Učitel matematiky

Petra Konečná

Zajímavosti z kryptologie (2) - obrana před frekvenční kryptoanalýzou

Učitel matematiky, Vol. 23 (2015), No. 2, 65–78

Persistent URL: http://dml.cz/dmlcz/149420

ZAJÍMAVOSTI Z KRYPTOLOGIE (2) OBRANA PŘED FREKVENČNÍ KRYPTOANALÝZOU

Petra Konečná

Úvod

Historie kryptologie je několik tisíc let trvajícím příběhem o souboji kryptografů a kryptoanalytiků. Kryptografové se snaží vymyslet a používat bezpečné šifry a kryptoanalytici se snaží využít slabin používaných šifer a najít metody na jejich rychlé rozluštění.

Až do prvního tisíciletí našeho letopočtu platilo, že šifra je dostatečně bezpečná, pokud je odolná proti „útoku hrubou silou“. To znamená, že pouhým zkoušením všech možností klíčů není kryptoanalytik schopen v reálném či potřebném čase správný klíč odhalit. Pokud tedy byla použita substituční šifra s dostatečným množstvím potencionálních šifrových abeced, byla tajná komunikace nerozluštitelná[1]. Zlom nastal díky arabským učencům, kteří vynalezli tzv. frekvenční kryptoanalýzu. Ta spočívá v nalezení šifrové abecedy na základě porovnání relativní četnosti znaků v šifrované zprávě a vyskytujících se písmen v daném jazyce.

Toto byl trumf kryptoanalytiků, který jim vydržel několik set let, přestože se kryptografové snažili proti frekvenční kryptoanalýze uplatňovat různé zdokonalující šifrovací postupy. Některé si nyní představíme.

Článek navazuje na [6] a opět čerpá z již citovaných zdrojů v tomto článku. Základní historické momenty a obecné informace

[1] Bezpečnou šifrou pro dlouhé zprávy byla také transpoziční šifra. Tato však nese komplikaci, jelikož pro její bezpečnost je potřeba použít vhodný klíč, tj. dostatečně nepravidelnou permutaci. Používání a distribuce takových klíčů je složitější než práce se substituční šifrou.

jsou čerpány zejména z (Singh, 2003), (Janeček, 2008) a (Piper & Murphy, 2006). O homofonní šifře jsou dále doplněny z (Berloquin, 2008). Doplňující a rozšiřující informace o šifrovacím stroji Enigma nalezneme v (Janeček, 2008).

První obranné mechanismy proti frekvenční kryptoanalýze

Přestože byla frekvenční kryptoanalýza objevena na přelomu 1. a 2. tisíciletí našeho letopočtu, evropští panovníci, politici, velitelé i papež se o existenci slabin svých šifer dověděli až v patnáctém století na základě studia arabské vědy[2]. Reagovali pomalu, stále používali zejména monoalfabetickou substituční šifru[3], kterou se snažili zdokonalit. Prvními vylepšeními této šifry byly *klamače* a *nomenklátory*. Klamače jsou znaky, které nemají žádný význam a jsou dodatečně vkládané do šifrového textu, aby zmátly kryptoanalytika, přičemž ve větším množství mohou zkreslit i četnosti znaků, čímž zkomplikují použití frekvenční kryptoanalýzy. Nomenklátor je substituční šifra, kde je šifrová abeceda doplněna ještě o seznam kódových slov odpovídajících vybraným slovům zdrojové zprávy. Text se tedy šifroval standardní substituční šifrou s tím rozdílem, že vybraným slovům byly přiřazeny samostatné symboly tzv. „kódová slova".

Uvažujme například monoalfabetickou substituční šifru s následující převodní tabulkou.

Naší zprávou bude důležitá logistická informace: ZASOBY BUDOU LODEMI DOPRAVENY 3. NOC PO UPLNKU DO BRESTU; CELKEM 100 TUN OBILI, 200 LITRU VINA, 20 DEL, 200 PUSEK A MUSKET VCETNE MUNICE. Pro vybraná stěžejní slova zavedeme speciální znaky.

[2]Je možné, že některé skupiny např. templáři frekvenční kryptoanalýzu znali dříve, ale nezveřejnili to.

[3]Například v 16. stol. španělští kryptografové, kteří stále věřili nerozluštitelnosti svých šifer, obvinili francouzského kryptoanalytika P. Babou ze spolčení s ďáblem a chtěli, aby byl povolán do Vatikánu před soud. Papež, který měl sám také přístup k rozluštěným španělským zprávám, jejich žádost zamítl a oni sami byli pro smích celé Evropě.

