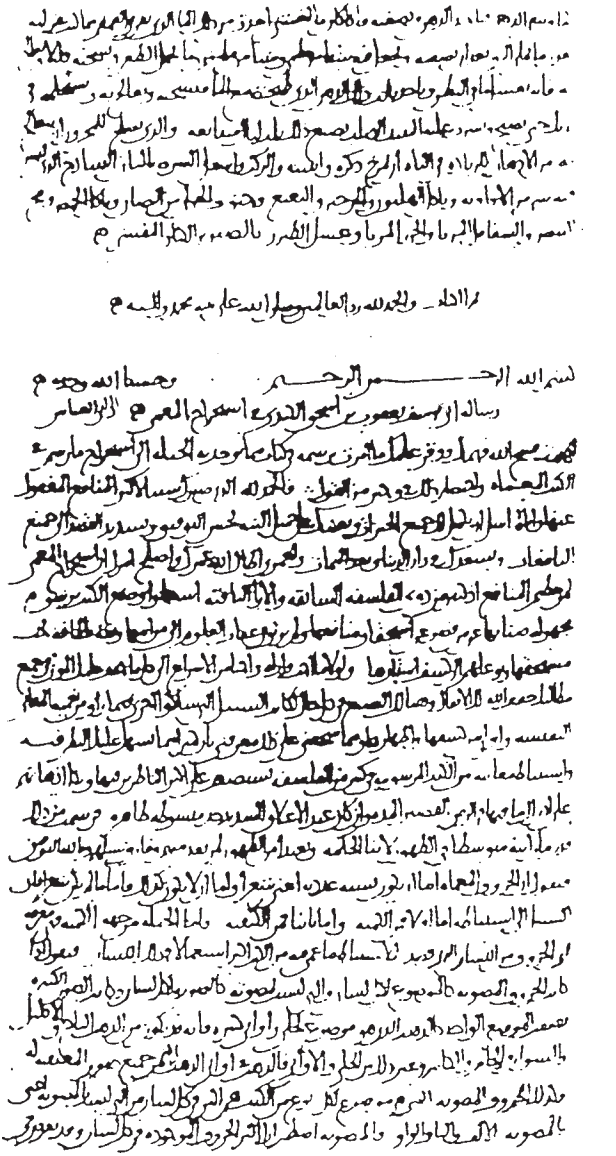
Islámská civilizace byla schopna nejen znalosti shromažďovat, ale rovněž je dále šířit – díky tomu, že od Číňanů převzala technologii výroby papíru. Tak vnikla nová profese *warraqín* neboli „ten, kdo pracuje s papírem" – jakási kopírka v lidské podobě, opisovač rukopisů, který zásoboval rychle se rozvíjející 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, Kúfě a Bagdádu se nacházely hlavní teologické školy, kde se zkoumala Muhammadova 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 *hadíth* – 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` a `l` 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 Jusúf 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 Sülajmanově osmanském archivu v Istanbulu, se nazývá *Rukopis o dešifrování kryptografických 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-li 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.



Obrázek 6: První strana *Rukopisu o dešifrování kryptografických zpráv* od al-Kindího. Text obsahuje nejstarší známý popis využití frekvenční analýzy pro luštění šifer.

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
i	7,0	**v**	1,0
j	0,2	**w**	2,4
k	0,8	**x**	0,2
l	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 *Cipher 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 čtyřnožců v Africe nebude přímočarou frekvenční analýzou snadno řešitelná: „From Zanzibar to Zambia and Zaire, ozone zones make zebras run zany 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 PYDBLK

Představte 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 `O` 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 `aov`.

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		Znak	Frekvence	
	Počet výskytů	V procentech		Počet výskytů	V procentech
A	3	0,9	N	3	0,9
B	25	7,4	O	38	11,2
C	27	8,0	P	31	9,2
D	14	4,1	Q	2	0,6
E	5	1,5	R	6	1,8
F	2	0,6	S	7	2,1
G	1	0,3	T	0	0,0
H	0	0,0	U	6	1,8
I	11	3,3	V	18	5,3
J	18	5,3	W	1	0,3
K	26	7,7	X	34	10,1
L	25	7,4	Y	19	5,6
M	11	3,3	Z	5	1,5

Tabulka 2: Frekvenční analýza zašifrované zprávy.

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

O = 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 O, 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 O s mnoha různými písmeny, nebo je jeho výskyt vázán na několik konkrétních písmen? Odpověď na tuto otázku nám napoví, zda O 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 O, X a P a shrnuje, jak často je nalezneme před jiným písmenem či po něm. Například O se vyskytuje před A jednou, po něm nikdy, takže první políčko tabulky má hodnotu 1. Písmeno O 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 O a X reprezentují samohlásky, zatímco P souhlásku.

