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

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

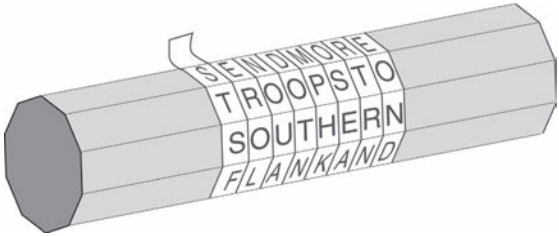
příliš bezpečný u velmi krátkých zpráv, například takových, jež sestávají z jednoho slova, protože dostupných kombinací písmen je příliš málo. Tři písmena lze například uspořádat jen šesti různými způsoby: `bok`, `bko`, `kbo`, `obk`, `okb`, `kob`. S rostoucím počtem písmen však počet variací prudce roste,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

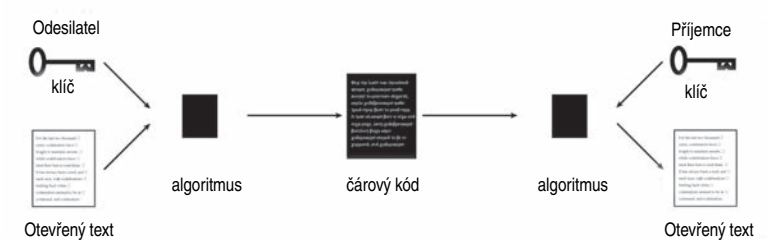
Suetonius se zmiňuje pouze o posunu o tři písmena, je však jasné, že lze použít posun o jakýkoli počet znaků od 1 do 25 a vytvořit tak 25 odlišných šifer. Kromě toho se nemusíme omezovat jen na posun abecedy. Její znaky můžeme seřadit libovolným způsobem, čímž se počet možných šifer významně zvýší. Existuje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

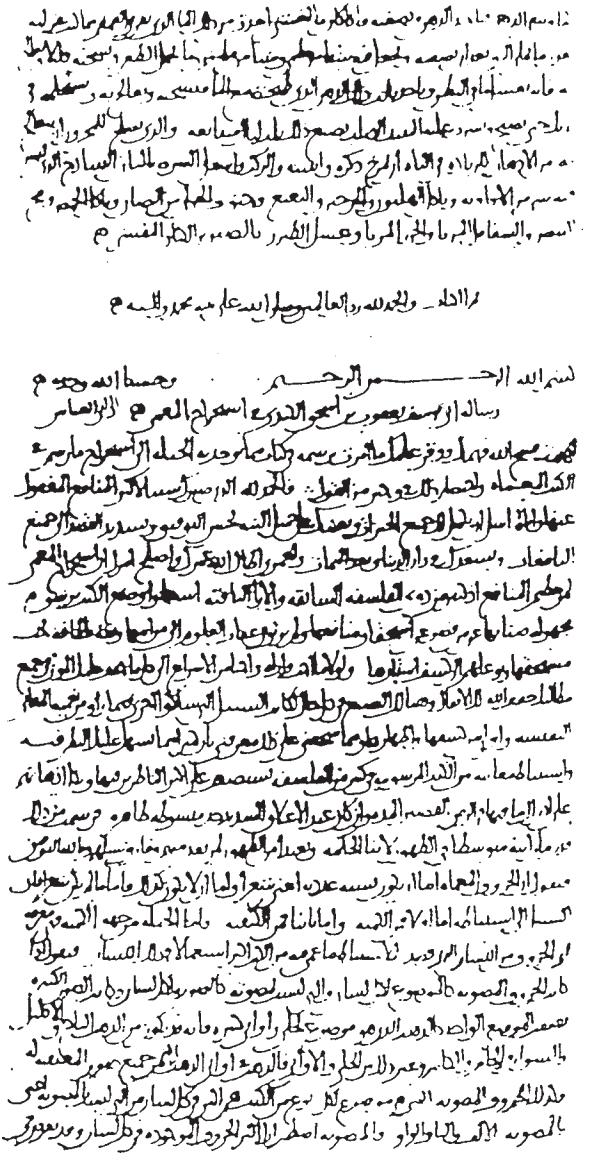
Islámská civilizace byla schopna nejen znalosti shromažďovat, ale rovněž je dále šířit – díky tomu, že od Číňanů převzala technologii výroby papíru. Tak vnikla nová profese *warraqín* neboli „ten, kdo pracuje s papírem" – jakási kopírka v lidské podobě, opisovač rukopisů, který zásoboval rychle se rozvíjející 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