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

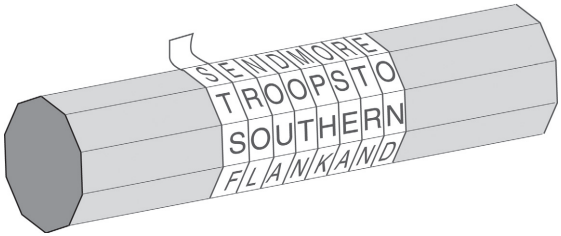
příliš bezpečný u velmi krátkých zpráv, například takových, jež sestávají z jednoho slova, protože dostupných kombinací písmen je příliš málo. Tři písmena lze například uspořádat jen šesti různými způsoby: **bok**, **bko**, **kbo**, **obk**, **okb**, **kob**. S rostoucím počtem písmen však počet variací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

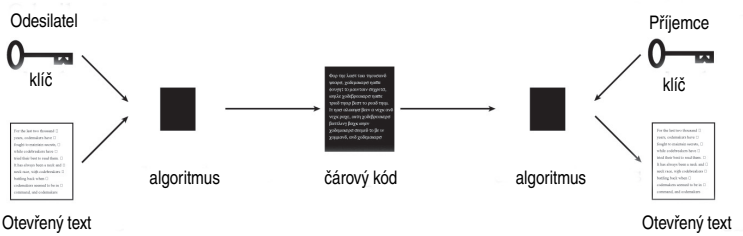
Suetonius se zmiňuje pouze o posunu o tři písmena, je však jasné, že lze použít posun o jakýkoli počet znaků od 1 do 25 a vytvořit tak 25 odlišných šifer. Kromě toho se nemusíme omezovat jen na posun abecedy. Její znaky můžeme seřadit libovolným způsobem, čímž se počet možných šifer významně zvýší. Existuje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