Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 9, číslo 6/2007 **15. červen 2007**

6/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1195 registrovaných odběratelů)

Obsah : str.

Příloha:
Mikulášská kryptobesídka (6.-7.12.2007): **MKB2007_CallForPapers_cerven.pdf**

A. Přehled a historie polyalfabetických šifer

Pavel Vondruška (pavel.vondruska@crypto-world.info)

(příspěvek z konference Security 2007, Praha, 30.5.2007
http://www.aec.cz/index.php?id=244,981,0,0,1,0)

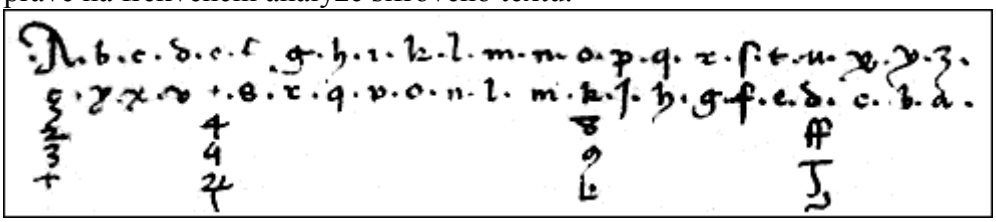
Anotace

Přednáška se zabývá vznikem a vývojem polyalfabetických šifer a dále jejich přínosem a významem pro kryptologii. Mimo řady historických informací a souvislostí, je podán systematický a téměř úplný výklad jednotlivých typů polyalfabetických šifer. Přednáška zabývá i vznikem klíčového hospodářství. Popsán je vývoj návrhu výběru šifrové abecedy od prostého „pořadí“ (Trtheimiova Tabula Recta), přes různé verze periodických hesel až po Cardanův revoluční objev autoklávu. Přednáška končí využitím zobecněného polyalfabetického systému využívajícího nekonečný „klíč“, který vedl k důkazu existence absolutně bezpečného systému (Gilbert S. Vernam, C. E. Shannon). Text vznikl sloučením a upravením odstavců, které se zabývají polyalfabetickými šiframi, z knihy *Kryptologie, šifrování a tajná písma* (edice OKO, Albatros, Praha 2006).

Hledá se odolná šifra proti frekvenční analýze

Zatímco arabský svět znal využití *frekvenční analýzy* pro luštění jednoduché substituční šifry již v devátém století (viz např. práce Abú-Yūsuf Ya'qūb ibn Ishāq al-Kindīho (801–873)), objevila západní Evropa tuto metodu pravděpodobně až na začátku století čtrnáctého. Učenci proto začali hledat vylepšení v té době dominantního šifrového systému – jednoduché záměny. Jimi navržená zlepšení se soustředila na zakrytí statistických závislostí v šifrovém textu, které prozrazují informace o otevřeném textu.

V polovině 14.století se jako přirozený výsledek tohoto snažení objevily homofonní šifry (nejstarší dochovaná *homofonní šifr*a na evropském kontinentu je šifra, kterou používal vévoda Simeone de Crema z Mantovy pochází až z roku 1401). Tyto šifry, na rozdíl od jednoduché substituce, kde každý otevřený znak se převádí pomocí jednoho znaku šifrové abecedy, používají pro převod některých vybraných znaků (zpravidla těch nejfrekventovanějších) více šifrových znaků. Tím se výrazně ztížilo luštění, které je založeno právě na frekvenční analýze šifrového textu.



Tato nová metoda se velmi rychle ujala. Např. je známo, že již v roce 1379 Ital Gabrieli di Lavinde vytvořil soubor individuálních šifer pro 24 vyslanců vzdoropapeže Klementa VII. Lavindeho metoda byla založena nejen na využití homofonní substituce, ale dále byla pro větší složitost přidán seznam kódových ekvivalentů pro vybraný počet celých slov (většinou jmen a názvů). Takovýto kombinovaný systém byl nazván nomenklátor. Nomenklátory pozdější doby obsahují mimo klasické substituční homofonní záměny i kódy pro slabiky a dále kódy pro nejfrekventovanější slova a jména, a navíc i tzv. klamače, nevýznamové

skupiny písmen, které měly ztížit kryptoanalýzu zašifrovaných textů. Nomenklátory postupně rozšiřovaly slovník na stovky až tisíce kódových slov. Tato metoda se udržela dalších více než 500 let, a to i tehdy, když již byly známé mnohem lepší a dokonalejší metody šifrování. Metoda má totiž jednu nepřekonatelnou výhodu: její použití je nesmírně jednoduché a při troše zběhlosti i rychlé. Každý si také může jednoduše vytvořit svůj nomenklátor nebo malou kódovou knihu. Je to prvé řešení (ač neuvědomělé) všeobecného rozporu v kryptologii, a to mezi bezpečností a jednoduchostí použití.
Hledání způsobu, jak zvýšit odolnost substituční šifry proti luštění pomocí četnosti znaků šifrové abecedy vedlo nejen k myšlence přiřadit ke každému znaku více znaků šifrové abecedy, ale i k objevu nového převratného řešení, kdy šifrový text se vytváří pomocí několika jednoduchých substitučních šifer, které jsou podle dohodnutého systému postupně použity na zašifrování jednotlivých znaků otevřeného textu

Takovýto šifrový systém se nazývá ***polyalfabetická substituce*.**

Historii a popisu jednotlivých polyalfabetických systémů, včetně vývoji hledání řešení problému předání informace o výběru jednoduché záměny (klíče), je věnován tento příspěvek.

Vznik polyalfabetického systému

1. Leon Battista Alberti (první polyalfabetický šifrový systém, kotouč)

Leon Battista Alberti (1404–1472) byl všestranně vzdělaný člověk – stavitel, nadaný varhaník, filozof, básník…. Nás však zajímá především proto, že za svůj příspěvek k rozvoji kryptologie byl v pozdějších letech nazýván otcem západní kryptologie. Alberti se na sklonku života začal zabývat (na podnět papežského tajemníka Leonarda Data) utajováním zpráv. Napsal stručnou 25 stránkovou práci, která se stala jednou z nejvýznamnějších prací tohoto druhu napsanou v západní Evropě. Dílo obsahuje hned tři důležité mezníky: první „evropský“ systematický výklad luštění na základě frekvence a jazykových znalostí, objev nového šifrového systému *polyalfabetické substituce* a používání zašifrovaných kódů.

K rychlému šifrování pomocí polyalfabetické substituce sestrojil Alberti *šifrovací disk,* který se skládá ze dvou otočných kotoučů reprezentujících otevřené a šifrované znaky, přičemž otáčením se zajišťoval výběr příslušné abecedy. Alberti doporučuje posunout abecedy vždy po třech nebo čtyřech slovech.

Tento objev nového šifrového systému, který byl zásadní v dějinách kryptologie, korunoval Alberti ještě dalším pozoruhodným návrhem jak pro zvýšení bezpečnosti kódy před jejich použitím ještě zašifrovat. Příjemce nejprve kódy podle použitého systému dešifroval a pak je teprve použil k získání otevřeného textu pomocí kódové knihy.

2. Johannes Trithemius (tabula recta)

V roce 1508 se pustil Johannes Trithemius (1452-1516) do psaní šestidílné knihy výhradně zaměřené na kryptologii. Tuto knihu nazval *Polygraphia,* a to vzhledem k rozmanitosti možných metod psaní, které se v knize vyskytují. Knihu (rukopis) věnoval 24. dubna 1508 císaři Maxmiliánovi I. Dva roky po jeho smrti byla kniha roku 1518 vytištěna, a stala se tak vůbec první tištěnou knihou pojednávající o kryptologii. Její celý název je *Šest knih o polygrafii od Johanna Trithemia, opata z Würzburgu, dříve ze Spanheimu věnované císaři Maxmiliánovi*. Kniha má 540 stran, je tištěna černým a červeným písmem.

V knize je představen jím navržený šifrový systém nazývaný Ave Maria. Šifra spočívá v tom, že jednotlivým písmenům jsou přiřazena celá slova. Seznam slov volí autor tak, aby dávala smysluplný text – jakousi nevinnou modlitbu. Tak třeba slovo abbot (opat) se zašifruje jako DEUS CLEMENTISSIMUS REGNES AEVUM INFINIVET, kde DEUS = A, CLEMENTISSIMUS = B, REGNES = B atd.
V pátém díle, který je z kryptologického hlediska nejvýznamnější, je uvedena šifrovací tabulka, tzv. "**tabula recta**", která je základem pro polyalfabetické šifry.

