Jemný úvod do kryptografie

Jan Přikryl

12. prosince 2013

Toto je vývojová verze dokumentu. Obsahuje první kapitolu rozepsaných skript pro předmět 11KZK ve formě, v jaké se nacházela k datu, uvedenému nahoře.

Historie úprav:

1.1.2011	jprk	Zrestaurovaná první verze po vykradení auta na základě jakéhosi PDF, které náhodou přežilo.
25.11.2013	jprk	Opravy v historii šifrování.
12.12.2013	jprk	Doplněno rozptýlení a zmatení informace.

Obsah

V této kapitole si vysvětlíme základní pojmy z oblasti kryptologie, vysvětlíme pojem šifry, ukážeme si, jak fungují jednoduché šifry a jaké zásady musí korektně navržená šifra splňovat, abychom o ní mohli prohlásit, že je bezpečná. Další informace nalezne čtenář v Mollinově monografii [Mol01, Mol07] či v textu pánů Paara a Pelzla [PP10], případně ve Cvrčkově textu [Cvr05].

1 Základní pojmy

Vědní obor nazývaný *kryptografie*[1] studuje metody utajení srozumitelného obsahu zpráv pomocí převodu na obsah nečitelný či nesrozumitelný takovým způsobem, že pouze zamýšlený příjemce zprávy je schopen toto utajení odstranit a zprávu si přečíst. Zprávu s takto utajeným obsahem nazýváme *kryptogram*. Kryptogram vznikne transformací *nešifrovaného textu* na text *zašifrovaný*. Nešifrovaný text se v literatuře někdy označuje také jako čistý text, hladký text nebo prostý text. Metody transformace nešifrovaného textu na text šifrovaný nazýváme *šifry*, nastavení šifry pro danou situaci udává tak zvaný *klíč*. Proces vzniku kryptogramu z nešifrovaného textu nazýváme *šifrování*, jeho převod ze zašifrované formy nazýváme *dešifrování*.

Příklad 1. *Alice chce poslat Bobovi zprávu* DNESKA MAJI V MENZE DOBRY OBED. *Z hladkého textu vynechá mezery a hladký text zašifruje transpoziční šifrou s posunem 1. Výsledek bude* EOFTLBNBKJWNFOAFEPCSZPCFE. *V tomto případě je šifrou přepisující i-tý znak* a_i *na znak* b_i *předpis*

$$b_i \leftarrow (a_i + k) \bmod 26,$$

kde klíč k *udává transpoziční posun. Bob obdrží zprávu, ví, že dnes bude Alice používat kód* $k = 1$ *a zašifrovaný text dešifruje pomocí předpisu*

$$a'_i \leftarrow (b_i - k) \bmod 26.$$

Vyjde mu DNESKAMAJIVMENZEDOBRYOBED.

Zatímco na jedné straně se lidé snaží navrhovat co nejkvalitnější šifry, jež zajistí bezpečné utajení předávané zprávy, rozvíjí se i vědní obor, jehož hlavním cílem je odhalovat slabiny v navržených šifrovacích algoritmech a umožnit dešifrování zprávy. Tento vědní obor se nazývá *kryptoanalýza*. Vědní disciplína, zastřešující jak kryptografii, tak i kryptoanalýzu, se nazývá *kryptologie*.

Příklad 2. *Alice s Bobem pro zašifrování své komunikace používají stále tu samou transpoziční šifru s posunem 1. Zdeněk, který jejich zprávy odposlouchává, postupně odhalí, že v zašifrovaném textu odpovídá písmeno* F *písmenu* E *v nezašifrovaném textu a že to samé platí pro pár* B *a* A. *Odhadne proto, že by mohlo jít o transpoziční šifru s posunem 1 a na příští zprávě tuto teorii vyzkouší. Vyjde mu* DNESKAMAJIVMENZEDOBRYOBED.

[1] Z řeckého *cryptós* (skrytý) a *gráphein* (psát)

2 Trocha historie

Nejstarší známé použití kryptografických technik je známé ze starého Egypta z doby přibližně před 4500 lety. Egyptský písař tehdy do kamenných stěn jisté hrobky vytesal nápisy, v nichž použil velmi jednoduchou substituci (permutaci znaků) u hieroglyfů. Dnes předpokládáme, že nešlo o pokus utajit obsah zprávy, mnohem spíše šlo o snahu pobavit a zaujmout vzdělané čtenáře, či dodat zapsaným textům větší váhu. Podobné rysy nesou i dochované destičky s klínovým písmem z dob Mezopotámské říše. Později, někdy v 6. či 5. století př.n.l., používají Hebrejští učenci jednoduché monoalfabetickoé substituční šifry (například Atbash, zmíněný v Příkladu 4). Kryptografie má dlouhou tradici využití v raných religiózních textech, obsahujících v mnoha případech výroky, jež mohly znít pro tehdejší kulturní a politickou elitu urážlivě. Asi nejčastěji zmiňovaným je v této souvislosti číslo 666 (číslo šelmy, angl. *number of the beast*), objevující se v knize Zjevení v Novém zákoně. V textu zmíněné číslo označuje jednoznačně nějakou osobu, většina badatelů předpokládá, že se jedná o odkaz na Římskou říši či přímo na římského císaře Nera (a tedy na původce represí vůči v tehdejší době se rozšiřujícímu křesťanství). Význam použití čísla místo reference spočívá v tom, že zasvěcení věděli, koho číslo označuje, ale číslo samo o sobě umožňovalo tuto vědomost do jisté míry popřít[2].