A	B	C	D	E	F	G	H	I	J	K	L	M
T	C	U	P	X	H	A	I	V	B	Z	D	Y

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	W	F	S	G	R	Q	O	N	L	J	M	K

1	2	3	4	5	6	7	8	9	0
0	9	8	7	6	5	4	3	2	1

Tabulka 1: Převodní tabulka pro tvorbu substituční šifry

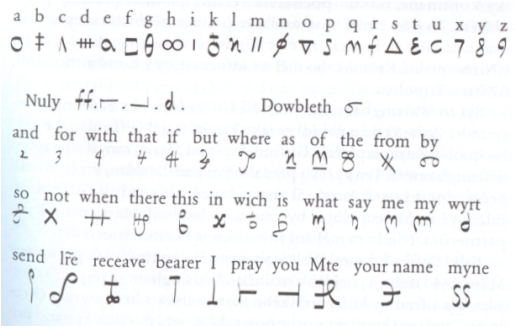
BREST	⋆
LOD	☼
OBILI	►
VINO	◄
DELO	↕
PUSKA	!!
MUSKETA	§

Tabulka 2: Seznam kódových slov

Šifra by poté vypadala následovně: KTRWCMCOPWO☼PWFGTNXEM8EWUFWOFDEZOPW⋆UXDZXY011QOE►911DVQGO◄91↕911!!§

Klamače a nomenklátory mohly kryptoanalytiky zmást a mírně při luštění zpomalit, jinak však byly proti frekvenční kryptoanalýze slabou obranou. Klamače se daly časem odhalit a kódová slova odhadnout z kontextu, často s využitím dalších informací z pozorování v terénu a od špionů. Jednou z významných osob, která doplatila na používání slabé šifry, přestože již v její době byly známé bezpečnější systémy, byla skotská královna Marie Stuartovna (1542–1587). Pro komunikaci z vězení používala právě nomenklátor a klamače a pro bezpečné doručení zprávy z vězení využívala steganografii – údajně ukrývala zprávu v kolíku sudu s vínem. Byla natolik přesvědčena o bezpečnosti své tajné komunikace, že padla do připravené pasti. Její komunikace byla zachycena a frekvenční kryptoanalýzou rozluštěna. Na zašifrovanou

zprávu, kde měla dát souhlas ke vzpouře proti Alžbětě I. a jejímu odstranění, odpověděla kladně. Tímto si podepsala rozsudek smrti.

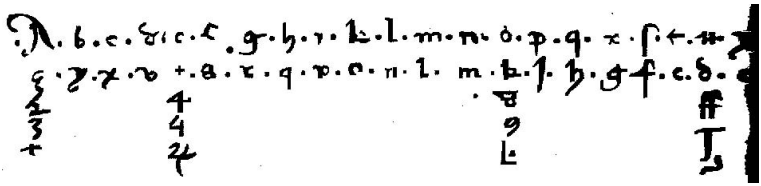


Obr. 1: Nomenklátor Marie Stuartovny s klamači (Singh, 2003)

Konečně účinná zbraň kryptografů

První účinnou reakcí na frekvenční kryptoanalýzu byla *homofonní šifra*. Nejstarší záznam využívající homofonní šifru pochází od S. de Cremy z roku 1401. Základem je použití šifrové abecedy s větším množstvím znaků, přičemž některým písmenům je přiřazováno více různých znaků. Tímto je narušena podobnost frekvence výskytu znaků zdrojové zprávy a šifrového textu. Problémem se v patnáctém století výrazně zaobíral italský architekt L. B. Alberti, který dbal na to, aby se každé písmeno nahrazovalo větším množstvím znaků, zejména ta, která se v původním textu vyskytují nejčastěji.

Ideální homofonní šifra každý jeden zdrojový znak nahrazuje skupinou různých šifrových znaků, jejichž počet je úměrný frekvenci zdrojového znaku ve zprávě. Tím se úspěšně brání frekvenční kryptoanalýze. Její slabinou je však zachování lingvistických pravidelností, opakujících se formálních náležitostí a frází ve zprávách zdrojových i šifrových. Často také nebylo nahrazování znaků aplikováno důsledně, navíc neexistovalo zabezpečení přenosu zpráv.



