Učitel matematiky

Petra Konečná

Zajímavosti z kryptologie (1) - od prvopočátků až po frekvenční kryptoanalýzu

Učitel matematiky, Vol. 23 (2015), No. 1, 1–15

Persistent URL: http://dml.cz/dmlcz/149410

ZAJÍMAVOSTI Z KRYPTOLOGIE (1) OD PRVOPOČÁTKŮ AŽ PO FREKVENČNÍ KRYPTOANALÝZU

Petra Konečná

Úvod

Stále se setkávám s názory, které zpochybňují smysluplnost matematiky a její význam pro běžný život. Lidé často matematiku chápou jako abstraktní a nepochopitelnou vědu izolovanou od každodenního života. Spousta žáků a studentů je přesvědčena, že jí s výjimkou jednoduchých počtů nikdy v životě nevyužijí, je to pro ně jen nutné zlo, které z nějakých důvodů musí trpět. Úmyslně si vybírají vysokoškolské studijní obory tak, aby se matematikou už nemuseli zaobírat. Jaké je jejich zděšení, když se ve studijním plánu biologie, geografie nebo jiných „oborů nesouvisejících s matematikou“ předměty opakující a rozvíjející základy středoškolské matematiky objeví, nemusím asi popisovat.

Nechci se věnovat analýze, proč tomu tak je. Cílem mého příspěvku je na základě historického exkurzu do kryptologie ukázat, že matematika není a nebyla izolovanou vědou a prolíná se s mnoha obory včetně historie, archeologie, jazykovědy apod. Chci zprostředkovat učitelům informace, kterými mohou zpestřit výuku nejen matematiky, mohou být inspirací pro projektovou výuku, protože propojují historii, jazyky, matematiku[1], informatiku, výpočetní techniku, chemii a lze najít souvislosti i s dalšími předměty.

[1] Z matematiky nejvíce využívá základy statistiky, teorii čísel, modulární aritmetiku a kombinatoriku.

Jako zdroj obecných informací jsem použila zejména [7], [6] a [5], pro upřesnění a sjednocení české terminologie publikace [2] a [3]. Další zajímavosti jsem čerpala z odborných a popularizačně vědeckých prací, které jsou uvedeny v seznamu použité literatury.

Kryptologie

Slovo *kryptologie* je složeno ze dvou řeckých slov *kryptos* a *logos*. Logos znamená slovo, řeč, myšlenka či pojem. Kryptos lze přeložit jako tajný či skrytý. Složeninu kryptologie lze tedy volně přeložit jako tajné slovo, tajná řeč, tedy tajná komunikace.

Komunikace je jednou z nepostradatelných schopností lidí. V rámci komunikace se snažíme prioritně o co nejlepší a nejpřesnější přenos našich myšlenkových pochodů do mluvené či psané verze tak, abychom je mohli předat. Člověk se však také občas dostává do situace, kdy naopak chce informaci utajit. Pokud ji chce utajit jen pro sebe, je nejlepší si ji zapamatovat. Pokud však má paměť horší nebo chce informaci předat pouze vybrané osobě, dostává se do problému. Jak informaci předat určené osobě a přitom ji utajit před ostatními?

Tajnou komunikaci využívali lidé od pradávna. V období starověku a středověku byla nezbytná zejména pro vládce, politiky, vysoce postavené osoby pracující ve vojenství a policii a také „špičky“ z náboženských kruhů. Postupně v moderním věku k těmto skupinám přibývali zejména lidé pracující ve světě velkých financí. V současné době využívá alespoň jistých prvků tajné komunikace každý člověk, pokud užívá moderní technologie, prostřednictvím kterých se předávají informace všeho druhu. V běžném životě jsme zvyklí používat platební karty, elektronické bankovnictví, elektronický podpis, mobilní sítě, sledovat různé televizní kanály atd. Na moderní kryptologické metody spoléháme při zajištění vojenských technologií, zbraní a dalších systémů, na kterých je postavena bezpečnost stávající civilizace. Říká se, že I. světová válka byla kvůli užití bojových plynů válkou chemiků, II. světová válka válkou fyziků díky jaderné bombě. S největší pravděpodobností by III. světová válka byla válka matematiků

a informatiků – byla by to válka o informace[2].