Trithemiova šifra používá tabulku sestavenou z 26 seřazených abeced. Šifrování probíhá velmi prostě a jednoduše. Písmeno otevřeného textu se vyhledá v prvém řádku, jeho šifrový ekvivalent se najde pod ním v abecedě, která odpovídá pořadí znaku v otevřeném textu. V praxi to znamená, že první znak otevřeného textu zůstává nezměněn, druhý znak se zašifruje pomocí druhé abecedy atd. Po vyčerpání všech 26 abeced se pokračuje znovu první abecedou.
Tabula recta (doplněno očíslování řádků) :

```
 1  ABCDEFGHIJKLMNOPQRSTUVWXYZ
 2  BCDEFGHIJKLMNOPQRSTUVWXYZA
 3  CDEFGHIJKLMNOPQRSTUVWXYZAB
 4  DEFGHIJKLMNOPQRSTUVWXYZABC
 5  EFGHIJKLMNOPQRSTUVWXYZABCD
 6  FGHIJKLMNOPQRSTUVWXYZABCDE
 7  GHIJKLMNOPQRSTUVWXYZABCDEF
 8  HIJKLMNOPQRSTUVWXYZABCDEFG
 9  IJKLMNOPQRSTUVWXYZABCDEFGH
10 JKLMNOPQRSTUVWXYZABCDEFGHI
11 KLMNOPQRSTUVWXYZABCDEFGHIJ
12 LMNOPQRSTUVWXYZABCDEFGHIJK
              . . .
24 XYZABCDEFGHIJKLMNOPQRSTUVW
25 YZABCDEFGHIJKLMNOPQRSTUVWX
26 ZABCDEFGHIJKLMNOPQRSTUVWXY
```

Příklad použití:

```
Otevřený text      OKO ALBATROS
Šifrový text       OLQ DPGGAZXC
```

Příjemce postupuje při dešifrování opačně. Vezme šifrový znak a podle jeho pořadí v šifrovém textu zvolí příslušnou abecedu. Pak v této abecedě vyhledá zvolený šifrový znak a jeho otevřený ekvivalent nalezne nad ním v prvém řádku.

Kniha významně ovlivnila myšlení středověkých kryptologů a byla přepisována, vydávána a šířena po celá další století.

3. Girolamo Cardano (autoklíč)

Girolamo Cardano (1501-1576), milánský fyzik, astronom a matematik trpěl až chorobnou touhou získat popularitu. Za svého života napsal neuvěřitelné množství knih (131 vyšlo a dalších 111 zůstalo v rukopise). O kryptologii nenapsal samostatnou knihu, ale své poznatky uložil do dvou spisů věnovaných popularizaci vědy. První se nazýval *De Subtiliate* (1550) a druhý *De Rerum Varietate Libri XVII* (1557). Obě knihy si veřejnost oblíbila pro jejich jasný popis, využití zajímavých až anekdotických příběhů a bohaté ilustrace.
Pokud jde o vývoj kryptologie, přidal Cardano další významnou myšlenku pro zvýšení bezpečnosti polyalfabetické šifry. Pochopil, že změna klíče, který se využívá k určení abecedy pro zašifrování dalšího znaku zprávy, má významný vliv na bezpečnost. Je jasné, že změna

hesla před každou zprávou je z hlediska bezpečnosti výhodnější než používat jeden klíč na šifrování všech zpráv. Kompromitace (prozrazení) hesla v prvním případě vede k rozluštění jen jedné zprávy, ve druhém případě ke kompromitaci celé korespondence. Jak však zajistit, aby mohl být klíč pro výběr abecedy pokaždé jiný? Cardano navrhuje použití autoklíče. Bohužel tuto novou nádhernou myšlenku formuluje nedokonale. Jím popsaný způsob dovoluje určitou nejednoznačnost šifrování, navrhuje opětovné použití klíče vždy na začátku otevřeného slova a nestanoví předání začátečního hesla autoklíče – tj. příjemce i luštitel jsou ve stejném postavení. Proto se jím uvedený systém nepoužíval. Kdyby jej byl dotáhl k dokonalosti, získal by mezi kryptology nesmrtelnou slávu, po které tolik toužil.
Věhlas mu však přinesla jiná zde publikovaná šifrovací metoda, která se zabývá utajením textu, tedy steganografická metoda. Metoda je dnes známá pod názvem Cardanova mřížka.

4. Giovanniho Battisty Belasa (zavedení klíče)

Roku 1553 vyšla knížka *La cifra* (Šifra) italského šlechtice Giovanniho Battisty Belasa popisující kryptosystém založený na znalosti hesla, dnes bychom přesněji řekli tajného klíče. Rozvinul tím dříve popsané skvělé myšlenky Albertiho a Trithemia na využití více abeced k šifrování (polyalfabetická šifra). Současně se tímto nápadem staly šifrové postupy realizovatelné na vysokém stupni zabezpečení. Právě výběr použité abecedy byl v původních systémech dosud velkou slabinou. Zde je tedy metoda, která umožňuje „dohodu“ na pořadí využívání jednotlivých šifrových abeced. Tajným klíčem v tomto systému může být slovo nebo celá věta, která se opakovaně píše nad otevřený text. Každé písmeno otevřeného textu je potom šifrované abecedou, která je určená písmenem z hesla nad ním. Pro šifrování se používala Trithemiova tabulka. Nestačí tedy znát pouze šifrový systém, ale je potřeba znát i tajný klíč.

5. Giovanni Battista Porta (obecná polyalfabetická šifra)

Ital Giovanni Battista Porta (1535-1615) se věnoval přírodním vědám a magii. Založil první vědeckou učenou společnost – *Accademia Secretorum Naturae* (Akademii přírodních tajemství). V roce 1563 vydal Porta knihu, která mu zajistila slávu a věhlas na poli kryptologie. Jde o opravdu mimořádnou práci, a to nejen svým obsahem, ale i dokonalým pedagogickým výkladem. Její název je *De Furtivis Literarum Notis*. Její čtyři části zabývající se starými šiframi, moderními šiframi, luštěním a jazykovými zvláštnostmi, které pomáhají při luštění, v sobě soustřeďovaly kryptologické znalosti tehdejší doby.
Porta ve svém díle klasifikoval tři základní šifrovací systémy: změnu pořadí písmen (transpozice), změnu tvaru písma (substituce za symbol), změnu kvality písmene (substituce písmene jiným písmenem). Toto dělení šifer se víceméně dochovalo dodnes. Do dějin kryptografie se nesmazatelně zapsal jako první, kdo popsal digrafickou šifru. Při šifrování se dva znaky otevřeného textu nahrazují jedním symbolem. Portova digrafická šifra byla realizovaná tabulkou, kde řádky a sloupce byly označené písmeny abecedy. Zabýval se i kryptoanalýzou a publikoval způsob, jakým se dá rozluštit monoalfabetická šifra bez znalosti dělení slov. Porta byl také prvním, kdo odmítl nerozluštitelnost polyalfabetických šifer a vymyslel několik metod k jejich luštění. Jeho největším přínosem byla však malá poznámka, která definovala *obecnou polyalfabeticku šifru*. Jednak doporučil používat k výběru abecedy klíč, a to co nejdelší, ale především poznamenal, že Trithemiova šifrovací tabulka nemusí obsahovat jen vzájemně posunuté abecedy, ale abecedy úplně zpřeházené a nijak spolu nesouvisející. Sám však dále využíval abecedy, které byly srovnané. **Porta skloubil všechny tři základní složky, které jsou podstatou moderní koncepce polyalfabetického systému: využití různých abeced, abeced, které mohou být zpřeházené, změnu výběru abecedy po každém písmenu, výběr abecedy určený dlouhým heslem.**

6. Francouz Blaise de Vigenére (Vigenérova šifra, periodické heslo, autoklíče)

Francouz Blaise de Vigenére (1523-1596) publikoval v roce 1586 knihu *Traicté des chiffres (Pojednání o šifrách)*. Díky svému systému, který zde představil, se natrvalo zapsal mezi nejznámější kryptology.