Z doby tzv. klasického období starověkého Řecka se nám zachovaly zmínky o použití jednoduchých šifer. Ve starověké Spartě jde o *scytale*, transpoziční šifru používaná údajně vojenskými kruhy (dnes se vedou spory o to, jestli šlo opravdu o šifru, nebo jestli šlo o nástroj k ověření autenticity posílané zprávy). Z doby helénské potom pochází *Polybiův čtverec*, nástroj sloužící pro transkripci zprávy do číselného kódu, kde vlastní šifra je dána polohou písmen ve čtvercové mřížce. Polybiův čtverec si ukážeme v Příkladu 7.

Pravděpodobně díky textové analýze Koránu byla v arabském světě v období okolo roku 1000 vypracována metoda *frekvenční analýzy* textu, použitelná i pro analýzu jednoduchých monoalfabetických substitučních šifer. Proti této metodě nebylo v podstatě obrany až do doby rozvoje substitučních polyalfabetických šifer v 15. a 16. století (základem je práce Leona Battisty Albertiho o použití různých šifrovacích abeced pro různé části zprávy a tak zvaná Vigen'erova šifra) a mnoho šifer bylo s pomocí této metody analyzováno a prolomeno i později. Frekvenční analýza textu je považována za zásadní průlom v kryptoanalýze až do období druhé světové války.

V přímém důsledku politické soutěživosti a náboženské revoluce se kryptografie postupně (a tajně) stává velmi důležitým oborem. Například, v období renesance to byli občané různých italských států, včetně papežského státu a činovníků římskokatolické církve, kdo byl zodpovědný za rychlé rozšíření kryptografických technik, z nichž ale jen několik odráží pochopení (nebo alespoň znalost) Albertiho průlomové práce. Tehdejší „pokročilé šifry", a to i poté, co Albertiho práce vešla v širší známost, nebyly rozhodně tak pokročilé, jak jejich vynálezci a uživatelé tvrdili (a patrně i sami věřili). Tato přemíra optimismu může být kryptografii určitým

[2] Trochu to připomíná dnešní *ilegální čísla*, tedy čísla, obsahující utajované informace a obchodní tajemství, jako je například šifrovací klíč k DVD či Blu-ray diskům

způsobem vlastní i dnes, neboť jak v tehdejší době, tak i dnes spočívá zcela zásadní obtíž kryptografie v rozpoznání toho, jak zranitelný váš šifrovací systém ve skutečnosti je.

Kryptografie, kryptoanalýza a zrada tajného agenta a kurýra byly tři klíčové prvky, které vedly k odhalení Babingtonova spiknutí za vlády britské královny Alžbety I. a k popravě skotské panovnice Marie Stewartovny (dnes ovšem historici soudí, že celé spiknutí bylo zosnováno právě královnou Alžbětyou s cílem zbavit se definitivně uvězněné Marie). Zašifrovaná zpráva z období života Muže se železnou maskou, dešifrovaná teprve na konci 19. století Étienne Bazeriesem, částečně naznačuje identitu tohoto legendárního a záhadného francouzského vězně.

Mimo střední východ a Evropu se kryptografie do 19. století nijak výrazně nerozvíjela. Z Japonska přichází první zmínky o šifrování někdy začátkem 16. století, a pokročilé techniky šifrování se v zemi rozvíjejí az po prolomení izolace země po roce 1860.

Ačkoliv má kryptografie dlouhou a složitou historii, teprve v 19. století se začíná systematicky rozvíjet a překonávat do té doby používané ad hoc přístupy k šifrování a kryptoanalýze. Prvním moderním kryptoanalytikem je patrně Charles Babbage (muž, jenž navrhl první mechanický počítač) a jeho práce na matematické analýze polyalfabetických šifer z období Krymské války. V oblasti tvorby šifer se v té době znalosti návrhářů omezovaly na množinu obtížně vydobytých empirických pravidel, jako jsou například Kerckhoffsovy principy, uváděné v Odstavci 4. Jedním z prvních systematických luštitelů šifer byl i básník Egdar Allan Poe, jenž vybízel veřejnost k tomu, aby mu zasílala své kryptogramy k rozluštění. Jeho úspěch lze připsat výjimečným analytickým a literárním schopnostem a také tomu, že i okolo roku 1840 lidé stále věřili, že k utajení informace stačí jednoduchá substituční šifra.