Vzhledem k výše uvedené charakteristice je zřejmé, že tajná komunikace a prostředky, které využívali jak ti, kteří s pomocí ní komunikovali, tak ti, kteří se snažili tajné zprávy ukrást a rozluštit, stály za mnoha historickými událostmi. Pokusím se tedy pomocí střípků z historie kryptologie představit základní podstatu této disciplíny. Nejdříve však musím osvětlit základní pojmy, které tento vědní obor používá.

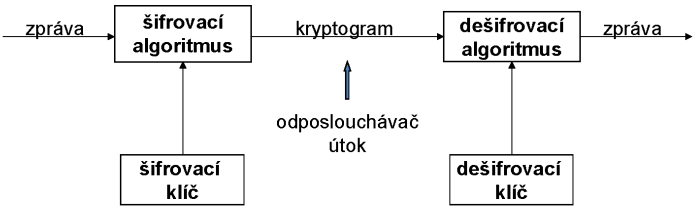
Základní pojmy kryptologie

Jak jsem již uvedla, tajnou komunikací se můžeme zabývat ze dvou základních důvodů. Prvním z důvodů je využití prostředků tajné komunikace za účelem přenosu tajné informace od *odesílatele* k *příjemci*. Odesílatel vezme *otevřenou zprávu* a prostřednictvím *šifrovacího algoritmu* ji převede do šifrového textu, tzv. *šifry*. Tento proces se nazývá *šifrování*. Zpráva je následně odeslána příjemci, který jí s využitím *dešifrovacího algoritmu dešifruje* a získá tak otevřený text. Pro užití šifrovacího a dešifrovacího algoritmu je stěžejní znalost *klíče*; zpravidla se jedná o nějaké heslo či jiný parametr, který je pro úspěšné použití algoritmu potřeba znát. Procesy šifrování a dešifrování společně tvoří oblast *kryptografie* a šifranti i dešifranti se souhrnně nazývají *kryptografové*.

Druhým důvodem je snaha získat zašifrovaný text a *rozluštit* jej, přestože nejsem příjemce. Nemusím a zpravidla neznám dešifrovací algoritmus nebo dešifrovací klíč (nebo obojí). Metody, které se zabývají luštěním šifer, jsou obsahem *kryptoanalýzy*, a osobám, které se věnují odkrývání obsahu utajených zpráv a prolamování šifer, říkáme *kryptoanalytici*, česky luštitelé[3].
Oblast kryptografie a kryptoanalýzy tedy souhrnně nazýváme kryptologie.

[2] Význam informace se již zřetelně projevil v obou světových válkách, přičemž postupně narůstal a v současnosti je považován za stěžejní.

[3] Snaze rozluštit šifru se často říká útok na šifru a samotnému rozluštění pak rozbití či prolomení šifry.



Obr. 1: Schéma procesu šifrování

Steganografie

Historie kryptologie (či spíše kryptografie) se začala psát již ve 4. tisíciletí před naším letopočtem. Známky šifrování vykazují některé hieroglyfy i hliněné tabulky z Mezopotámie, později také např. hebrejské texty. Nejstarší zmínky přímo o metodách tajné komunikace nacházíme v dílech z období 5.–4. století před naším letopočtem. Jedním z autorů, který nás informuje o prvopočátcích kryptografie, je řecký historik Herodotos. Věnuje se zejména příběhům, kdy byla pro tajnou komunikaci použita *steganografie*.