Narodil se roku 1523, v 17 letech byl poslán ke dvoru. Ve 24 letech vstoupil do služeb vévody Navarrského, kde zůstal po celý svůj život s výjimkou dvou let (1549-1550), kdy byl vyslán do Říma jako diplomat. Zde poprvé přišel do kontaktu s kryptologií. Četl práce Trithemia, Belasa, Cardana, Porty, publikoval dílo Albertiho. V roce 1570 se začal věnovat psaní knih. V roce 1586 vyšla již zmíněná objemná kniha *Traicté des chiffres* (přes 600 stran). I když se obsah knihy uchýlil spíše k okultním vědám, černé magii, kabale, tajemství vesmíru, hledání receptury na výrobu zlata a filozofickým úvahám, jeho dílo poskytovalo velmi cenné kryptologické informace také tím, že přesně cituje jiné autory. K celé řadě šifer, které Vigenére v knize rozebíral (např. ukrytí zprávy do obrazu hvězd), patřily i šifry polyalfabetické. Abecedy zapisoval do podobné tabulky, jakou používal Trithemius. Uvedl různé výběry abeced, a to buď postupné použití abeced za sebou, nebo podle hesla, kterým mohlo být slovo, věta nebo celá báseň. Jeho největším přínosem však je zlepšení Cardanova šifrovacího autoklíče. Zlepšení spočívalo v doplnění požadavku na předání počátku klíče a v tom, že vytváří jeden autoklíč (buď z otevřeného nebo šifrového textu) pro celou zprávu, zatímco Cardano začíná vytvářet autoklíč na každém slově otevřeného textu znovu.

Přesto, že Vigenére vyložil metodu velmi jasně a srozumitelně, zapadla v této podobě zcela v zapomenutí a v kryptologii se začala používat až v 19. století. Autoři různých kryptologických statí navíc jeho důmyslný systém degradovali na systém mnohem elementárnější, pro který se časem vžil název Vigenérova šifra. V něm se používá pouze standardních abeced a krátkého opakujícího se hesla, které se k otevřenému textu podle převodové tabulky přičítá. Tento systém někdy též nazývaný „periodické heslo“ je daleko zranitelnější než Vigenérem navržený autoklíč.

Systém Vigenére – periodické heslo

Jedná se o nejpoužívanější variantu této polyalfabetické šifry, která je založena na využití stejné tabulky, jakou používal Trithemius. Na rozdíl od něj však určuje výběr převodové abecedy nikoliv pořadí znaků v otevřeném (resp. šifrovém textu), ale znak hesla. Toto heslo zná odesílatel a příjemce. Heslo si uživatel zapíše opakovaně nad text, aby věděl, jakou abecedu má pro zašifrování (resp. dešifrování) konkrétního písmene použít. Proto se tomuto systému někdy říká **periodické heslo**. Systém byl úspěšně používán po řadu století. Měl pověst velmi bezpečného systému. Ve skutečnosti je pro krátké heslo a dostatečně dlouhý text poměrně lehce řešitelný. Na systém lze úspěšně útočit i odhadováním slov, která se v něm vyskytují.

```
A ABCDEFGHIJKLMNOPQRSTUVWXYZ
B BCDEFGHIJKLMNOPQRSTUVWXYZA
C CDEFGHIJKLMNOPQRSTUVWXYZAB
D DEFGHIJKLMNOPQRSTUVWXYZABC
E EFGHIJKLMNOPQRSTUVWXYZABCD
…
T TUVWXYZABCDEFGHIJKLMNOPQRS
U UVWXYZABCDEFGHIJKLMNOPQRST
V VWXYZABCDEFGHIJKLMNOPQRSTU
W WXYZABCDEFGHIJKLMNOPQRSTUV
X XYZABCDEFGHIJKLMNOPQRSTUVW
Y YZABCDEFGHIJKLMNOPQRSTUVWX
Z ZABCDEFGHIJKLMNOPQRSTUVWXY
```

Princip tzv. Vigenérova systému (periodicky se opakující klíč OKNO):

```
Klíč:               OKNOOKNO
Otevřený text:      ALBATROS
Šifrový text:       OVOOHBBG
```

7. Gaspar Schott (systém Gronsfeld)

Německý kryptolog Gaspar Schott (1608-1666) vydává v roce 1665 knihu *Schola steganographica*. Je také autorem jednoduchého polyalfabetického systému, který vychází ze systému Vigenére, ale k výběru abecedy se používá číselné, periodické heslo a vybírá se pouze z deseti abeced (nikoliv 26 jako u Trithemia nebo Vigenéra). Systém je v současnosti znám pod názvem Gronsfeld.
Používá se tabulka o deseti (seřazených) abecedách. K výběru abecedy se používá číselný klíč, který se opakovaně (periodicky) nadepíše nad otevřený text. Šifrový text se pak určí stejně jako ve Vigenérově systému. Klíč určí řádek šifrové abecedy a sloupek určí znak otevřeného textu, který se vyhledá v prvém řádku tabulky. Odpovídající šifrový znak je v textu určeném průsečíku.

Příklad použití Gronsfeldova systému (periodicky se opakující klíč 52973):

```
Klíč:               5297 35297352
Otevřený text:      DNES NEPRIJDU
Šifrový text:       IPNZ QJRAPMIW
```

	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**
0	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

Při dešifrování příjemce nejprve nad šifrový text opakovaně napíše domluvené číselné heslo (v našem případě 52973). Potom postupně vyhledává znaky šifrového textu v abecedě (řádku), která je určena heslem zapsaným nad šifrovým textem. Hledaný znak otevřeného textu nalezne v prvém řádku tabulky nad šifrovým znakem.

Gronsfeldův systém byl oblíbeným systémem, který byl používán ještě ve 20. století. Zvláště oblíbený byl mezi vězni a galerkou. Jeho obliba plynula z toho, že šifrování i dešifrování je rychlejší než při použití plné tabulky, jako v systému Vigenére. Systém (tak jako všechny obdobné polyalfabetické systémy) měl pověst bezpečného systému.

8. Giovanni Sestri (Beaufortova varianta Vigenérovy šifry, Sestri-Beafort)

Pro úplnost ještě dodejme, že Ital Giovanni Sestri navrhl roku 1710 ve své knize úpravu výše popsaného Vigenérova systému. Úprava spočívá v tom, že šifrant nezačíná písmenem otevřeného textu, ale písmenem klíče.
Na řádku, který je zvolen podle klíče, se vyhledá znak otevřeného textu a ten v prvním řádku ve stejném sloupci určí šifrový znak. Rozmyslíme-li si, jak jednotlivé systémy přesně fungují, zjistíme, že tato varianta je vlastně určitou logickou inverzí (převráceným postupem) k Vigenérově systému. Systém byl později v devatenáctém století pojmenován podle podobného systému (se kterým se někdy zaměňuje) admirála Beuforta a je v současnosti

znám jako Beufortova varianta Vigenérovy šifry, výjimečně se používá „spravedlivější“ pojmenování systém Sestri-Beuafort.

Vzestup a pád polyalfabetických šifer

1. Morseovka

Samuel F. B. Morse vynalezl a patentoval v roce 1840 telegraf. Hned od počátku vyvstal požadavek podniknout taková opatření, aby se vyvrátila námitka zaměřená proti posílání soukromých zpráv telegraficky – totiž porušení soukromí. To vyvolalo značný zájem veřejnosti o šifrování, obdobně jako takovou pozornost vyvolalo např. používání Internetu v současné době.

2. Ochrana telegrafních zpráv

Francis O. J. Smith vydal komerční telegrafní kód pod názvem *The Secret Corresponding Vocabulary; Adapted to Morse's Electro-Magnetic Telegraph* (Slovník tajného dopisování upravený pro použití ve spojení s Morseovým elektromagnetickým telegramem).
Smithův průkopnický kód následovaly desítky a nakonec stovky dalších obchodních kódů. Některé měly až 100 000 položek a některé jen několik málo set. V jiných systémech zase byl zaveden velký počet kódů pro celé věty (Smith měl ve svém kódu 67 vět). Tato opatření byla zavedena zejména z důvodu snížení telegrafních poplatků.

3. Francis Beaufort (systém Beuafort)

Lidé však stále hledali jiný jednoduchý, levnější a přitom bezpečný způsob šifrování zpráv, které si pomocí telegrafu předávali. Takový systém jim nabídl Angličan admirál sir Francis Beaufort (1774-1857). Systém se stal postupně všeobecně známý díky tomu, že byl základem rozšířené pomůcky pro šifrování telegramů, která se v Anglii úspěšně prodávala pro ochranu krátkých telegrafních zpráv. Pomůcka se skládala z převodové tabulky, podrobného návodu k použití a návodu na vytvoření vhodného hesla.
Šifrování probíhá následovně: šifrant zapíše smluvené heslo – klíč nad otevřený text, heslo opakuje tak dlouho, až pokryje celý otevřený text.
Nyní vybere řádek, který začíná prvním písmenem otevřeného textu, očima vyhledá v tomto řádku první znak klíče a pak se podívá do tabulky na znak v prvním řádku ve stejném sloupci. Takto získaný znak je prvním znakem šifrového textu. Postup se opakuje zcela shodně pro další znaky otevřeného textu.