Obr. 2: Homofonní šifra od S. Cremy (Berloquin, 2008)

To vše vedlo k tomu, že i homofonní substituční šifra byla prolamována, velkou zásluhu na tom má francouzský matematik F. Viète.

L. B. Alberti se zasloužil nejen o zavedení homofonní substituční šifry, ale také navrhl systém pro tvorbu *polyalfabetické substituční šifry*, dokonce k tomu navrhl a sestrojil jednoduchou šifrovací pomůcku, tzv. *šifrovací disk*, vlastně první šifrovací stroj. Princip, jak už název napovídá, byl v tom, že se pro šifrování nepoužívala pouze jedna šifrová abeceda, ale hned několik.

Obr. 3: Šifrovací disk[4]

Podobným systémem se zabývali v té době také další dva významní vědci a to německý opat J. Trithemius či známý italský vědec G. Porta. Ovšem celý systém do konečné dokonalé podoby dotáhl až francouzský diplomat B. Vigenére; v roce 1586 vypracoval tzv. *Vigenérův čtverec*, který pro šifrování používá všech 26 šifrových abeced podle principu Caesarovy šifry.

[4]Zdroj `http://friedo.szm.com/CryptoloHistory.htm`

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabulka 3: Vigenérův čtverec

Pro vytvoření šifry potřebujeme klíč, zvolme si např. FRANCIE. Znaky otevřeného textu šifrujeme postupně tou abecedou, která začíná písmenem klíčového slova, který je nad ním umístěn. Tedy první písmeno šifrového textu bude ležet v průniku P-sloupce a 5. řádku, druhé v průniku O-sloupce a 17. řádku atd.

Tímto objevem se karta obrátila. Kryptografové disponovali šifrou, o které se soudilo, že je nerozluštitelná. Ano, frekvenční analýzou se šifra prolomit nedala. A nebyla prolomena dalších skoro 300 let. Podařilo se to až britskému vědci Ch. Babbageovi a pruskému důstojníkovi W. Kasiskemu[5].

Kasiského přístup ke kryptoanalýze Vigenèrovy šifry vychází z úvahy, že dvě stejné posloupnosti písmen v šifrovém textu zřejmě vznikly, až na výjimky, ze stejného slova (posloupností písmen) vyskytujícího se dvakrát v otevřeném textu a zašifrovaného v obou případech stejně. Odtud plyne, že odstup dvou stejných posloup-

[5]W. Kasiski prolomení Vigenèrovy šifry publikoval v roce 1863. Až podle nalezených záznamů Ch. Babbage se ukázalo, že šifra byla prolomena pravděpodobně o 10 let dříve právě tímto britským vědcem.

Klíč	F	R	A	N	C	I	E	F	R	A	N	C	I	E
Zpráva	P	O	L	Y	A	L	F	A	B	E	T	I	C	K
Šifra	U	F	L	L	C	T	J	F	S	E	G	K	K	O

F	R	A	N	C	I	E	F	R	A	N
A	S	U	B	S	T	I	T	U	C	E
F	J	U	O	U	B	M	Y	L	C	R

Tabulka 4: Ukázka polyalfabetické substituční šifry tvořené s pomocí Vigenérova čtverce

ností v šifrovém textu je většinou násobkem periody odpovídající délce klíče. Na základě této průlomové myšlenky lze aplikovat následující postup:

1. Hledáme opakující se sekvence znaků v šifře.
2. Určíme vzdálenosti mezi nalezenými opakujícími se sekvencemi znaků.
3. Hledáme společné dělitele těchto vzdáleností. Společní dělitelé určují potencionální délky klíče.
4. Rozdělíme text podle délky klíče do jednotlivých částí. Jednotlivé části jsou zašifrovány monoalfabetickou substituční šifrou.
5. Na každou část aplikujeme samostatně frekvenční kryptoanalýzu.

Uvedený postup je geniální a současně relativně jednoduchý (i když pracný bez použití počítače). Je postaven na základní slabině polyalfabetické substituční šifry a tou je opakující se používání šifrových abeced určených klíčem. Je zřejmé, že tato slabina by byla odstraněna, pokud by se šifrové abecedy neopakovaly. Přesně toho bylo využito v období I. světové války a vznikla naprosto bezpečná šifra, tzv. *Vernamova* neboli *jednorázová tabulková šifra*. Vtip spočívá v tom, že použijeme klíč, jehož délka odpovídá délce samotné zprávy. Tím je odstraněn problém s cyklickým opakováním šifrových abeced. Proto, aby šifra byla dokonalá, tj. naprosto bezpečná je potřeba dodržet dvě základní pravidla – klíč musí být naprosto náhodně generován a může být

použit pouze jednou. Tímto se dostáváme k důvodu, proč tato dokonalá šifra nenašla odpovídající uplatnění. Samotné generování naprosto náhodných klíčů je složité a nákladné. A bezpečná distribuce kódových knih obsahující tyto jednorázově použitelné klíče je prakticky ve větší míře nemožná. Přesto Vernamova šifra našla své důležité uplatnění, používala se na horké lince mezi prezidenty SSSR a USA v období studené války.