Slovo steganografie je složeno z řeckého *steganos* – schovaný a *graphein* – psát. Jedná se o metody, které otevřený text nemění, ale snaží se jej důmyslně ukrýt. Tyto metody byly úspěšně využívány již ve starověku. Herodotos ve svém díle *Dějiny* uvádí, jak steganografie pomohla Řekům ve válce s Peršany. V roce 480 př. n. l. byl perský král Xerxes připraven překvapit náhlým útokem Řecko, neboť na rozdíl od ostatních zemí odmítaly Athény a Sparta odvádět Peršanům poplatky a posílat jim dary. Na útok se připravoval pět let. Tuto situaci vypozoroval Demaratus, řecký vyhnanec žijící v perském městě Susy, a rozhodl se Řeky varovat. Nebezpečí prozrazení varovné zprávy bylo velké, a tak vymyslel, jak ji bezpečně před perskými kontrolami ukrýt. Seškrábal vosk ze dvou psacích destiček, napsal zprávu přímo na dřevěný podklad a znovu destičky zalil voskem. Prázdné destičky nevzbudily

podezření a dorazily do cíle. Řekům se i přes počáteční rozpaky z prázdných destiček nakonec podařilo zjistit, o co jde, a tak se o nebezpečí dozvěděli včas. Stačili se vyzbrojit a připravili na Peršany v zálivu nedaleko Athén past, do které perskou flotilu vlákali, a během jediného dne se jim podařilo obrovské perské vojsko porazit.

Další steganografickou metodu, kterou Herodotos zachytil, je ukrytí zprávy na hlavě posla. Zmiňuje se o ní v příběhu, který popisuje, jak jistý Histiaios chtěl povzbudit Aristagora Milétského ke vzpouře proti perskému králi. Oholil svému poslovi vlasy, vytetoval zprávu na hlavu a poté počkal, až mu zase dorostou vlasy. Takto se zpráva dostala ke svému příjemci.

Steganografické metody byly používány v různých částech světa a v různých obdobích. Ve staré Číně používali metodu, kdy zprávu napsali na jemné hedvábí, poté smotali do kuličky, zalili voskem a posel ji musel spolknout. Během cesty byla vosková kulička bezpečně uschována v trávicím systému, z něhož se po určité době dostala ven a byla doručena.

Ke steganografii patří také používání neviditelných inkoustů. Z 16. století máme od Giovanniho Porty zachován návod, jak schovat zprávu ve vejci natvrdo. Musí se připravit roztok „z jedné unce kamence a pinty octa“. Tímto roztokem se napíše zpráva na skořápku vajíčka, která pronikne póry a ukáže se až na vařeném bílku po oloupání vajíčka. Údajně taktéž objevil metodu psaní neviditelnými inkousty přímo na lidské tělo.

Problematika výroby a využití tajných inkoustů je vynikajícím prostředkem pro propojení matematiky a chemie. Proto užití tajných inkoustů rozebereme trochu podrobněji a uvedeme si několik příkladů.

Tajný inkoust je v podstatě roztok složený z určitých chemických látek, který je za normálních podmínek bezbarvý (popř. slabě zbarvený tak, aby nebyl na používané psací ploše vidět), ale při použití určitého způsobu podle druhu inkoustu se zviditelní. Obecně můžeme tajné inkousty rozdělit podle jejich základů nebo podle toho, jakým způsobem je lze zviditelnit. Pokud použijeme organické kapaliny, např. moč, mléko, citrónovou šťávu, ocet,

ovocné šťávy, lze text zviditelnit lehkým zahřátím, zbarví se dohněda. V případě chemických látek, které nejsou organického původu, můžeme text zviditelnit také zahřátím. Když například použijeme roztok kyseliny sírové, potom po zahřátí papír v místech s inkoustem zuhelnatí, pokud použijeme chlorid kobaltnatý, dojde po zahřátí k jasně modrému zbarvení. Pro zviditelnění lze dále využít jiné chemické látky nebo ultrafialového či infračerveného záření. Například použijeme-li jako tajný inkoust chlorid železitý, můžeme jej zviditelnit dvěma způsoby. Pokud tajnou zprávu potřeme žlutou krevní solí, zbarví se nám tajný inkoust modře. Pokud použijeme rhodanid draselný, získáme tajnou zprávu zbarvenou do červena. Jako tajný inkoust můžeme použít i hydroxid sodný. Po potření fenolftaleinem získá bezbarvý text intenzivní růžovou barvu. Pro změnu v případě využití kyseliny salicylové text uvidíme pod ultrafialovým světlem.