Příklad šifrového textu (domluvené heslo - klíč PAVEL):

```
Klíč:                PAVELPAV
Otevřený text:       ALBATROS
Šifrový text:        PPUESYMD
```

Při dešifrování příjemce nejdříve nadepíše smluvené heslo nad znaky šifrového textu. K určení znaků otevřeného textu postupuje formálně shodně jako při šifrování (to je určitá výhoda proti Vigenérovu systému). Příjemce vybere řádek, který začíná písmenem šifrového textu, očima vyhledá v tomto řádku odpovídající znak klíče a pak se podívá do tabulky na znak v prvním řádku ve stejném sloupci. Takto získaný znak je hledaný znak otevřeného textu. Postup se opakuje až po dešifrování posledního znaku.

4. Porovnání polyalfabetických šifrových systémů

Rozdíl mezi těmito jednotlivými představenými polyalfabetickými systémy (Beaufort, Beaufortova varianta Vigenérovy šifry a Vigenére) je v pořadí výběru řádků a sloupců, které určují šifrový znak.

Pro lepší zapamatování, jak se šifrovalo podle těchto tří systémů, a pro jejich porovnání jsme pro vás připravili dvě tabulky. První tabulka porovnává postup šifrování podle těchto systémů.

Šifrování

Tritheim, Cardano Vigenére, Gronsfeld			Beuafort			Beaufortova varianta Vigenérova systému	
	O(1)			Š(3)			Š(3)
			Beuafort				
K(2)	Š(3)		O (1)	K(2)		K(1)	O(2)

Druhá tabulka porovnává způsoby dešifrování podle těchto tří systémů.

Dešifrování

Tritheim, Cardano Vigenére, Gronsfeld			Beuafort			Beaufortova varianta Vigenérova systému	
	O(3)			O(3)			Š(1)
K(1)	Š(2)		Š (1)	K(2)		K(2)	O(3)

Z grafického vyjádření těchto systémů jasně plyne, že systém Beaufort je reciproční (logicky opačný) systém. Pokud jde o šifrování a dešifrování, je vidět, že jeho algoritmus práce se znakem a klíčem je formálně shodný, a to bez ohledu na to, jestli se zpracovává otevřený nebo šifrový znak. Z grafického vyjádření je současně vidět, že systém Vigenére a Beaufortova varianta jeho systému jsou „obrácené operace“. Postup pro šifrování a dešifrování je v těchto systémech odlišný. Naopak šifrování v jednom z těchto systémů je formálně shodné s postupem dešifrování ve druhém ze systémů a naopak.

Francouz de Viaris (1847-1901) publikoval v roce 1888 dvoudílný příspěvek, který později vyšel jako kniha pod názvem *Cryptographie*. Příspěvek je cenný tím, že pomocí vzorců osvětlil konstrukci výše uvedených polyalfabetických systémů.

K jejich odvození použil de Viaris nejprve převod znaků abecedy na čísla (A = 0, B = 1, … L = 11, …, P = 15,…, V = 21, … Y = 24, Z = 25). Při sestavování algebraických rovnic upravil definici sčítání a odčítání tak, aby výsledek vždy opět ležel v rozmezí hodnot 0 až 25 a šel zpětně převést podle stejné tabulky na některý znak abecedy. Byl-li součet dvou čísel větší než 25, odečetl od výsledku hodnotu 25 a opačně, byl-li rozdíl menší než 0, přičetl číslo 25. Dále zavedl označení pro libovolný znak šifrového textu jako řecké písmeno χ (chí), libovolný znak klíče Γ (gama) a libovolný znak otevřeného textu písmeno c. Následně dokázal, že algebraický vzorec $c + \Gamma = \chi$ popisuje Vigenérovo šifrování, a to samozřejmě bez

ohledu na to, jak je technicky realizováno (tabulkou, kryptografickým proužkem, šifrovacím kotoučem).

Použijeme-li dnes běžnější značení (*K* znak klíče, *O* znak otevřeného textu a *Š* znak šifrového textu), pak vzorce jednoznačně popisující nejpoužívanější polyalfabetické systémy jsou:

systém	**šifrování**	**dešifrování**
Vigenére	$O + K = Š$	$Š - K = O$
Beaufort	$K - O = Š$	$K - Š = O$
Varianta Beaufort	$O - K = Š$	$Š + K = O$

Tento de Viariův objev, kterému autor nepřikládal příliš velký význam, umožňuje odstranit jednu ze slabin výše uvedených systémů, a tou byla zdlouhavost a časté chybování při šifrování a dešifrování za použití vyhledávání v tabulce 26 × 26.

5. Pád : Friedrich Wilhelm Kasiski

Důstojník pruské armády Friedrich Wilhelm Kasiski zveřejnil roku 1863 v knize *Die Geheimschrifften und die Dechiffrirkunst* (Tajné šifry a umění je dešifrovat) obecnou metodu na řešení Vigenérovy polyalfabetické šifry (s periodickým heslem) pomocí vyhledání periody hesla a následným zredukováním na řešení řady monoalfabetických šifer.

Happy End (absolutně bezpečný systém)

Zdálo by se, že vzhledem ke kryptoanalytické analýze Friedricha Wilhelma Kasinského, odzvonilo periodickým polyalfabetickým šifrám Vigenérova typu. Jenže na začátku dvacátého století se stalo něco, co tyto konstrukce opět vzkřísilo a „nepatrným trikem“ (kvalitní heslo se prodloužilo na délku otevřeného textu) z nich udělalo absolutně bezpečný šifrový systém…

1. Gilbert S. Vernam

Píše se rok 1917, Gilbert S. Vernam, zaměstnanec americké firmy AT&T, vymyslel polyalfabetický šifrovací stroj schopný používat náhodný neopakující se kód. Do zařízení se vkládala děrná páska s otevřeným textem a současně i děrná páska, na které byl náhodně vyděrovaný klíč (heslo). Šifrový text vznikl sečtením příslušných bitů obou pásek modulo 2 (0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, ale 1 + 1 = 0).Velkou výhodou zařízení bylo, že proces šifrování a dešifrování probíhal úplně stejně a automaticky. Tento systém je bezpečný, pokud je klíč (heslo) náhodný, je stejně dlouhý jako otevřená zpráva a použije se pouze jednou (tzv. systém One Time Pad).

2. Claud Elwood Shannon

V časopise *Bell System Technical Journal* vyšly dvě práce dalšího z velikánů kryptologie dvacátého století Clauda Elwooda Shannona. Práce otiskuje časopis v roce 1948 a 1949, jedná se o články "Matematická teorie sdělování" a "Sdělovací teorie tajných systémů". Prvý z článků dal vznik teorii informací, druhý článek pojednával o kryptologii v termínech informační teorie. Pojetí nadbytečnosti (redundancy) je hlavním termínem, který Shannon zavedl. Velice zhruba řečeno nadbytečnost znamená, že ve zprávě je vysíláno více informace, než je skutečně třeba k poskytnutí celé zprávy. Jako elementární příklad uvádí Shannon nadbytečnost psaní písmene *u* v bigramu *qu*, protože v anglických slovech po písmenu *q* vždy následuje *u*. Shannon dále poukazuje na to, že nadbytečnost dává podklad ke kryptoanalýze.

Píše: „Ve … většině šifer je to pouze existence nadbytečnosti v původních zprávách, která činí řešení možným.“
Oba články fakticky odstartovaly moderní pojetí matematického zkoumání základů kryptografie a kryptoanalýzy. Díky této teorii se podařilo dokázat, že systém navržený Gilbert S. Vernamem, který „vyrostl“ z polyalfabetických šifrových systémů je *bezpečný kryptosystém (tzv. absolutně bezpečný šifrový systém)*. Dodnes je tento způsob šifrování jediným známým absolutně bezpečným systémem.

3. Příklady použití

Kubánská krize na začátku šedesátých let, která málem vyústila v jadernou válku, vyvolala potřebu rychlého a bezpečného spojení mezi USA a SSSR. Obě mocnosti se domluvily na vybudování horké linky mezi hlavami obou států. Horká linka byla uvedena do provozu 30. 8. 1963. Kreml i Bílý dům si vzájemně vyměnily heslové materiály - pásky. Otevřené texty se převedly do dálnopisného kódu a sčítaly se s heslovým materiálem, heslová páska byla ihned po použití automaticky ničena, čímž se mělo zamezit jejímu nechtěnému opětnému použití. Při zavedení tohoto systému se použilo zařízení ETCRRM-II (Electronic Teleprinter Cryptographic Regenerative Repeater Mixer II). Každou hodinu se přenášely zkušební relace.