Kryptografie a její zneužití v mocenském boji stojí za francouzským politickým skandálem z přelomu 19. a 20. století, známé *Dreyfusově aféře*. Na štěstí pro Alfreda Dreyfuse, kryptografové (a matematičtí statistici) přispěli k odhalení machinací, které vedly k vykonstruovanému obvinění a Dreyfus byl po několika letech osvobozen.

V době první světové války kryptoanalytici britské Admirality (velení Královského námořnictva) četli německé námořní kódy, a získané informace přispěly mimo jiné ke změnám plánů britské Velké flotily v námořních bitvách v Severním moři – u písčiny Dogger Bank v roce 1915 a u Jutska v roce 1916. Hlavním úspěchem Britů je ovšem dekódování tak zvaného Zimmermanova telegramu z roku 1917, v němž tehdejší německý ministr zahraničí navrhoval představitelům Mexika, aby Mexiko za jistých podmínek vstoupilo do války po boku Německa.

V roce 1917 navrhl Gilbert Vernam, technik Bellových laboratoří, elektromechanický šifrovací stroj založený na dálnopisu, u něhož se šifrovací klíč četl z děrné pásky a kombinoval se znak po znaku s textem šifrované zprávy. Tento objev zahájil éru elektromechanických šifrovacích strojů a vedl k návrhu jediného systému šifrování, než nelze prolomit – tak zvané *jednorázové šifry*, o níž bude řeč v Odstavci 3.3.

Kryptoanalytici amerického námořnictva (po roce 1940 spolu s britskými a holandskými kolegy) prolomili několik šifrovacích systémů používaných japonským

námořnictvem. Znalost jedné z těchto šifer, označované jako JN-25, vedla k vítězství americké Tichomořské flotily v bitvě u atolu Midway v roce 1942. Američané přitom již před vstupem spojených států do války prolomili nejtajnější japonskou diplomatickou šifru, tak zvaný *Purpurový kód*, produkovaný elektromechanickým strojem s krokovým voličem, jenž byl Američany označen kódovým názvem PURPLE. Rozluštili tak i zprávy naznačující, že dojde k útoku na Pearl Harbor.

Německé vojsko používalo také několik mechanických implementací jednorázové šifry, založených na dálnopisech firmy Lorenz. Šifrám se proto také často říká *Lorenzovské šifry*. Britští kryptoanalitici nazývali nejrozšířenější šifrovací stroj *Tunny*, tuňák (patrně proto, že celý šifrovaný dálnopisný provoz byl označován kódem Fish), a k jeho analýze sestrojili Colossus, první digitální programovatelný elektronický počítač na světě (Colossus byl po válce na přímý vládní rozkaz zničen, patrně proto, aby sovětští pozorovatelé nezjistili, jakým způsobem dokázali spojenci číst německou korespondenci – v SSSR se podobný typ šifer používal až do padesátých let a tyto zprávy dokázali britové číst). Německé ministerstvo zahraničí začalo používat jednorázové šifry již v roce 1919, některé zprávy čtené během druhé světové války se podařilo dekódovat díky klíčům, jichž se neopatrně zbavil jakýsi německý kurýr, zbytek šel na vrub neopatrnému používání klíčů obslužným personálem a opakování textu, šifrovaného různými klíči.

Spojenci užívané elektromechanické rotorové šifrovací stroje v druhé světové válce (TypeX, SGABA) byly podobné německé Enigmě, ovšem s výraznými vylepšeními. Není známo, že by se komukoliv podařilo za války tyto šifry prolomit.

3 Jednoduché šifry

Jak jsme viděli výše, velmi dlouhou dobu stačilo k utajení zpráv použít velmi jednoduchých metod: mnoho metod šifrování používalo různých transpozicí či substitučních tabulek.

3.1 Substituční šifry

Asi nejjednodušším způsobem utajení klasické psané zprávy jsou substituční šifry. V této šifře se nahrazuje každý znak abecedy nešifrovaného textu jiným znakem abecedy šifrovaného textu. Příjemce původní zprávu obdrží po inverzní substituci.

V dostupných zdrojích nalezeneme zmínky o čtyřech typech substitučních šifer:

- *Jednoduchá substituční šifra* (nebo také *monoalfabetická šifra*) je šifra, ve které se každý znak otevřeného textu nahradí příslušným znakem šifrovaného textu.
- *Polyalfabetická substituční šifra* sa skladá z několika jednoduchých šifer, které se postupně pro jednotlivé znaky otevřeného textu střídají. Pořadí střídání určuje klíč šifry.
- *Homofonní substituční šifra* se podobá jednoduché substituční šifře, avšak v tomto případě platí, že počet znaků v abecedě šifrovaného textu je vyšší,

než v abedecě nešifrovaného textu. Jeden znak abecedy nešifrovaného textu je pak nahrazen náhodně zvoleným znakem z několika možných znaků abecedy šifrovaného textu. Stále ovšem platí, že mezi abecedami existuje pouze surjektivní zobrazení (zobrazení „na“). Počet ekvivalentů v abecedě šifrovaného textu je dán procentuálním zastoupením výskytu daného znaku v textu – šifrovaný text má tedy v podstatě uniformní zastoupení všech znaků abecedy a je více odolný vůči frekvenční analýze.