Šifrovací stroje

Jak jsme si již uvedli, první šifrovací stroj byl pravděpodobně šifrovací disk, který zkonstruoval již v patnáctém století J. B. Alberti. Sloužil zejména jako pomůcka pro usnadnění šifrování a dešifrování.

Za dynamickým vývojem dalších *mechanických šifrovacích strojů* stojí Kasiského metoda kryptoanalýzy polyalfabetické substituční šifry. Jelikož absolutně bezpečná Vernamova šifra nebyla pro častou tajnou komunikaci použitelná, hledal se kompromis, tzn. šifra, která by používala dostatečně dlouhý a nepředvídatelný klíč a tímto by bylo dosaženo dostatečného narušování cyklického opakování šifrových abeced.

Nejznámějším příkladem je německý šifrovací stroj Enigma používaný v průběhu II. světové války, jehož vynálezcem byl německý inženýr A. Scherbius. Nejpodstatnější součástí tohoto stroje (v základní verzi) byly tři otáčivé kotouče, které svým systémem otáčení zajišťovaly narušení cykličnosti klíče.

Šifrovací vojenská Enigma se skládala ze tří částí – klávesnice pro zadávání otevřeného textu, šifrovací jednotky a signalizačních lampiček, které zobrazovaly zašifrovaný text. Nejdůležitější součástí stroje jsou disky (rotory). Scherbius ke stroji přidal ještě část zvanou reflektor. Ten odráží signál, který projde přes tři disky a vrací ho přes ně zase zpátky, avšak ne na klávesnici, nýbrž na signální desku. Šifrování a dešifrování jsou zrcadlové postupy a reflektor zajistil jednoduchost dešifrování.

Celkový počet možných nastavení Enigmy byl tedy závislý na nastavení disků (263 možností), uspořádání disků (3! možností) a nastavení propojovací desky (100 391 791 500 možností).

Obr. 4: Enigma[6]

Odolnost stroje spočívá v kombinaci propojovací desky s otáčivými disky. Samotná propojovací deska zajišťuje velký počet možných klíčů, avšak nedělá nic jiného než monoalfabetickou substituci. Tudíž snadno podlehne frekvenční kryptoanalýze. Na druhou stranu disky produkují jen 17 576 možných kombinací, které lze teoreticky v relativně krátkém čase vyzkoušet. Avšak díky pravidelnému otáčení odolá šifra právě frekvenční analýze.

I přes důmyslnost šifrovacích strojů, byla většina těchto šifer v průběhu II. světové války nepřítelem rozluštěna. Slabým místem byl stále klíč, který musel být utajen. Většinou se podařilo kombinací špionážní práce, uloupením některých stěžejních dokumentů a především vynikající prací členů kryptologických center klíč odhalit a potom již titěrnou prací a s použitím prvních počítačů byly jednotlivé zprávy rozluštěny. Například výše uvedená Enigma byla prolomena díky práci polských kryptoanalytiků a vědců pracujících v britském kryptoanalytickém centru *Bletchley Park*.

[6]Zdroj `http://artblart.com/tag/enigma/`

Další dvě významné válečné šifry – šifra ADFGVX a kód Navaho

V období I. a II. světové války se používaly i jiné typy kryptografických systémů než polyalfabetické šifry. Uvedu dva z nich, které se úspěšně používaly a současně jsou příklady dalších typů šifer.

První z nich je německá *šifra ADFGVX*, používaná v roce 1918. Je příkladem tzv. *smíšené šifry*, kdy se kombinuje jednoduchá substituce a transpozice. Substituční šifra vychází z Polybiovy šifrovací mřížky, přičemž pozice řádků a sloupců jsou určeny písmeny, které se v Morseovce dostatečně liší pro eliminaci případné chyby při vysílání (podle těchto písmen je šifra pojmenována). Tabulka navíc obsahuje číslice.