Modifikovaný systém byl v praxi používán v době studené války tajnými službami (BND, CIA apod.). Otevřený text se nejprve převedl do číselné podoby a to zpravidla pomocí jedno-dvoumístné číselné záměny. Protože takto by byl text lehce luštitelný, následovalo přičtení dohodnuté číselné sekvence – hesla. Pokud byla dodržena určitá pravidla, heslo bylo dostatečně dlouhé, bylo kvalitní (náhodné a stejně pravděpodobné) a nebylo kompromitováno, byla výsledná šifra při záchytu nerozluštitelná (**absolutně bezpečná šifra**).

Příklad:
Použijeme jednu z originálních převodových tabulek používaných západoněmeckou tajnou službou BND (Bundes Nachrichten Dienst) během studené války. Tabulka se podle „konstrukčního hesla“ nazývala DEIN STAR (tvá hvězda)

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

```
Otevřený text (o):              Děkuji za pozornost.
Převod do mezinárodní abecedy: DEKUJI ZA POZORNOST
Převod podle tabulky (O):      0 1 57 63 62 2  69 8  61 60 69 60 9 3 60 4 7
Rozpis do pětimístných skupin: 01576 36226 98616 06960 93604 7
Heslo (K):                     75409 78210 87302 10834 52019 3
Vigenére (O + K = Š):          76975 04436 75918 16794 45613 0
```

Pro úplnost odkazy na další tabulky včetně verze DEIN STAR pro NDR:
http://kryptografie.de/kryptografie/chiffre/dein-star.htm
http://www.cryptomuseum.com/spy/bnd_conv/index.htm

[1] Vondruška, P.: Kryptologie, šifrování a tajná písma, edice OKO, Albatros 2006
http://crypto-world.info/oko/index.php
[2] Vondruška,P.: Přehled a historie polyalfabetických šifer, Mikulášská kryptobesídka 2006 7.-8.prosinec 2006, Praha, http://mkb.buslab.org/cfp.htm

B. Matematizace komplexní bezpečnosti v ČR, část I.

RNDr. Jaroslav Hrubý, CSc. (hruby.jar@centrum.cz)

RNDr. Jaroslav Hrubý, CSc. je vědeckým pracovníkem FzÚ AV ČR a řešitelem grantu T300100403 v oblasti kvantového počítání. Je předsedou odborné skupiny kryptologie při matematické sekci JČMF (GCUCMP), a byl předsedou kryptologických konferencí PRAGOCRYPT 96 a EUROCRYPT'99. Je členem ISACA a IACR, kde v r. 98-99 byl členem předsednictva, dále je členem FVS JČMF a EPS.

1. Úvod

Komplexní pojetí všech aspektů bezpečnosti ve společnosti představuje z matematického hlediska složitý matematický systém, který má díky rychlým změnám nelineární vývoj.

Bez matematizace a kvantifikace komplexní bezpečnosti, zavedení metrik a aplikace známých i nových matematických modelů na bezpečnostní data a veličiny nelze objektivně takto složitý systém hodnotit, řídit a pokusit se predikovat v reálném čase.

Stanovení míry komplexní bezpečnosti a rizika komplexní bezpečnosti by mělo být v popředí zájmu každé společnosti i celé ČR, jako člena EU a NATO. Pro její znalost je zapotřebí stanovit měřitelnost, kvantifikaci a realizovat matematizaci komplexní bezpečnosti jako celku.

K tomu je nezbytné mít kvalitní databáze bezpečnostních dat s co nejdelší historií a kvalitní týmy expertů používající matematický aparát pro analýzy těchto dat pro prokazatelnou bezpečnost popřípadě pro predikci vývoje bezpečnostních událostí, a to s co největší pravděpodobností predikce.

V r. 2001 byla v práci [1] rozebrána tato potřeba matematizace a kvantifikace komplexní bezpečnosti, včetně použití nových technologií a bezpečnostních manažerských systémů řízení pro predikci vývoje komplexní bezpečnosti a predikci nových rizik v globálním světě.

Bylo v ní ukázáno, že bezpečnost společnosti a každé organizace se stává jedním z jejích nejvýznamnějších aktiv, a že informační bezpečnost je nedílnou součástí celkové bezpečnosti každé společnosti v informačním světě a je součástí všech jejich aktiv.

Bohužel situace v ČR se v tomto směru příliš nezměnila. Zatímco za posledních šest let byl učiněn pokrok ve vnímání bezpečnostních potřeb ve společnosti, posun k matematizaci bezpečnosti v ČR nenastal.

Matematické modelování bezpečnosti se stalo pilířem bezpečnostních strategií u velmocí jako je USA, Rusko … Tyto chápou bezpečnost jako otázku bytí a nebytí svého společenství, a to nejenom v oblasti vojenské, ale i ekonomické.

Na konferencích jsem s řadou kolegů diskutoval problém, bylo-li by možné např. predikovat hrůzný teroristický čin z 11. září v New-Yorku použitím matematického aparátu, jako např. nelineárních modelů, časových řad, aplikací aparátu neuronových sítí, kvantové teorie her, jakožto nástroje k hledání nových vítězných strategií atd, na bezpečnostní data (informace). Většinou jsme se shodli, že s velkou pravděpodobností ano, ale:

1) bezpečnostní databáze musí být kvalitní, tj. co nejúplnější s dostatečnou historií bezpečnostních dat, věrohodná, archivovaná data musí být rychle přístupná apod.
2) musí být vybrány správné matematické modely, včetně zahrnutí např. modelování deterministického chaosu apod. (pro dokreslení poznamenejme, že dáme-li počítači dostatečnou informaci o Mozartově stylu hudby, bude aplikací predikčních modelů vytvářet hudbu podobnou. Použijeme-li kvantového šumátoru a matematických modelů na predikci vývoje finančních kurzů na burze v New-Yorku, můžeme s velkou pravděpodobností **p** zbohatnout, avšak s pravděpodobností **(1-p)** zchudnout (bohužel křišťálová koule na predikci neexistuje, i kdybychom do výpočtů zahrnuli i možnost

pádu meteoritu).

3) Modelování musí být co nejrychlejší a data, týkající se modelovaného problému, musí být co nejrychleji aktualizována.

Ideální splnění těchto třech bodů (nejsou vyčerpávající) v současnosti lze splnit pouze částečně, s jistými omezeními technologickými i teoretickými např. ve smyslu problémů matematické složitosti, kde ani aplikace kvantových počítačů nebude v budoucnosti všelékem (pozn. že existují kvantově složité problémy z hlediska matematické složitosti, které neřeší ani kvantový počítač).

Naproti tomu jsou však reálně dostupné IS/ICT technologie, legislativa ČR včetně norem týkajících se této oblast, aby existovaly solidní bezpečnostní databáze, analyzované známým matematickým aparátem a modely s vazbou na bezpečnostní procesy, zrcadlící se v bezpečnostní předpisové základně, aby nedocházel k opakovaným bezpečnostním incidentům (opakované úmrtí pacientů v nemocnici, opakované úniky radioaktivní vody apod.).

Proto je nutno v ČR upozornit na nutnost věnovat pozornost matematizaci bezpečnosti, a to obzvláště v době, kdy budou do čela společností stavěni manažeři, kteří v rámci středoškolského vzdělání neměli ani povinně maturitu z matematiky.

Potřeba matematizace platí pro komerční společnosti, státní orgány i společnost jako celek.

Zopakujme si základní kuchařku, jak na to.

Představme si pro konkrétnost komerční společnost s rozvinutým informačním systémem, na kterém je závislá většina jejích aktiv, která je klíčová pro ČR a její bezpečnostní incidenty mají politické důsledky (např. jaderná elektrárna).

Dokonalou ochranu informační bezpečnosti v této společnosti lze dosáhnout pouze jejím nerozdělitelným vnořením do komplexní bezpečnosti této společnosti, ale zároveň komplexní bezpečnost musí být analyzována a řízena IS/ICT ve společnosti

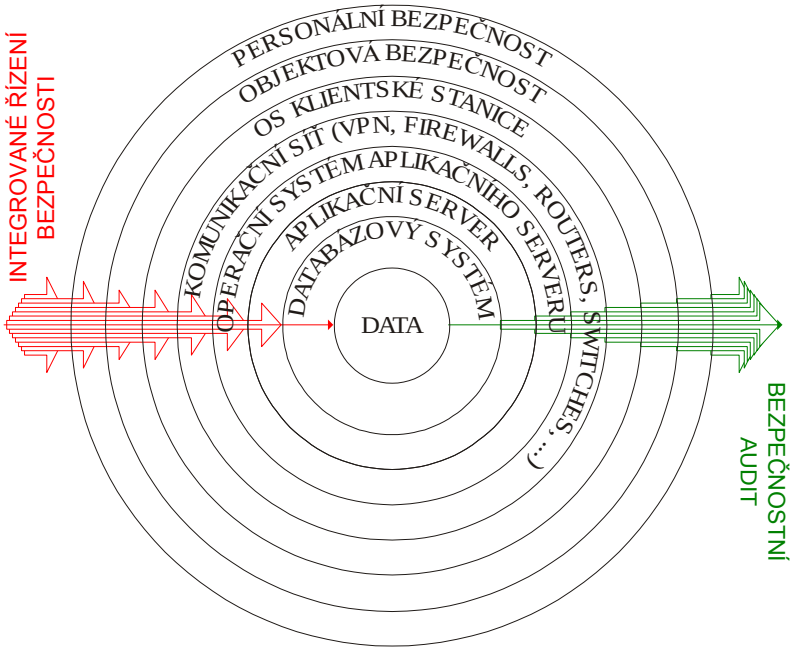
Komplexní bezpečnost je realizována provázaností korporátní a informační bezpečnosti ve společnosti, což znamená, že korporátní bezpečnost organizace prolíná informační bezpečnost v řadě jejich oblastí a naopak.