- *Polygramová substituční šifra* je ta, ve které šifrování probíhá mezi skupinami znaků. Skupina AA může být nahrazená skupinou JH, AB skupinou DK a tak dále.

Příklad 3 (Afinní šifra)**.** *Tato šifra je složitějším příkladem monoalfabetické substituční šifry. Šifra využívá výpočtů v aritmetice modulo m, kde m udává počet znaků použité abecedy. Šifruje se písmeno po písmenu vztahem*

$$c = (ax + b) \bmod m$$

a dešifruje vztahem

$$x = a^{-1}(c - b) \bmod m$$

Prvek a^{-1} se nazývá multiplikativní inverze a jeho vlastnosti si popíšeme později. Musí platit, že a a m jsou nesoudělná, $\gcd(a, m) = 1$.

Příklad 4 (Atbaš)**.** *Atbaš je monoalfabetická substituční šifra nad hebrejsou abecedou. Je založena na principu reverze abecedy – záměny písmen alef (první písmeno abecedy) a thav (písmeno poslední), písmen beth (druhé písmeno abecedy) a šin (předposlední písmeno), a tak dále. Pro anglickou abecedu by dvojice vypadaly následovně*

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

Jedná se o zvláštní případ afinní šifry: V případě Atbaš je $a = b = m - 1$ a tedy

$$\begin{aligned} c &= ((m-1)x + (m-1)) \bmod m \\ &= (m-1)(x+1) \bmod m \\ &= -(x+1) \bmod n. \end{aligned}$$

Šifruje a dešifruje se opět písmeno po písmenu a jak vidíme výše, tak stejným vztahem

$$\begin{aligned} c &= -x - 1 \bmod m, \\ x &= -c - 1 \bmod m. \end{aligned}$$

Příklad 5 (Homofonní substituční šifra)**.** *Uvažujme, že budeme chtít zakódovat český text bez diakritiky, psaný velkými písmeny. Pro české texty může platit například následující frekvenční distribuce:*

A	B	C	D	E	F	G	H
0.1000	0.0267	0.0310	0.0554	0.1223	0.0023	0.0002	0.0151
I	J	K	L	M	N	O	P
0.0522	0.0331	0.0639	0.0501	0.0395	0.0490	0.0904	0.0321
Q	R	S	T	U	V	W	X
0.0002	0.0342	0.0554	0.0384	0.0352	0.0374	0.0002	0.0002
Y	Z						
0.0151	0.0204						

Pokud budeme uvažovat, že pro šifrovaný text použijeme dvojciferná čísla 00-99, budeme hledat takové zobrazení, jenž bude původních 26 znaků mapovat na možných 100 dvojciferných čísel. Možné řešení v tomto případě umožňuje použít 9 různých čísel pro zašifrování znaku A, 2 dvojice pro znak B, 4 dvojice pro znak C a tak dále. Jedna z možností kódové tabulky je uvedena v následující tabulce:

A	81 16 14 38 33 59 68 30 12
B	2 97
C	7 94 21 0
D	18 98 73 32 20
E	78 62 64 80 17 99 43 15 25 45 71
F	72
G	10
H	4
I	29 19 70 87 5
J	82 50 65
K	55 63 96 79 46 27
L	13 49 66 6 3
M	35 31 86 57
N	26 8 88 95
O	28 60 85 67 42 69 91 54
P	22 51 84 41
Q	93
R	39 83 40
S	9 61 77 92 89
T	90 37 44 11
U	76 56 48
V	47 23 58 53
W	52
X	75
Y	24
Z	34 74 36

Homofonní substituční šifrou získáme z textu DNESKA DO MENZY SNAD ANI NECHOD *šifrovanou zprávu* 18 26 78 09 55 81 98 28 35 62 08 34 24 61 88 16 73 14 95 29 26 80 07 04 60 32. *V použité šifře platí například, že* Y *je nahrazováno pouze symbolem* 24.

Příklad 6 (Hillova šifra)**.** *Tato šifra je příkladem polygramové substituční šifry. Šifra využívá výpočtů v aritmetice modulo m a počítá s vektorem znaků (znaky šifruje tedy po dvojicích, trojicích, či delších sekvencích). Šifruje se*

$$\mathbf{c} = \mathbf{A}\mathbf{x} \bmod m$$

a dešifruje vztahem

$$\mathbf{x} = \mathbf{A}^{-1}\mathbf{c} \bmod m$$

kde $\mathbf{A}^{-1}$ je inverzní matice k matici $\mathbf{A}$.