Zvolíme si substituční klíč NEMECKASIFRA a vepíšeme jej do tabulky ovšem tak, že opakovaná písmena již nevpisujeme, poté doplníme chybějící písmena a číslice.

	A	D	F	G	V	X
A	N	E	M	C	K	A
D	S	I	F	R	B	D
F	G	H	J	L	O	P
G	Q	T	U	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

Tabulka 5: Tabulka pro první část šifrovacího mechanismu šifry ADFGVX

Podle této tabulky zašifrujeme zprávu ZAJIMAVOSTI Z KRYPTOLOGIE. Zvolíme si transpoziční klíč JARO a šifrovanou zprávu vepíšeme v řádcích do tabulky – sloupce jsou určeny transpozičním klíčem.

Výslednou zprávu dostaneme postupným vypsáním sloupců po provedení transpozice: DFFGADVADGADVFAGDDAVGFFAXDXVDDGXVVDADAFGVDFFFD

Šifru se nakonec podařilo v závěru války rozluštit francouzskému kryptoanalytikovi G. J. Paivinovi, který při kryptoanalýze

J	A	R	O		A	J	O	R
V	D	A	X		D	V	X	A
F	F	D	D	Přehození sloupců	F	F	D	D
A	F	A	X	dle abecedního	F	A	X	A
G	G	F	V	pořadí klíče	G	G	V	F
D	A	G	D		A	D	D	G
D	D	V	D		D	D	D	V
A	V	D	G	⟶	V	A	G	D
V	A	F	X		A	V	X	F
G	D	F	V		D	G	V	F
F	G	F	V		G	F	V	F
F	A	D	D		A	F	D	D
A	D				D	A		

Tabulka 6: Tabulka pro druhou šifrovacího mechanismu šifry ADFGVX

využil mj. opakujících se segmentů v otevřených zprávách (podpisy, oslovení).

Kódováním standardně rozumíme proces transformace zprávy do lépe přenositelné či zaznamenatelné podoby. Příkladem je přenos naší mluvené řeči do psané podoby, vysílání s pomocí Morseovy abecedy či stávající přepis informací do řetězců nul a jedniček, tzv. binárních kódů. Matematicky vyjádřeno, jedná se o zobrazení z množiny zdrojových znaků do množiny všech slov nad kódovou abecedou, což jsou posloupnosti znaků ze zvolené kódové abecedy[7]. *Kódem* poté nazýváme množinu všech kódových slov. Tato jsou vytvářena za účelem lepší komunikace, ne za účelem utajení.

S termínem kód se však můžeme setkat i v teorii šifrování. Kód zde zpravidla reprezentuje číslo, symbol nebo slovo, který nahrazuje celé jiné slovo nebo frázi. Cílem je utajit smysl, přičemž se může například utajovat identita tajného agenta nebo povel ke

[7]V případě binárních kódů je kódová abeceda tvořena dvěma znaky – nulou a jedničkou.

konkrétnímu útoku[8]. Tento typ kryptografie pro standardní tajnou komunikaci v průběhu času ztratil svůj význam díky své nepraktičnosti a komplikovanosti. Proto, abychom mohli takto prakticky komunikovat, bychom museli sestavit celou kódovou knihu, která by reprezentovala celý slovník pojmů a významů. V podstatě je potřeba vytvořit „nový jazyk“, který by byl pro útočníka nečitelný. Výjimky však potvrzují pravidlo, a přestože takto definovaný kód je nepraktický a standardně se nepoužívá, uvedeme nyní příklad, kdy byl tento typ šifry úspěšně užit a navíc nebyl nikdy prolomen. Jedná se o *kód Navaho*.

V průběhu II. světové války během bojů v Tichomoří nastal problém s využitím šifrovacích strojů. Tyto stroje byly pro komunikaci poměrně bezpečné, pokud se užívaly správně, byly ovšem pro potřeby boje v džungli často nepoužitelné. Na tento problém zareagoval inženýr z Los Angeles P. Johnston, který byl synem misionáře, v dětství vyrůstal v navažské rezervaci, znal kulturu Navahů a plynně hovořil jejich jazykem. Věděl, že jazyky původních obyvatel jsou natolik odlišné od jiných jazyků, že kdyby se zprávy zašifrovaly tak, že by byly přeloženy do takového jazyka a vysílány, byly by nerozluštitelné.