Pro názornost si opět představme slupkový model bezpečnostních vrstev, chránící ve svém jádře data. Informace obsažená v datech je chráněna vrstvami bezpečnostních mechanismů týkající se předpisů, personalistiky, budov, klientských stanic, komunikační sítě, operačních systémů aplikačních serverů, databázového systému, ale také naopak bezpečnostní informace o budovách, lidech, počítačích, sítích, změnových řízeních atd. je součástí jejich ochrany.

Slupkový model je inversní v tom smyslu, že i informace v datech chrání osoby, budovy, a také informační technologie a systémy.

Bezpečnost IS/ICT je tudíž od korporátní bezpečnosti neoddělitelná.

Takto komplexně provázané bezpečnosti informačních systémů, korporátní, personální, fyzické atd. chápeme jako jednu komplexní bezpečnost (KB) organizace.



Obrázek 1 – Slupkový model bezpečnostních vrstev

Je zřejmé, že tato KB je z matematického hlediska složitý dynamický systém sám o sobě, který je v průniku všech částí, činností a existence celé společnosti. Pokud se vedení společnosti pokouší nějakými metodami, např. ekonomickými modely, ekonometrií apod. řídit celou společnost z hlediska ekonomického růstu a nárůstu aktiv, mělo by umět mapovat, popsat, řídit a předpovídat vývoj tohoto ústředního aktiva – KB, který všechna ostatní aktiva chrání.

Tento problém je o to složitější, že IS/ICT prorůstají téměř do každé činnosti společnosti, že rychlost změn v tomto prorůstání uvnitř společnosti je značná, ale i změny ve vývoji IS/ICT jsou dynamické – komplexní bezpečnost organizace není tedy stacionární komplexní systém, ale systém nesmírně dynamický, tj. s vysokým gradientem změn v čase.

Vzhledem k dynamickému rozvoji hlavně v oblasti informačních systémů, informačních technologií, informační bezpečnosti, a také kryptologie, je nezbytné, aby správa informační bezpečnosti ve všech organizacích a společnostech v ČR byla v souladu s KB organizace a dále se sérií základních mezinárodních dokumentů vydaných v sérii ISO/IEC, platných u nás i v EU, a to takovým způsobem, aby:

- bezpečnostní opatření byla komplexní a dostatečně rychle implementována,
- systém správy komplexní a informační bezpečnosti byl řiditelný v reálném čase a otevřený pro jakékoliv budoucí změny,
- systém správy KB včetně informační bezpečnosti plně akceptoval zákony v ČR, týkající se této oblasti ,
- v maximální míře využil stávajících systémů v organizace, aby jeho realizace byla v optimalizovaném poměru mezi finančními náklady a výsledkem dosažené bezpečnostní úrovně.
- úroveň bezpečnosti bylo možno jednoznačně hodnotit.

Cílem je dosáhnout stabilní vysokou úroveň KB ve společnosti s minimálním hodnotou míry rizika.

Cesta k tomuto cíli je přes matematizaci a kvantifikaci KB, včetně aplikace modelů popisujících dynamiku systému a jeho vývoj od regulárního chování k chaotickému.

V této práci se pokusíme nastínit jednu z možných cest k tomuto cíli. Ve 2. kapitole stručně vysvětlíme, jak je nutno chápat matematizaci a kvantifikaci KB. Ve 3. kapitole se věnujeme matematizaci metodiky CRAMM (lze vybrat i metodikou jinou, kterážto umožní získávat kvanifikovaně bezpečnostní informace, ukládané do bezpečnostních databází, pro další analýzy) pro analýzu rizik, jakožto metodiky získávající a hodnotící informace o aktivech, hrozbách a zranitelnosti z pohledu KB.

2. Matematizace a kvantifikace KB

Vycházíme z předpokladu, že v organizacích a společnostech je v ČR vše v souladu s platnými zákony a normami.

Bezpečnostní audity a doporučení, která se většinou soustředí na oblast bezpečnosti IS/ICT, méně již na korporátní celkovou bezpečnost a ještě méně na jejich průnik, tj. celkovou bezpečnost všech aktiv společnosti, a tedy nejenom informačních aktiv, jsou však pouze subjektivní, pokud nevychází z jednotné kvantitativní metriky pro hodnocení aktiv, rizik a hrozeb, působících na tato aktiva ve společnosti.

Pro nedostatečnost těchto subjektivních hodnocení si jako další příklad uvedeme oblast bankovnictví, kde jistě u renomovaných bank provádí audity neméně renomované společnosti, dávající žádaná důležitá razítka, a přesto např. v přímém bankovnictví došlo k opakovaným případům „phishingu“ [2] apod.

Je to možné právě proto, že na základě bezpečnostních dat banky, v průniku s rozvojem IS/ICT a bezpečnostních trendů ve světě, nejsou přijímána opatření před, ale vždy až po bezpečnostních incidentech. Možná je to dáno tím, že banky málo vydělávají, poplatky klientů za služby jsou „nízké“, a proto zavedení podepsaných e-mailů elektronickým podpisem s ověřitelným certifikátem banky by bylo již před několika lety, tak „drahé“.

Snad po zavedení pokročilých metod Baselu II (směrnice pro banky), včetně aplikací matematických metod pro určení operačního rizika, bude v této oblasti kladen větší důraz na kvantitativní metriky a méně na auditní dojmologie.

Takové jednotné metriky, vzniklé na základě analýzy pro různé oblasti bezpečnostních dat (státní správa, bankovnictví, telekomunikace, atd.), v ČR nejsou předepsány, a proto se při auditech jedná o často pouhou „dojmologii“ hodnotitelů (auditorů), kteří hodnotí soulad, či nesoulad stavu se zákony, předpisy a normami, pouze ze svého subjektivního hlediska, pokud to, co posuzují, nebylo kvantifikováno podle jednotného měřítka. Pro kvantifikaci je nezbytná znalost všech hodnotitelů, kteří doplňují informace do bezpečnostní databáze, jak bezpečnostní informace hodnotit a jak měřit. Je tedy nezbytné tyto metriky zavádět a předpisy vyžadovat bezpečnostní výpočty na základě bezpečnostních dat pro prokazování bezpečnosti.

To se bohužel týká i vyhlášky č. 528/2005 Sb. k zákonu č.412/2005 Sb., kde vyhodnocení rizik se provádí:

a) identifikací stupňů utajovaných informací a zjištěním množství utajovaných informací, které se v objektu vyskytují nebo budou vyskytovat, zejména z hlediska následku jejich vyzrazení nebo zneužití,
b) popisem a vyhodnocením hrozeb, kterým jsou tyto utajované informace vystaveny,
c) popisem a vyhodnocením zranitelnosti utajovaných informací vůči těmto hrozbám,
d) stanovením míry rizika, jako "malé", "střední" nebo "velké", na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací.

Nikde, ani v příloze nejsou uvedeny metriky, jak vyhodnotit a jakou kvantitativní hodnotu tedy přiřadit hrozbám a zranitelnosti. Bylo by záhodné takovéto metriky a kvantitativní hodnoty pro různé druhy organizací uvést v příloze této vyhlášky (je zřejmé, že jiné metriky budou pro banku a jiné pro jadernou elektrárnu), aby výsledek byl objektivizován, a nezáležel na osobním vnímání hodnotitelů.

Proto vyvstává jednoznačná potřeba vytvořit tyto metriky pro různé oblasti, a to ve státní i v komerční sféře, aby nezávislí hodnotitelé docházeli alespoň v limitním případě ke shodnému výsledku.

To byl také hlavní požadavek při zavádění kritérií pro hodnocení bezpečnosti v informačních technologií (ITSEC) [4] a metodologie hodnocení (ITSEM) [5].