Příklad 7 (Polybiův čtverec)**.** *Polybiův čtverec je jednoduchá pomůcka, vyvinutá starořeckým historikem a učencem Polybiem, určená původně ke snížení počtu symbolů v předávaném textu za cenu prodloužení zprávy. Jedná se v podstatě jednoduchou substituční tabulkovou šifrou, v níž je jeden znak nešifrovaného textu šifrován jako dva znaky šifrovaného textu. Původní verze čtverce byla samozřejmě řecká, moderní anglická verze může vypadat například takto:*

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Pořadí znaků ve čtverci je možno volit libovolně. Zpráva DNES ZADNY OBED *by v tomto případě byla kódována sekvencí* 14 33 15 43 25 11 55 11 14 33 54 34 12 15 14*.*

3.2 Transpoziční šifry

Transpoziční šifry mění pouze pozice písmen ve slovech, zobrazení mezi abecedou nešifrovaného textu a abecedou šifrovaného textu je bijektivní – abecedy jsou shodné. Příjemce text dešifruje pomocí inverzního zobrazení.

Příklady jednoduchých transpozičních šifer jsou například:

- Psaní zprávy či jednotlivých slov odzadu
- Psaní shora dolů či zdola nahoru do několika řádků
- Psaní hadovitě do několika řádků
- Psaní do čtverce či spirály

Příklad 8. *Jednoduchá transpozice textu* PRILIS ZLUTOUCKY KUN UPEL DABELSKE ODY *hadovitě do několika řádků může dopadnout například takto:*

PLILUUCKUPEABSKDY
RISZTOKYNULDELEO

Složitější metody transpozice jsou například transpozice s pomocí otočné mřižky, kterou možná znáte ze skauta, nebo tak zvaná královská či jezdcova procházka po šachovnici.

Transpozice se často kombinovala s jinými metodami šifrování, velmi často jako doplněk jednoduché monoalfabetické substituční šifry, neboť rozepsáním například do sloupců se výrazně ztíží frekvenční analýza textu. Transpozice je velmi efektivní v kombinaci s metodou digrafické (obecně n-grafické) substituce, například pomocí již zmíněného Polybiova čtverce. Výsledek substituce, kde jednomu znaku nešifrované zprávy odpovídá n znaků substituční šifry se pak zašifruje pomocí transpozice. Příkladem takovéto šifry jsou německé polní šifry ADFGX a ADFGVX z období konce první světové války.

Nevýhodou kombinací transpozice s dalšími šifrovacími metodami je hlavně vyšší pracnost šifrování a dešifrování a také menší odolnost vůči chybám při přenosu zprávy (ADFGX šifra byla určena pro přenos zpráv Morseovou abecedou a znaky A, D, F, G, V a X jsou údajně snadno rozeznatelné i při špatném příjmu).

Příklad 9 (Šifra ADFGVX)**.** *Základním stavebím kamenem šifry je Polybiův čtverec o 36 prvcích, jenž umožňuje – na rozdíl od výše zmíněné verze – použít 26 znaků latinské abecedy a navíc všech deset číslic. Rozmístění znaků ve čtverci je prvním klíčem šifry:*

	A	D	F	G	V	X
A	*p*	*h*	*0*	*q*	*g*	*6*
D	*4*	*m*	*e*	*a*	*1*	*y*
F	*l*	*2*	*n*	*o*	*f*	*d*
G	*x*	*k*	*r*	*3*	*c*	*v*
V	*s*	*5*	*z*	*w*	*7*	*b*
X	*j*	*9*	*u*	*t*	*i*	*8*

Kromě toho používá šifra ještě jedno slovo jako klíč pro transpozici, my použijeme třeba KOENIG*.*

Při šifrování nejprve šifrujeme zvolený text pomocí Polybiova čtverce. Zpráva HEUTE NICHT *bude tímto prvním krokem pozměněna na* AD DF XF XG DF FF XV GV AD XG*. Kromě toho, že se dvojnásobně prodlouží délka, jedná se stále o poměrně jednoduchou substituční šifru, kterou lze snadno prolomit.*

V dalším kroku použijeme předem dohodnutý klíč pro transpozici tak, že nejprve pod klíč do sloupečků zapíšeme kódový text z prvního kroku šifry,

K	O	E	N	I	G
A	D	D	F	X	F
X	G	D	F	F	F
X	V	G	V	A	D
X	G				

a jednotlivé sloupce poté zpřeházíme tak, aby klíč pro transpozici měl jednotlivé znaky seřazené podle abecedy

E	G	I	K	N	O
D	F	X	A	F	D
D	F	F	X	F	G
G	D	A	X	V	V
			X		G

Výsledný kryptogram vznikne z transponovaného textu čtením znaků po sloupcích, v našem případě je zakódovaná zpráva tedy DD GF FD XF AA XX XF FV DG VG.