Tajné inkousty se používaly dlouho, například nedávno CIA odtajnila recepty na neviditelné inkousty, které byly používány ještě za I. světové války. Šest dokumentů pocházelo z posledních dvou let I. světové války a dříve byly v archivu námořní rozvědky. Jeden z nich popisuje složení neviditelného inkoustu, který používali němečtí špioni.

Mezi další modernější steganografickou metodu, která byla používána německými agenty působícími v Latinské Americe za II. světové války, patří ukrývání fotograficky zmenšené zprávy do tečky v textu. Zpráva byla náhodně objevena díky tomu, že fotograficky zmenšená tečka se v textu více leskla.

V rámci steganografie však nemusíme zprávy pouze zmenšovat či ukrývat tak, aby nebyly vůbec vidět. Příkladem jsou tzv. otevřené kódy, kdy jsou slova tajné zprávy schována v nějakém obecném textu, který je následně volně distribuován. Analogií je ukrytí zprávy ve volně dostupném textu tak, že pravidelně využijeme písmen jednotlivých slov tohoto textu, přičemž samotná písmena nám dávají skrytou zprávu (viz obrázek 2). S využitím moderních technologií je možné tajné texty ukrývat do souborů s hudbou nebo obrázku na místo náhodného šumu.

Aktualni pocasi v Adamove: polojasno, eventualne zatazeno, anomalie misty.

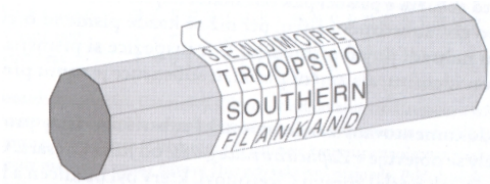
Obr. 2: Ukázka steganografie – zprávu dává každé druhé písmeno ve slovech s výjimkou předložek

Velice často se steganografické metody kombinují s dalšími klasickými šifrovacími metodami a to transpozicí a substitucí.

Transpoziční a substituční šifra

Šifře, kdy je zachován soubor použitých písmen otevřeného textu, pouze je zaměněno pořadí, říkáme *transpoziční*. Transpoziční šifra je jednou ze dvou základních typů šifer, které mění samotný charakter otevřeného textu za účelem utajení zprávy. Jedná se o všechny šifry, které vznikají popřehazováním písmen zpravidla dle nějakého řádu (například nejdříve vypíšeme všechna lichá písmena v pořadí a poté všechna sudá písmena) nebo formou přesmyček ve slovech. Z matematického pohledu se jedná o permutaci znaků otevřené zprávy.

Jedním z nejstarších příkladů transpoziční šifry je tzv. *Scytala* ze Sparty. Jednalo se o dřevěnou tyč, kolem které se omotal pruh kůže, a na ní se podélně napsala zpráva. Po odmotání pásku kůže zůstala zpráva s přeházenými písmeny a opět se dala přečíst, pokud měl příjemce tyč stejného průměru.



Obr. 3: Scytala (Sighn, 2003)

Druhou alternativou, která se nabízí, je zaměnit znaky otevřeného textu za znaky jiné. Takovým šifrám říkáme *substituční*. Souboru znaků, kterými nahrazujeme znaky původní zprávy, říkáme *šifrová abeceda*.