Dále je nutno vytvořit jednoznačné postupy, jak měřit a hodnotit, tak jak je tomu v přírodních vědách, včetně implementace norem pro měření na všechny oblasti KB. To se zatím v ČR nerealizuje a zde je optimální příležitost spolupráce akademické obce, státních orgánů, ale také komerční sféry pro vytvoření těchto metrik a postupů ve shodě s legislativou ČR a tím, co je již v EU akceptováno.

V nemalé míře se tedy jedná o matematizaci hodnocení a řízení procesu bezpečnosti, a to v celé jeho šíři, počínaje globální bezpečnostní politikou, analýzou rizik, návrhu bezpečnostních opatření, bezpečnostní politikou pro IS/ICT, a to až do bezpečnostního projektu a implementaci opatření do jednotlivých činností a provozu v organizaci.

Řízení KB by mělo být minimálně na stejné úrovni jako celkové ekonomické řízení společnosti a to právě z důvodu průniku KB do všech ekonomických aktivit společnosti.

O matematickém modelování, ekonometrii v oblasti ekonomického řízení nikdo nepochybuje a má i v ČR dobrou tradici a úroveň. V oblasti KB je situace na mnohonásobně nižší úrovni a mnohdy je hrubě podceněna.

Přesto je KB z matematického hlediska stejně složitým systémem jako ekonomie s řadou skrytých parametrů, nahodilostí atd.

Matematizací KB zde nerozumíme pouze to, co se jí rozumí ve velmi kvalitní metodice analýzy rizik, ale na universální úrovni následující:

- výběr vhodných metodik pro dotazníkové metody pokrývající celou problematiku KB a výběr vhodných technických detektorů bezpečnostních dat a informací,
- škálování otázek v dotazníkových metodách pro různé bezpečnostní úrovně požadované na IS/IT, včetně škálování množství a požadavků na technické prostředky získávající bezpečnostní informace,
- aplikovaní matematických statistických metod na tato hodnocení, za účelem prověření věrohodnosti získaných bezpečnostních informací a korelací mezi odpověďmi a hodnoceními různých dotazovaných subjektů v průniku s informacemi získanými z technických prostředků (z měřičů průniku do sítě, z firewalů apod.),
- modelování funkce míry rizika f(a,h,z), která je pro každou oblast specifická a je funkcí aktiv(a),
- hrozeb (h) a zranitelnosti (z),
- matematický výpočet dopadu hrozby,
- výběr dat bezpečnostní databáze, která mají časový vývoj, sestavení časových řad, včetně aplikace modelů predikujících jejich dynamiku a vývoj, predikce vývoje bezpečnosti a predikce nových rizik,
- aplikaci manažerských bezpečnostních systémů na bezpečnostní databázi,

- matematické modelování různých strategií při vzniku havárií, použitím optimalizace metod, aplikace neuronových sítí, teorie her apod.

Je zřejmé, že tento výčet není úplný a že lze aplikovat ještě další řadu známých vědeckých metod pro zkoumání složitých dynamických systémů, i na KB.

Aby matematické zpracování bezpečnostních dat bylo efektivní, je pro vytvoření bezpečnostní databáze nutné vytvořit společná měřítka a kritéria:

- jak unifikovaně bodově hodnotit proměnné a,h,z,
- jak škálovat dotazy (na procesy, služby, řízení apod.) a požadavky pro technické detektory bezpečnostních dat pro různé kategorie bezpečnostní úrovně (např. pro bezpečnostní úrovně EAL 1,2,3,…),
- jak volit funkce f(a,h,z) např. pro banky, telekomunikační společnosti, energetické společnosti, různé oblasti státní správy apod.,
- jakými matematickými a bezpečnostními modely popisovat bezpečnost pro danou společnost, bezpečnostní úroveň atd.

Je nezbytné, aby stejně jako pro státní správu vznikly národní profily pro hodnocení bezpečnosti v komerční sféře, které budou zřejmě jiné pro různé oblasti, jako např. bankovnictví, telekomunikace, energetika, apod. Toto je nezbytné i pro případné objektivní udělování sankcí ze strany nadřízených úřadů.

Kvantifikace hodnocení KB umožňuje vytvořit bezpečnostní databázi s časovým vývojem, nad kterou fungují matematické modely, bezpečnostní modely a řídící systémy, tj. to, co nazýváme matematizace bezpečnosti.

Jedině takto lze konstruovat výše zmíněný kvantitativní nástroj, který v průniku s kvalitativním hodnocením umožňuje kvalitní manažerská rozhodnutí, chránící všechna aktiva společnosti vůči téměř všem hrozbám.

Slovo téměř je zde podstatné, protože tak, jako neexistuje absolutní bezpečnost (a vrcholem veškerého bezpečnostního snažení je se ji v nějaké rozumné limitě přibližovat), tak principiálně nelze předpovídat všechny možné hrozby v delším časovém horizontu.

V kratším časovém horizontu je predikce možná, a to s vysokou pravděpodobností výskytu nové hrozby.

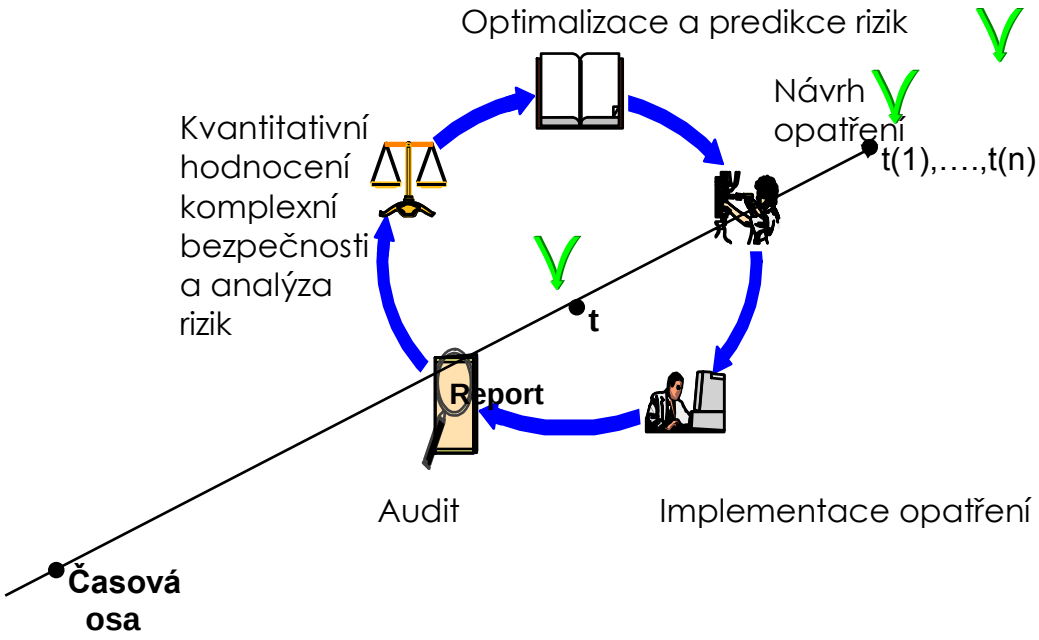
Bezpečnostní databází se zde rozumí multidimensionální datový sklad věrohodných bezpečnostních, informací (transformovaných na data) získaných netechnickými dotazníkovými metodami na úroveň procesů IS/IT infrastruktury ve společnosti v provázanosti na KB dle platných norem a legislativy. Tyto jsou doplněny informacemi z technických prostředků jako např. měřičů průniku, manažerských bezpečnostních systémů pro dohled nad sítí, detektorů garantujících objektovou a personální bezpečnost, atd. až po data ze zpravodajských prostředků. Tato data jsou řazena do časových řad pro podchycení dynamiky změn KB.

Věrohodnost dat je možné zajistit aplikací metod matematické statistiky a studiem korelací mezi jednotlivými informacemi s následným vyloučením informací nevěrohodných

Jak tedy postupovat při matematizaci a kvantifikaci bezpečnosti:

1. Definovat technické a netechnické zdroje informací a vytvořit bezpečnostní databázi ve společnosti.
2. Realizovat bezpečnostní cyklus.
3. Realizovat bezpečnostní cykly v časovém vývoji.

Obrázek 2 – bezpečnostní cyklus



Obrázek 3 – Znázornění realizace bezpečnostních cyklů v časech t(1), …, t(n) na časové ose

Pro predikci vývoje KB je možná aplikace standardních modelů pro tyto časové řady hodnot bezpečnostních dat, ale pro stabilitu KB je možné aplikovat modely hledajících souvislosti mezi jednotlivými faktory, bezpečnost ovlivňujícími, které ovlivňují dynamiku vývoje KB. Na jednu metodiku analýzy rizik (CRAMM) se pro příklad soustředíme.