3.3 Jednorázová tabulková šifra

Princip jednorázové tabulkové šifry, nazývané podle svého objevitele Gilberta Vernama také *Vernamova šifra* spočívá v posunu každého znaku zprávy o náhodně zvolený počet míst v abecedě. To se prakticky rovná náhradě zcela náhodným písmenem a na tomto faktu je založeno tvrzení, že tato šifra je v principu nerozluštitelná.

To ovšem platí pouze v případě, že neporušíme kteroukoliv z následujících podmínek:

Klíč je tak dlouhý jako přenášená zpráva. Jiné šifrovací systémy používají kratší klíče, což znamená, že počet možných klíčů je menší než počet možných zpráv. Kratší klíč v principu umožňuje útok hrubou silou.

Klíč je dokonale náhodný. Pro návrh klíče nemůžeme použít počítačové generátory pseudonáhodných čísel, neboť jejich činnost lze poměrně snadno předvídat. Nejvhodnější je užití fyzikálních metod, jejichž základní vlastností je náhodnost (například tepelného šumu či kvantových procesů).

Klíč nelze použít opakovaně. Opakovaným použitím přestává být klíč náhodný. Dostane-li kryptoanalytik do ruky dvě zprávy zašifrované týmž klíčem, usnadní mu to cestu k rozluštění obsahu zpráv.

Hlavní nevýhodou tohoto systému je nutnost skladování velmi dlouhého a zcela náhodného klíče a s tím spojené problémy při předávání klíčů. Zatímco v nepříliš vzdálené minulosti existovaly tabulky se šiframi v papírové podobě, nyní lze pro klíče použít například napodobeniny USB flash disků či CD-ROM a DVD-ROM nosiče.

Příklad 10. *Předpokládejme, že Alice s Bobem používají jednorázovou šifru. Alice chce Bobovi předat zprávu* DNESKA DO MENZY SNAD ANI NECHOD. *Alice zprávu zašifruje náhodným řetězcem* RFVSR VXAEQ PPYNT BZQUW EVQXE OHRZLH *a Bob obdrží šifrovaný text* USZKB VAOQU COWFG BCQHE RZSES R.

4 Kerckhoffsovy principy

Holandský kryptolog Auguste Kerckhoffs publikoval v roce 1883 dva články o vojenské kryptografii, v nichž formuloval šest základních principů návrhu vojenských šifer. Tyto principy jsou následující:

1. Šifra musí být v praxi nerozluštitelná i v případě, že nelze matematicky dokázat její neprolomitelnost.

2. Princip šifry nesmí být utajován a jeho pád do rukou nepřítele nesmí být důvodem ke změně šifrovacího systému.

3. Šifrovací klíč musí být lehce sdělitelný a uchovávatelný bez nutnosti písemných poznámek. Klíč musí jít jednoduše změnit či modifikovat na přání komunikujících stran.

4. Systém musí být použitelný pro telegrafickou korespondenci.

5. Systém musí být přenosný, jeho použití a funkce nesmí vyžadovat součinnost více osob.

6. Vzhledem k okolnostem použití musí být systém jednoduchý na použití, nesmí uživatele vystavovat psychickému napětí. Celý proces šifrováhní a dešifrování musí být jednoduchý a nekomplikovaný.

Některé z těchto principů nejsou již v současné době relevantní – i v polních podmínkách dnes mají vojáci k dispozici počítače, které v Kerckhoffsově době složité úkoly šifrování a dešifrování dnes hravě zvládnou. Druhý z principů (nyní nazývaný často *Kerckhoffsův princip* případně Kerckhofsův axiom, předpoklad, či zákon) stále platí a má pro konstrukci šifer zcela zásadní význam.

Věta 1 (Kerckhoffsův princip)**.** *Kryptografický systém musí být bezpečný i v případě, kdy všechny informace o jeho funkci, kromě šifrovacího klíče, jsou veřejně známé.*

Kerckhoffsův princip je původní verzí výroku, jenž možná bez znalosti Kerckhoffsovy práce formuloval Claude Shannon: „Nepřítel zná systém“. Jedná se o výrok, jenž zásadním způsobem ovlivňuje konstrukci kryptografických systémů. Říká nám totiž, že při návrhu systému je třeba počítat s tím, že prostistrana bude dříve nebo později znát funkci celého systému a jediné, co v ten okamžik zaručí utajení přenášených informací, budou šifrovací klíče. V dnešní době je tento princip kryptografy všeobecně uznáván, na rozdíl od snah dosáhnout bezpečnosti systému naprostým utajením jeho vnitřních funkcí.