Jeden z prvních popisů substituční šifry můžeme najít překvapivě v díle Kámasútra, jejíž rukopisy pocházejí pravděpodobně z roku 400 před naším letopočtem. Je v ní ženám doporučováno studovat celkem 64 umění od vaření, oblékání a masáží až po šachy či tesařství. Jedním z doporučených umění je tzv. „mlecchita – vikalpa“, sloužící k tajné milostné korespondenci. Mezi doporučenými technikami nacházíme typ substituce, který je z matematického hlediska prostým zobrazením z množiny znaků otevřené abecedy do množiny znaků šifrové abecedy, přičemž šifrová abeceda je takovou permutací původní abecedy, že ke každému písmenu otevřeného textu je přiřazené jiné písmeno abecedy. Pokud naší zprávou bude vzkaz SEJDEME SE V ZAHRADE ZA SOUMRAKU BUDE BEZPECNO, potom s pomocí převodní tabulky, kde je v prvním řádku abeceda otevřeného textu a v druhém řádku šifrová abeceda, získáme šifru RXBPXYXRXNKTIGTPXKTRWOYGTZOCOPXCXKFXUEW.

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

Tabulka 1: Převodní tabulka pro tvorbu substituční šifry

Dalším známým příkladem substituční šifry je *Caesarova šifra*. Zachoval se písemný záznam o jedné z mnoha šifer, které Julius Caesar používal. Celý princip spočíval v nahrazení písmen otevřené zprávy písmeny, které se nacházejí v abecedě o tři pozice dále[4]. Bude-li tedy naší otevřenou zprávou text ZAPISKY

[4]V současnosti pod pojmem Caesarova šifra rozumíme všechny typy substitučních šifer, kdy je šifrová abeceda dána posunem, a to o libovolný počet míst.

O VALCE GALSKE, potom šifrou bude CDSLVNBRZDOFHJDUVNH.

Nemusí vždy automaticky platit, že jeden znak otevřeného textu musí být nahrazen jedním znakem šifrové abecedy. Takovým příkladem substituční šifry je Polybiova šifrovací mřížka, někdy také nazývána *Polybiův čtverec*. Šifru popsal řecký politik Polybios asi 200 let před naším letopočtem. Princip je velmi jednoduchý, můžeme říci, že každý znak je reprezentován dvojicí čísel řádku a sloupce, kde se vyskytuje.

	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

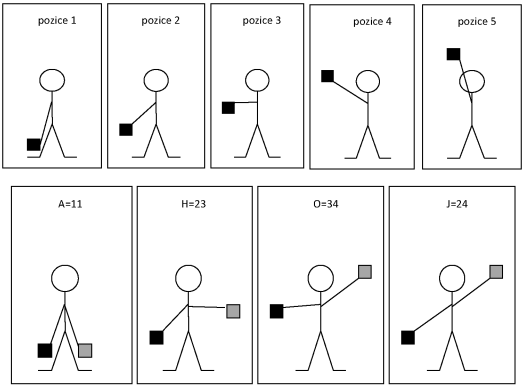
Tabulka 2: Polybiův čtverec

Tento typ šifry je vhodný i pro různé druhy signalizace – řecký politik popisuje světelnou signalizaci pomocí loučí. Další možností je vlajková signalizace. Předpokládejme, že chceme odsignalizovat zprávu AHOJ. Nejdříve ji musíme zašifrovat s pomocí Polybiova čtverce, získáme šifru 11 233 424. Obrázek 4 znázorňuje jednotlivé pozice vlajek pro čísla i posloupnost signálu pro námi odesílanou zprávu.

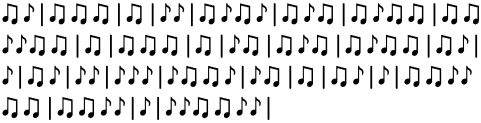
Další alternativou je tzv. šifrovaná morseovka. Jednotlivé znaky, tj. čárky, tečky a oddělující znak nahradíme znaky šifrové abecedy. U prvního příkladu (obrázek 5) je čárka nahrazena dvojicí osminových not a tečka jen jednou notou. U druhého příkladu tečku nahrazuje čtyřúhelník a čárku oválný útvar (obrázek 6).