Se svým nápadem se obrátil na velitele pro komunikaci v Camp Elliot a úspěšně jej se dvěma Navahy demonstroval. Návrh byl přijat. Nakonec při rozhodování, který indiánský jazyk vybrat padla volba zrovna na Navahy. Bylo zapotřebí, aby kmen byl početný a pokud možno více gramotný. Vybíralo se ze čtyř kmenů Navahů, Siouxů, Chippewa a Pima-Papago. Navahové byli vybráni i přes svou největší negramotnost proto, že byli nejpočetnějším a zároveň jediným kmenem, který nebyl v posledních dvaceti letech infiltrován německými studenty. Nyní stačilo vybrat skupinu navažských mužů, vycvičit je, rozšířit jejich slovník o chybějící, především vojenské pojmy. Vše proběhlo úspěšně. Kód Navaho se ujal a patří mezi malou část válečných kódů, které nebyly nikdy prolomeny.

[8]Např. pod kódem Barbarossa byl za II. světové války skryt povel k útoku na Sovětský svaz.

Pojem či písmeno abecedy s reprezentujícím slovem	česky	Kód Navaho
Bojové letadlo	Kolibřík	Da-he-tih-hi
Ponorka	Železná ryba	Besh-lo
A (ant)	Mravenec	Wol-la-chee
B (bear)	medvěd	Shush

Tabulka 7: Příklady kódových slov v kódu Navaho

Závěr druhé části

Můžeme konstatovat, že období od 1. tisíciletí našeho letopočtu do 2. pol. 20. století skončilo remízou mezi kryptografy a kryptoanalytiky, alespoň co do umu a nalezených metod. Některé šifry rozluštěny byly, jiné nebyly, u některých to trvalo velice dlouho, za prolomením dalších šifer stála nejen obrovská práce kryptografů, ale i špionážní činnost a štěstí. Kryptologie nejvíce ovlivňovala politiku a hrála významnou roli v obou světových válkách.

V druhé polovině 20. století začaly kryptografické metody používat širší vrstvy obyvatel, zejména v bankovnictví, obchodu a průmyslu. Nastal ohromný rozmach používání kryptografie, což se sebou neslo nároky na generování a distribuci bezpečných klíčů. Situace byla dlouhodobě neudržitelná... (pokračování v 3. části)

Literatura

[1] Adams, S. (2003). *Šifry a kódy.* Překlad J. Koval, Banská Bystrica: Slovart, s. r. o.

[2] Berloquin, P. (2008). *Skryté kódy a velkolepé projekty.* Překlad Z. Dušek, Banská Bystrica: Euromedia Group, k. s.

[3] Farana, R. (1995). *Šifrování pro radost a poučení.* Brno: Mravenec.

[4] Janeček, J. (2008). *Rozluštěná tajemství.* Praha: Nakladatelství XYZ.

[5] Jiroušek, R., Ivánek, J., Máša, P., Toušek, J. & Vaněk, N. (2006). *Principy digitální komunikace.* Voznice: Leda.

[6] Konečná, P. (2015). Zajímavosti z kryptologie. Část I – Od prvopočátků až po frekvenční kryptoanalýzu. *Učitel matematiky* **23**(1), s. 1–15.

[7] Konečná, P., Vavříčková, L. & Wrublová, M. (2009). *Kódy a šifry – jejich matematický základ a historie.* Ostrava.

[8] Menezes, A. J., Oorschot, P. C. & Vanstone, S. A. (1997). *Handbook of applied cryptography.* Boca Raton: CRC Press.

[9] Piper, F. & Murphy, S. (2006). *Kryptografie.* Překlad P. Momdschein, Praha: Dokořán.

[10] Singh, S. (2003). *Kniha kódů a šifer.* Překlad P. Koubská a D. Eckhardtová, Praha: Dokořán a Argo.

[11] Vondruška, P. (2000). *Od zákopové války k asymetrické kryptografii.* Computerworld, 38.

Abstract

Cryptology is the science of encryption, decryption and deciphering. The ability to use secret means of communication and the ability to decipher secret messages were behind many historical events. This article – by means of selected historical events – represents cryptology as an interesting scientific discipline that has been accompanying the mankind since ancient times and has been permeating our daily lives up to present times. The text also points at the mixture of many branches and disciplines which can be used in teaching. The second part describes basic ciphers defending against frequency cryptoanalysis.

RNDr. Petra Konečná, Ph.D.
Přírodovědecká fakulta OU
30. dubna 22
701 03 Ostrava
e-mail: Petra.Konecna@osu.cz