5 Zmatení a rozptýlení informace

Aby bylo možné prohlásit nějakou šifru za bezpečnou, musí z hlediska teorie informace splňovat požadavky *zmatení* a *rozptýlení* přenášené informace (angl. *confusion and diffusion*). Tyto požadavky, kladené na jakýkoliv bezpečný kryptosystém, teoreticky definoval Claude E. Shannon již v roce 1949 [Sha49].[3]

[3] Ono to vlastně bylo o pár let dříve, první verze zmíněného textu vznikla za druhé světové války a byla samozřejmě utajována.

Podle původních definic označuje *zmatení* postup, při němž se snažíme učinit vztah mezi nešifrovanou zprávou a kryptogramem tak složitý a spletitý, jak je to jen možné. *Rozptýlení* označuje statistickou vlastnost šifrovaného textu, kdy veškerá redundantní informace, obsažená v nezašifrované zprávě, je rovnoměrně rozptýlena v šifrovaném textu.

Rozptýlení informace je spojeno se závislostí bitové sekvence na výstupu na bitové sekvenci na vstupu. Pokud má šifra dobrý rozptyl, změna hodnoty jediného bitu vstupní sekvence vyvolá u každého bitu výstupní sekvence změnu jeho hodnoty s 50% pravděpodobností.

Substitutční šifry jsou mechanismem pro zmatení informace (viz například S-box šifry DES), transpoziční a permutační šifry jsou mechanismem, sloužícím k rozptýlení informace (v dnešní době se používá i jiných technik, například lineárních transformací). Moderní šifry proto ve svých algoritmech prokládají permutační a substituční kroky – výsledkem je šifrovaný text, v němž je původní informace dostatečně „zmatená a rozptýlená“.

Podívejme se na doposud probrané šifry z hlediska zmatení a rozptýlení informace: Monoalfabetické substituční šifry nevyhovují ani jednomu ze Shannonových požadavků – nedochází zde k transpozici a znaky otevřeného textu jsou nahrazovány stále stejnými znaky kryptogramu. U polyalfabetických šifer (například u zmíněněné Vigenèrovy šifry) je sice splněn požadavek zmatení informace, protože znaky otevřeného textu jsou transformovány na různé znaky šifrovací abecedy, opět zde ale nedochází k rozptýlení informace. Transpoziční šifry sice rozptylují informaci (to je dáno jejich definicí), ale ke zmatení informace u nich nedochází a pokud ano, není to nijak efektivní proces.

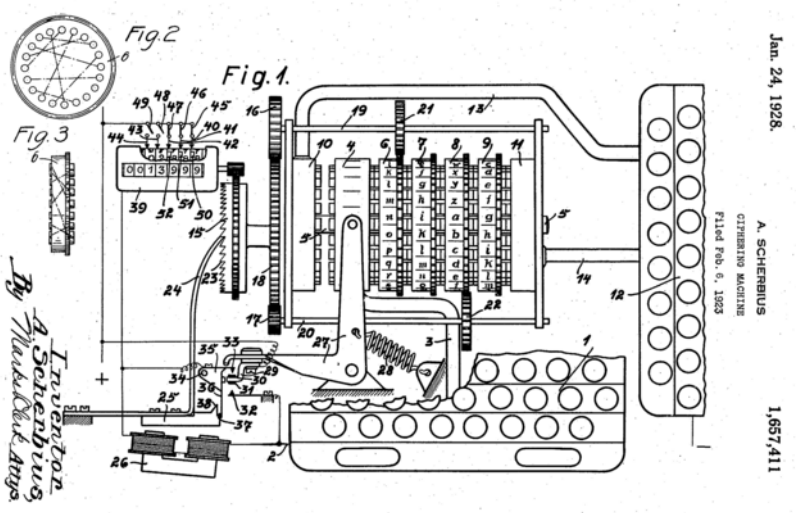
6 Zajímavé šifry dvacátého století

6.1 Enigma

Enigma je německý přenosný elektromechanický rotorový šifrovací přístroj, implementující polyfalfabetickou substistuční šifru, hojně využívaný za druhé světové války. Prakticky byla používána od dvacátých let dvacátého století a předpokládalo se, že zprávy zabezpečené její šifrou jsou velmi těžko rozluštitelné. Konstrukčně podobné systémy používaly ve své době všechny světové mocnosti.

Zcela dle Kerchoffsova principu nespočívá síla šifry Enigmy v utajení samotného přístroje, ale v utajení jeho počátečního nastavení, tedy v klíči. Chce-li kryptoanalytik dešifrovat zachycenou zprávu, musí nejprve zjistit, jaké z miliard možných počátečních nastavení použít. Německé memorandum to shrnulo slovy: „Při posuzování bezpečnosti šifrovacího systému vycházíme z předpokladu, že nepřítel má přístroj k dispozici.“

Enigma sestává z tlačítkové klávesnice, sady rotujících disků na společné ose, zajišťujících pomocí drátových propojek vlastní polyalfabetickou substituci, a krokového mechanismu, jež posunuje jeden nebo více rotorů poté, co šifrant stiskne klávesu. Rotory v sobě mají propojovací vodiče a jejich rotací se po každém stisku klávesy změní elektrické propojení definující šifrovací transformaci a provede se