Bezpečnost šifry

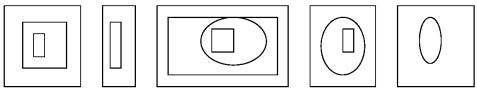
Pro utajení komunikace by bylo ideální zachování všech tří podmínek, tj. utajení klíče, utajení šifrovacího algoritmu a nemožnost



Obr. 4: Signalizace s pomocí Polybiova čtverce



Obr. 5: Šifrovaná morseovka, příklad 1



Obr. 6: Šifrovaná morseovka, příklad 2

odchycení šifry kryptoanalytikem. Toto však nebylo možné zajistit ani v době, kdy šifrovací algoritmy používala jen úzká skupina obyvatel a zprávy byly doručovány osobně poslem. V současné době, kdy je během každé vteřiny odesíláno prostřednictvím informačních technologií obrovské množství zpráv, nejsme schopni zaručit, že zpráva nebude zachycena. Taktéž algoritmy používané pro šifrování jsou ve většině případů známé mnoha skupinám lidí po celém světě. Bezpečnost šifry tedy stojí a padá výhradně s bezpečností klíče.

Jak již bylo uvedeno, klíč je určitý parametr, který je potřebný pro správnou aplikaci šifrovacího resp. dešifrovacího algoritmu. Klíče u doposud uváděných historických šifer jsou jednoduché. Pro Scytalu je to tyč, kolem které se omotává pásek. U substitučních šifer je to vždy převodní tabulka, podle které nahrazujeme znaky (resp. informace o posunu písmen v šifrové abecedě Caesarovy šifry). Šifru považujeme za bezpečnou tehdy, jestliže je schopna odolat tzv. *útoku hrubou silou*. To znamená, že pouhým zkoušením všech možností klíčů není kryptoanalytik schopen v reálném či potřebném čase správný klíč odhalit.

U transpozičních šifer je klíčem správná permutace znaků zprávy. Pokud máme zprávu délky pět, potom počet všech možných klíčů je 5!, tedy 120. Toto jsme schopni i bez použití jakékoliv techniky v relativně krátkém čase ověřit. Pokud je ovšem zpráva dostatečně dlouhá, počet možností výrazně narůstá – při délce zprávy n dostáváme $n!$ možností.

U substituční šifry je problém obdobný. Počet možností při hledání klíče je dán počtem všech možných nastavení pro substituci mezi abecedou otevřeného textu a šifrovou abecedou. Caesarova šifra není a ani v době svého aktivního používání nebyla bezpečná, protože počet možných šifrových abeced je dán počtem možných posunů v abecedě. Budeme-li tedy uvažovat naši abecedu se 26 znaky, potom počet všech možných klíčů je 26, což není problém ověřit. Pokud bychom se však neomezovali pouze na posuny, ale šifrová abeceda by mohla být nastavena libovolnou permutací původní abecedy, dostáváme již 26! možností, což je řádově 10^{27} potencionálních klíčů.

Dalo by se tedy říci, že pokud kryptografové v době bez moderních počítačů používali transpoziční šifru pro dostatečně dlouhé zprávy nebo substituční šifry s libovolnými možnostmi pro výběr šifrové abecedy, byla tajná komunikace bezpečná. Bylo tomu tak, ale pouze do 1. tisíciletí našeho letopočtu. Zlom nastal díky arabským učencům, kteří vynalezli tzv. *frekvenční kryptoanalýzu*, a dali tak základ vědní disciplíně kryptoanalýze.

Frekvenční kryptoanalýza

Zlatý věk islámské civilizace nastal asi v 7. století našeho letopočtu. Dobyvatelské ambice Arabů slábly a spíše se začaly soustředit na rozvoj kultury, vědy, obchodu, celé společnosti i zajištění její bezpečnosti. Arabové se po dobytí jednotlivých území setkali s daleko vzdělanějšími národy a postupně si začali jejich duchovní bohatství osvojovat, uchovávat i postupně rozvíjet.