	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
O	1	9	0	3	1	1	1	0	1	4	6	0	1	2	2	8	0	4	1	0	0	3	0	1	1	2
X	0	7	0	1	1	1	1	0	2	4	6	3	0	3	1	9	0	2	4	0	3	3	2	0	0	1
P	1	0	5	6	0	0	0	0	0	1	1	2	2	0	8	0	0	0	0	0	0	11	0	9	9	0

Nyní je třeba zjistit, které samohlásky se skrývají pod O a X. Pravděpodobně jde o hlásky e a a, nejběžnější anglické samohlásky, ale platí, že O = e a X = a, nebo je tomu naopak? K zajímavým vlastnostem šifrového textu patří to, že OO v něm nalezneme dvakrát, zatím-

co XX ani jednou. V angličtině se kombinace ee vyskytuje mnohem častěji než aa, takže je pravděpodobné, že O = 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 O, 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 O se vyskytuje devětkrát, zatímco po něm ani jednou. Žádné jiné písmeno nemá vůči O tak asymetrický vztah.

	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
po O	1	0	0	1	0	1	0	0	1	0	4	0	0	0	2	5	0	0	0	0	0	2	0	1	0	0
před 8	0	9	0	2	1	0	1	0	0	4	2	0	1	2	2	3	0	4	1	0	0	1	0	0	1	2

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 O = 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 LiSe KhahJaWaV haV ZCJPe EiPD
KhahJiUaJ LhJee KCPK. CP Lhe LhCMKaPV aPV IiJKL PiDhL,
QheP Khe haV ePVeV Lhe LaRe CI Sa'aJMI, Khe JCKe aPV
EiKKev Lhe DJCMPV ZeICJe hiS, KaUiPD: „DJeaL EiPD, 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, aPV 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 ZeICJe 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 kryptoanalýza 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 = l a S = 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	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
Šifrová abeceda	X - - V O I D B Y - - R S P C - - J K L M - - - - -

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 BY GEORGES 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 muselo kódovat A = a. Jakmile jsme takto stanovili celou šifrovou abecedu, můžeme dokončit luštění textu. Kryptoanalýza je hotova:

Otevřená abeceda	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
Šifrová abeceda	X Z A V O I D B Y G E R S P C F H J K L M N Q T U W

> Now during this time Shahrazad 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 have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favor of your majesty?"
>
> Epilogue, *Tales from the Thousand and One Nights*

Renesance na Západě

Mezi lety 800 a 1200 n. l. 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 *šin*, 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 et de nullitate magiae* (List o tajných dovednostech a neexistenci magie) obsahuje popis sedmi metod, jak uchovat tajemství zpráv, a varuje: „Blázen je ten, kdo sepíše 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 the Astrolabe* (Pojednání o astrolábu) uvedl několik dodatečných poznámek označených jako *The Equatorie of the Planetis* (O oběhu planet), v nichž je několik šifrovaných odstavců. Chaucerova šifra nahrazovala otevřený text symboly, například místo **b** psal **δ**. 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 Soro-

vi 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, kryptoanalytik 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 Françoisi Viètovi. 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 Viète 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 Viète 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-

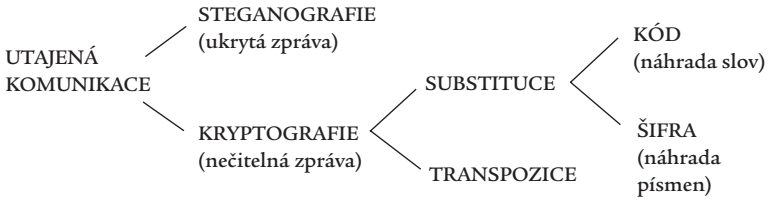
ní tzv. *klamačů* či *nul*, tedy symbolů nebo písmen, jež nereprezentují písmena původního textu (jsou to vlastně bezvýznamné vsuvky). Například můžeme nahradit každé písmeno číslem od jedné do 99, takže – pokud vezmeme v úvahu, že anglická abeceda má 26 písmen – 73 čísel neodpovídá žádnému písmenu. 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 freqenze jednotlivíh 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 odechnout 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 Tudo-

rovců. Své intriky zahájil tím, že propustil skotské šlechtice zajaté u Solway Moss – ovšem pod podmínkou, že se zasadí o sjednocení s Anglií.