Obrázek 1: Schéma zapojení šifrovacího stroje Enigma, jak jej ve své žádosti o patent popsal jeho autor, Arthur Scherbius (US patent 1,657,411).

zašifrování stisknutého písmene. Sada rotorů je ukončena tak zvaným reflektorem, jenž vrací signál z rotorů přes tu samou sadu rotorů zpět. Tento systém by sám o sobě nebyl dostatečně kryptograficky bezpečný. Dodatečné zabezpečení Enigmě dodává propojovací panel, jehož nastavení prohodí význam dvojice písmen před tím, než signál dorazí do rotorů.

Celkový počet možných počátečních nastavení pozice rotorů u třírotorové Enigmy je 17 576 (neboli 26^3). Rotorů má obsluha k dispozici celkem 5, a tři z nich vybrané lze do stroje vložit celkem v šesti různých kombinacích (123, 132, 213, 231, 312, 321), čímž se počet možných kombinací zvýší na 1 054 560 (tedy $5 \cdot 4 \cdot 3 \cdot 26^3$). Každý ze tří vložených rotorů má 26 možných pozic přenosového kroužku se zářezem, jenž má za úkol posunout následující rotor o jednu pozici, celkový počet nastavení kroužků je 676 (což je 26^2, poslední rotor nemá žádný vliv). Počet možných nastavení propojovací desky je dán počtem použitých písmen (26) a počtem propojovacích kabelů, které propojují dvojice písmen (těch bývalo většinou 10) a dosahuje celkově 150 738 274 937 250[4]. Celkový počet možných výchozích pozic, které by bylo třeba vyzkoušet při útoku hrubou silou, je tedy přes 10^{16}.

[4]Deseti kabely lze z 26 písmen propojit celkem 20, počet možných kombinací je tedy $C(26, 20)$. V každé této skupině 20 vybraných znaků máme celkem 19 možností, jak zapojit první kabel (jednu zdířku volíme jako výchozí), po zapojení prvního kabelu je celkem 17 možností, jak vést druhý kabel, a tak dále. Na poslední, desátý kabel, zůstanou volné poslední dvě zdířky a počet možností, jak jej zapojit, je 1. Celkový počet možností je proto

$$\frac{26!}{(26-2\cdot 10)!(2\cdot 10)!}\cdot 19\cdot 17\cdots 1 = \frac{26!}{6!2^{10}10!} = 150\,738\,274\,937\,250.$$

6.2 Mluvčí v kódech

Americké vojenské velení v sedmdesátých letech minulého století prohlásilo, že nejtajnější a nejúspěšnější americkou zbraní za druhé světové války v Pacifiku byli indiánští „mluvčí v kódech“ z kmene Navajo. Ještě více jak dvacet let po válce byly informace o výcviku a nasazení těchto indiánů tajné a veřejnost o vynikajících úspěších těchto mužů nic nevěděla. V současné době jsou již všechny informace uvolněny, včetně původní kódové knihy, kterou indiáni za války používali.

Řeč Navajů je velice zvláštní a obtížná, a to především svou speciální výslovností a gramatickými pravidly. Navajština v té době neměla téměř žádnou psanou literaturu, indiáni z tohoto kmene žili velice izolovaně a nekomunikovali ani s ostatními indiánskými kmeny. Na celém světě existovalo v té době údajně maximálně třicet lidí, kteří se jejich řeč naučili.

Zvukové záznamy „šifrovaných“ zpráv byly při ověřování šifry předloženy i americkým kryptologům. Ti je nebyli schopni zařadit a přepsat do správného textu. K jazyku se vyjádřili, že připomíná nejspíše hebrejštinu.

Pro přenos zpráv v šifře Navajo se používala kódová kniha, v níž byla pro jednotlivá písmena abecedy použita vybraná anglická slova začínající tímto písmenem a ta přeložena do jazyka Navajů. Pro zvýšení efektivity bylo v kódové knize pamatováno i na často používaná slova či slovní spojení. Typická kódová zpráva sestávala ze směsi otevřené řeči v dialektu Navajo, kódových slov v navajštině a případně hláskovaných anglických slov. Mluvčí v kódech byli trénováni pracovat zpaměti.

Reference

[Cvr05] Dan Cvrček. *Kryptologie a informační bezpečnost.* VUT FIT, 2005.

[Mol01] Richard A. Mollin. *An Introduction to Cryptography.* Chapman & Hall/CRC, 2001.

[Mol07] Richard A. Mollin. *An Introduction to Cryptography.* Taylor & Francis, 2nd edition, 2007.

[PP10] Christof Paar and Jan Pelzl. *Understanding Cryptography. A Textbook for Students and Practitioners.* Springer, 2010.

[Sha49] Claude E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.