3. Matematizace KB např. pomocí metodiky CRAMM

Z metodiky CRAMM vycházíme proto, že pro ní je vytvářeno národní bezpečnostní prostředí pro analýzu rizik v ČR (je však možné vybrat i metodiky jiné).

Cílem analýzy rizik je nalezení optimálního poměru mezi možnými ztrátami a náklady vynaloženými na bezpečnostní opatření, která by tyto ztráty měla omezit.
Pro splnění tohoto cíle je nutné získat věrohodné informace o aktivech (a), hrozbách (h) a zranitelnosti (z), a také správně určit funkci f(a,h,z) pro danou společnost. Zde může být klíčový přínos kvalitně provedené kvantitativní analýzy rizik včetně matematického zpracování, jelikož může ušetřit společnosti značné finanční prostředky pro dosažení požadované úrovně bezpečnosti.

Komplexní analýza rizik zahrnuje několik souvisejících činností:

- určení a odhad rizik
- vlastní analýzu rizik
- řízení a kontrolu rizik
- stanovení zbytkových rizik.

I když samotný CRAMM bez matematizace KB, tak jak je popsána výše, není oním nástrojem, který umožní popsat řídit bezpečnost ve společnosti, přesto je to metodika, kterou lze universálně zkoumat úroveň bezpečnosti IT/IS v návaznosti na KB ve společnosti a provést analýzu rizik.

CRAMM je metodika, která se skládá ze tří etap, z nichž každá je podporována cílovými dotazníky a pokyny, přičemž etapy lze zhruba charakterizovat následovně:

1.etapa
- identifikace fyzických, datových a softwarových aktiv,
- odhad hodnoty těchto aktiv podle možných ztrát,
- určení nejdůležitějších aktiv.

2.etapa
- sloučení aktiv do skupin,
- stanovení hrozeb vůči těmto skupinám,
- odhad zranitelnosti ,
- stanovení úrovně požadavku na bezpečnost pro jednotlivé skupiny.

3.etapa
- vypracování programu protiopatření k ochraně vybraných aktiv s danou úrovní bezpečnosti,
- porovnáním s existujícím programem proti opatření a provedení úprav a změn,
- provedení analýzy nákladu na protiopatření a hodnoty aktiv.

Správné použití programu CRAMM a stanovení správných vstupních údajů je umění. Bez doplnění alespoň základních statistických metod na vyhodnocování dotazníků nemusí být jeho účinnost při jednom použití optimální. Mnohonásobným použitím a značnou zkušeností hodnotitele lze se k optimálním výsledkům přiblížit, což je však oproti použití statistických

metod zdlouhavé. Rovněž tak funkce f(a,h,z) je universální, neakceptující charakteristiky jednotlivých společnosti

Doporučuje proto k statistickému zpracování dat použít např. osvědčené programy Mathematica nebo Matlab, které jsou vhodné i pro další modelování získaných bezpečnostních dat a informací.

CRAMM je v každém případě vhodný prostředek pro základní standardní analýzu rizik v rámci bezpečnostního cyklu – analýza, optimalizace, návrh opatření, implementace, audit. Je rovněž vhodný pro sběr bezpečnostních dat díky rozpracovaným dotazníkům (bohužel ne škálovaně na všechny bezpečnostní úrovně).

Lze jej požít i pro vytváření bezpečnostní databáze jako základní prostředek, který je nutno doplnit o další systémy kvantifikace a matematizace, včetně technických prostředků na řízení bezpečnosti.

KB ve společnosti by měla být řízena bezpečnostní radou (BR), která je zodpovědná i za kvalitní provedení analýzy rizik ve společnosti. BR by v každém případě měla stanovit nezávislou metodiku (případně několik nezávislých metodik) pro měření procesů bezpečnosti, které jsou důležité pro služby a činnosti společnosti.

BR společnosti si dále musí stanovit vlastní dotazníky, určit jejich škálování pro požadovanou bezpečnostní úroveň, definovat respondenty v průřezu přes celou společnost a zautomatizovat tento zdroj informací do bezpečnostní databáze.

Teprve takto včleněný CRAMM a doplněný CRAMM o další metodiky měření bezpečnosti včetně přijetí opatření a jejich implementace umožní auditem ukončit jeden ze série bezpečnostní cyklů.Ty by měly být opakovány po každém změnovém řízení, havarii apod., což vede jednoznačně k požadavku automatizace celého bezpečnostního cyklu.

BR musí neustále získané výsledky nezávislými metodikami křížově prověřovat s použitím statistických metod. Dále je musí konfrontovat s počty a typy skutečných bezpečnostních selhání ve společnosti, modelovat váhy významnosti jednotlivých případů apod.

Automatizace tohoto procesu je složitá úloha, ve které aplikace matematických metod z kapitoly o matematizaci je nezastupitelná. Rovněž je uměním spojení těchto dat získaných pomocí dotazníkových metodik s bezpečnostními daty ze softwarových a hardwarových bezpečnostních systémů. Problém je ve správném skloubení dat do skupin a jejich vzájemném vyvážení.

Pokud se toto BR podaří, může považovat bezpečnost ve společnosti za analyzovanou, změřenou a bezpečnostní databázi věrohodnou.

S kvalitní bezpečnostní databází lze teprve matematicky modelovat a optimalizovat přijatá doporučení na zvýšení KB. Zde se jedná o matematizaci, tj. jedná se o oblast aplikací matematických metod na informace v n-dimensionální bezpečnostní databázi, jako např.optimalizace, metoda minimální entropie, aplikace samoučících se systémů (např. neuronových sítí apod.),nelineárních modelů, teorie her atd.

Dále se jedná o určení bezpečnostních modelů prosazujících KB ve společnosti a aplikaci řídících manažerských systémů v n-dimensionální bezpečnostní databázi a síťových manažerských systémů a modelování optimalizace bezpečnosti v závislosti na vynaložených finančních prostředcích.

Nakonec lze i aplikovat predikční modely časových řad na predikci nových rizik z časových řad událostí v bezpečnostní časově doplňované databázi.

V bezpečnosti hraje podstatnou úlohu havarijní plánování a plány a postupy při obnově do původního nebo vylepšeného stavu. Rovněž v této oblasti hraje kvantifikace a matematizace bezpečnosti nezastupitelnou roli.

Bez matematizace však nelze dynamicky řídit bezpečnostní procesy.

C. Mikulášská kryptobesídka , Call for Papers

6. – 7. prosinec 2007, Praha , http://www.buslab.cz/mkb

Základní informace

Mikulášská kryptobesídka, český a slovenský workshop, se koná letos posedmé. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *6. prosince 2007* a (b) půldne prezentací příspěvků a diskusí v pátek *7. prosince 2007*. Pro workshop jsou domluveny zvané příspěvky:

- **Willi Meier** (Fachhochschule Nordwestschweiz) o návrhu a analýze kandidátů eSTREAM,
- **Claudia Diaz** (KU Leuven) na téma steganografických metod a útoků proti nim,
- **Vlastimil Klíma** na téma hašovacích funkcí,
- **Zdeněk Říha** na téma kryptografických mechanismů používaných v elektronických pasech a
- **Pavel Vondruška** – exkurz do historie kryptologie.

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.buslab.org.

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy příspěvků (5-15 stran A4) připravené pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo LaTeX a to tak, aby na uvedenou adresu přišly nejpozději do *2. října 2007*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2007 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *23. října*. Příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), do *20. listopadu*.

Důležité termíny

Návrhy příspěvků:	2. říjen 2007
Oznámení o přijetí/odmítnutí:	23. říjen 2007
Příspěvky pro sborník:	20. listopadu 2007
Konání MKB 2007:	6. – 7. prosince 2007

Programový výbor

Petr Hanáček, FIT VUT v Brně
Vašek Matyáš, FI MU, Brno – předseda
Martin Stanek, FMFI UK, Bratislava
Tomáš Rosa, eBanka
Luděk Smolík, FI MU, Brno
Jiří Tůma, MFF UK, Praha
Jozef Vyskoč, VaF, Bratislava

D. O čem jsme psali v červnu 2000 – 2006

Crypto-World 6/2000

Příloha : Navajo Code Talkers, revize z 15.6.1945, soubor Dictionary.htm

Crypto-World 6/2001

Příloha : priloha6.zip
(fotografie Security 2001, témata přednášek na konferenci Eurocrypt´2001)

Crypto-World 6/2002

Crypto-World 6/2003

Crypto-World 6/2004

Crypto-World 6/2005

Crypto-World 6/2006

Crypto-World 6/2007

E. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/