Skotský 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 uprchla, 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 samo-

zřejmě 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 osob 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 nacházela, 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 roce

1585 vrátil do Anglie, byl očividně odhodlán sloužit Marii Stuartovně, a proto navštívil francouzské vyslanectví v Londýně. Tam se pro Marii hromadila korespondence. Na vyslanectví věděli, že odešlouli 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.

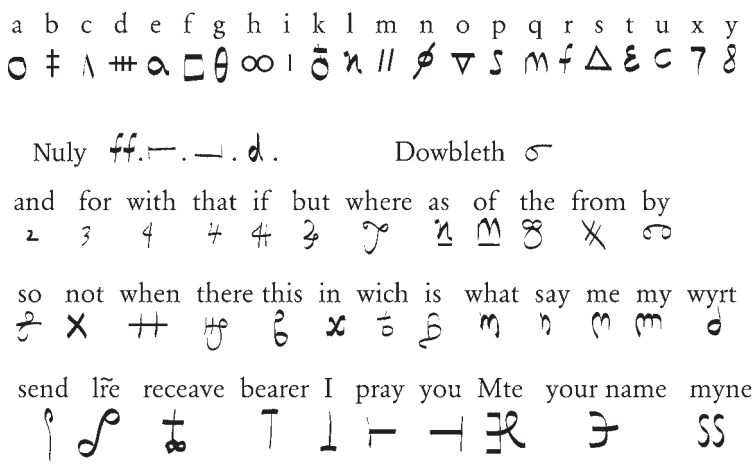
Spiknutí vzniklo jednoho večera v březnu 1586, kdy se Babington sešel se šesti důvěrnými přáteli v krčmě U pluhu poblíž Temple Bar*. Jak poznamenal historik Philip Caraman: „Silou své osobnosti a výjimečným šarmem k sobě připoutal mnoho mladých katolických gentlemanů vyznačujících se postavením, galantností, 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 Stuartovny, 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 Babingtonovi 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 (卐. —. _:. d.) a symbol ⌒, 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 Hall. 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 Girolama 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 pře-

svědčil především výkon vlámského kryptoanalytika Philipa van Marnix. Španělský král Filip II. si roku 1577 dopisoval pomocí šifer se svým nevlastním bratrem donem Juanem d'Austria, 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 tmavožlutými 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 – kryptografické 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.

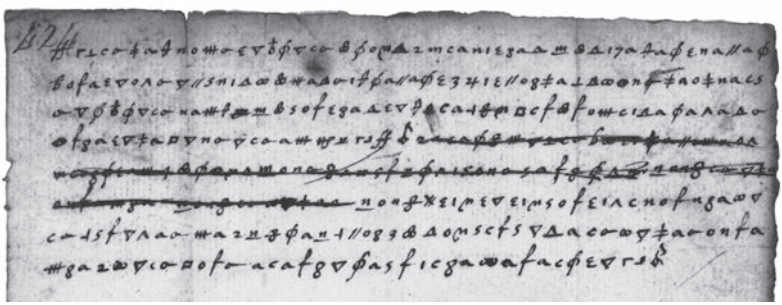
Marie odpověděla Babingtonovi 17. července a tím si doslova podepsala rozsudek smrti. Vyslovila souhlas se „záměrem" a vyjádřila starost, aby byla osvobozena před vraždou Alžběty nebo nejpozději souběžně – jinak by mohly novinky dorazit k jejímu žalářníkovi a ten by ji pak mohl zabít. Než se dopis dostal k Babingtonovi, obdržel jeho kopii Phelippes. Díky tomu, že již rozluštil předchozí

zprávy, zvládl i tuto lehce, přečetl obsah a označil ji symbolem Π – 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 Phelippesovým 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 Phelippesův 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



Obrázek 9: Padělané postskriptum, které doplnil Thomas Phelippes k Mariině zprávě, jež byla dešifrována pomocí nomenklátoru Marie Stuartovny (viz obrázek 8).

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 spolčování, 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 Babingtonem. „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 dopisů.

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 Stuartovna 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 *Narration of the Last Days of the Queen of Scots* (Vyprávění o posledních dnech královny skotské) popsal její poslední chvíle takto:

Obrázek 10: Poprava Marie Stuartovny.

„Potom tiše složila hlavu svou na špalek, ruce i nohy natáhla a několikráte odříkala In manus tuas domine, když tě 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 podvazcích, 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 monoalfabetické substituce. Bylo zřejmé, že v bitvě mezi kryptografy a kryptoanalytiky 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 kryptoanalytiky:

Otevřená abeceda	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
Šifrová abeceda 1	F Z B V K I X A Y M E P L S D H J O R G N Q C U T W
Šifrová abeceda 2	G O X B F W T H Q I L A P Z J D E S V Y C R K U H N