Pro svou komunikaci také používali šifry a to nejen pro utajení citlivých státnických záležitostí, ale například i při daňových záznamech. Kryptografie byla dostatečně rozšířená. První záznam o metodě, která slouží ke kryptoanalýze, pochází od „filozofa Arabů“ al Kindího z 9. století. Jedná se o důmyslné propojení statistiky a lingvistiky. Spočívá v tom, že určíme relativní četnosti znaků, které se nacházejí v šifrované zprávě. Na základě znalosti relativních četností vyskytujících se písmen v daném jazyce začneme přiřazovat znaky otevřené abecedy a šifrové abecedy. Samozřejmě málokdy bude tento odhad zcela přesný. Čím je zpráva delší, tím je odhad přesnější. Zpravidla musíme přiřazování upravovat, než dostaneme správné nastavení. Přesto je frekvenční kryptoanalýza velice efektivní.

Pro jednoduchost si uvedeme příklad, kdy víme, že byla použita Caesarova šifra. Všech možných klíčů je 26. My však nebudeme na šifru „útočit hrubou silou“, ale využijeme frekvenční kryptoanalýzu. Předpokládejme, že jsme zachytili tuto zprávu:
MYOLYVFDHVDYCDSLVNBRZDOFHJDOVNH.

Určíme absolutní četnost jednotlivých znaků v této zprávě.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	1	5	0	2	0	3	0	1	0	2	1

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	3	0	0	1	1	0	0	4	0	0	3	1

Tabulka 3: Absolutní četnosti znaků v šifrované zprávě

Nejčastěji se v této zprávě vyskytuje písmeno D. V českém jazyce je obecně nejčetnější písmeno E. Pokud tedy provedeme tento

písmeno	frekvence	Písmeno	Frekvence
A	8,6	N	6,8
B	1,7	O	8,0
C	3,3	P	3,2
D	3,6	Q	0,0
E	10,5	R	4,9
F	0,2	S	6,3
G	0,2	T	5,1
H	2,2	U	4,0
I	7,5	V	1,3
J	2,2	W	0,0
K	3,6	X	0,1
L	4,2	Y	2,8
M	3,5	Z	3,2

Tabulka 4: Relativní četnosti písmen v českých textech

posun v abecedě (k písmenu E v prvním řádku přiřadíme písmeno D v druhém řádku) a začneme postupně nahrazovat znaky, získáváme zprávu NZPM…, která zřejmě nedává smysl. Musíme tedy hledat nové nastavení. Druhým nejčastějším znakem v češtině je A. Vytvoříme tedy druhou tabulku, kdy písmenu A v prvním řádku bude odpovídat v druhém řádku D.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabulka 5: Tabulka pro dešifrování určena na základě frekvenční kryptoanalýzy

Postupně znakům šifrové zprávy dle druhého řádku tabulky přiřazujeme znaky otevřeného textu z prvního řádku a získáváme zprávu JULIUSCAESARZAPISKYOVALCEGALSKE.

Závěr první části

Historie kryptologie je vlastně stálým soubojem schopností kryptografů a kryptoanalytiků. Díky arabským učencům měli v prvním tisíciletí našeho letopočtu kryptoanalytici trumf, který jim vydržel několik set let. Přestože se kryptografové snažili proti frekvenční kryptoanalýze uplatňovat různé zdokonalující šifrovací postupy, nebyla tajná komunikace po dobu následujících 500 let dostatečně bezpečná.

Literatura

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

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

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

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

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

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

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

[8] Vondruška, P. (2000). Od Kámasútry k Máchovi. *Computerworld*, 37.

[9] 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 – will represent cryptology as an interesting scientific discipline that has been accompanying the mankind since antient times and has been permeating our daily lives up to the present times. The text also points at intermingling of many branches and disciplines which can be used in teaching.

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