Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 13, číslo 4/2011 **15.duben**

4/2011

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1349 registrovaných odběratelů)

Obsah :

A. Československé šifry z obdobia 2. svetovej vojny Diel 4., Šifra „Rímska deväť“

Jozef Kollár, jmkollar@math.sk
KMaDG, SvF STU v Bratislave

Mnohé informácie o československých šifrách z obdobia 2. svetovej vojny mi stále chýbajú. Preto ak niekto viete doplniť, prípadne opraviť mnou uvádzané popisy šifier (TTS, Rímska 2, 8, 9, 10, 13, Eva, Marta, Růžena, Utility a Palacký), alebo máte akékoľvek informácie o ďalších československých šifrách z obdobia 2. svetovej vojny, poteší ma, ak mi o tom pošlete správu.

4 Šifra „Rímska deväť“

Šifra „Rímska deväť“ bola v princípe šifrou typu SP, t.j. pozostávala zo substitúcie znakov dvojcifernými číslami a následného pričítania periodického hesla. K tomuto základu sa alternatívne mohlo pridať ďalšie pričítanie periodického hesla a prípadne spätná substitúcia čísel za znaky medzinárodnej abecedy. Takže typ šifry by sa správnejšie mohol označiť ako SP(P)(S), pričom operácie v zátvorkách sú voliteľné. Žial, nie je mi známe, či sa tieto voliteľné prešifrovania aj reálne v praxi využívali a prípadne v akých variantách. Túto šifru používala napríklad stanica Pavla v operácii Sulphur.

Popis šifry „Rímska deväť“ je uvedený v knihe [2] na stranách 119–120.

4.1 Všeobecný popis a príklad šifrovania depeší

Pri šifrovaní sa najskôr substituovali znaky za čísla. Z uvedeného zdroja nie je zrejmé, aká substitučná abeceda sa používala. V [2] je len spomenuté, že sa používala 49 znaková substitučná tabuľka. Zrejme sa teda jednalo o rovnaké písmená a znaky, aké sme použili v popise „rímskej osem“. Tam sme použili tiež 49 znakovú tabuľku, rozdiel bol len v tom, že pri „rímskej osem“ mali niektoré znaky viacero číselných vyjadrení, čiže sa jednalo o homofónnu substitúciu. V prípade „rímskej deväť“ sa jedná o jednoduchú substitúciu. Takouto substitučnou tabuľkou by mohla byť napr. tabuľka 1 na strane 3. Poradie špeciálnych znakov je upravené tak, aby zodpovedalo príkladu z [2] (str. 119)[1]. Mierne sa teda líši od poradia špeciálnych znakov pri „rímskej osem“.

[1]Tento príklad je sám o sebe dosť mätúci, pretože sa tam vyskytujú znaky Ď a Ň, ale ich číselné vyjadrenie zodpovedá znakom D a N. Ďalej tam je znak - ako oddeľovač slov,

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0		A	B	C	Č	D	E	Ě	F	G
1	H	I	J	K	L	M	N	O	P	Q
2	R	Ř	S	Š	T	U	V	W	X	Y
3	Z	Ž	-	.	:	,	”	/	?	!
4	1	2	3	4	5	6	7	8	9	0

Tabuľka 1: Česká 49 znaková abeceda pre „rímsku deväť“

Pri šifrovaní je potrebné heslo. Toto heslo slúži na vytvorenie čísla, ktoré sa periodicky pričíta k textu. Údajne bolo používaných 12 hesiel, ktoré vychádzali z prvých dvoch slôh básne Jána Nerudu *„Jen dál“*. Podľa ukážky z [2] boli heslá približne tridsaťznakové reťazce. My si ako heslo zvolíme Periklov[2] citát:

Čas je múdrejší zo všetkých radcov.

Zvolené heslo vyčíslime obvyklým spôsobom pomocou použitej substitučnej tabuľky, pričom vyčíslujeme len písmena. Medzery a interpunkčné znamienka vynechávame:

```
Č  A  S  J  E  M  U  D  R  E  J  Š  I  Z  O  V  Š  E  T  K  Y  C  H  R  A  D  C  O  V

5  1  21 13 8  16 25 6  19 9  14 22 12 29 17 26 23 10 24 15 28 3  11 20 2  7  4  18 27
```

Vyčíslené heslo sa ešte posúvalo. Ak si napríklad zvolíme posunutie tak, že za začiatok hesla zvolíme jeho siedmy znak, dostaneme heslo:

```
U  D  R  E  J  Š  I  Z  O  V  Š  E  T  K  Y  C  H  R  A  D  C  O  V  Č  A  S  J  E  M

25 6  19 9  14 22 12 29 17 26 23 10 24 15 28 3  11 20 2  7  4  18 27 5  1  21 13 8  16
```

Na základe posunutia hesla sa tvoril aj podpis depeše. Tento podpis bol tvorený prvým písmenom posunutého hesla a dvoma písmenami pred alebo za ním. V našom príklade môže byť podpis `UEM` alebo `UDR`. Podpis sa písal na koniec depeše a od textu bol oddelený bodkou.

Substitučnú tabuľku a vyčíslené heslo už máme. Ako príklad zašifrujeme Cicerov citát:

Smrti nikdo nemůže uniknout, avšak zbabělý útěk před smrtí je horší než sama smrt. *Cicero*[3]

ale pri tejto šifre sa slová oddeľujú iným spôsobom než pri TTS, STT a „rímskej osem“, čo si ukážeme ďalej.

[2]Perikles, 500–429 pred n.l.

[3]Pôvodná verzia v latinčine: *(Mortem) effugere nemo potest. Turpis autem fuga mortis omni est morte peior. Cicero (Ant.VIII,10,29)*

V knihe [2] to síce nie je explicitne uvedené, ale je pravdepodobné, že dlhšie texty sa rozdeľovali na časti. Bolo to vhodné z hľadiska bezpečnosti. Predpokladajme teda, že texty sa delili na časti dĺžky približne 100 znakov tak, aby každá časť končila kompletným slovom. Podobne ako pri predošlých šifrách budeme na začiatok a koniec jednotlivých častí pridávať znaky označujúce nadväznosť. Náš text je síce kratší než 100 znakov, ale pre ilustráciu ho rozdelíme na dve časti:

```
SMRTI NIKTO NEMUŽE UNIKNOUT, AVŠAK ZBABĚLY UTEK/A

A/PŘED SMRTI JE HORŠI NEŽ SAMA SMRT. CICERO.UDR
```

Teraz podľa substitučnej tabuľky zameníme znaky za čísla. Namiesto medzier sa, podľa informácii z [2], písali cifry `6, 7` alebo `8`, ktoré sa nemôžu vyskytovať na mieste desiatok. Za interpunkčné znamienka sa medzery nedávajú. Slová sú teda oddelené buď medzerou, alebo interpunkčným znamienkom, ale nie oboma. Naše dve časti seriálu potom budú mať číselnú podobu:

```
22152 02411 61611 13241 77160 61525 31068 25161 11316 17252
43501 26230 11363 00201 02071 42972 52406 13370 17867

01371 82106 05822 15202 41161 20671 01720 23118 16063 16220
11501 72215 20243 30311 03062 01733 25052 08667
```

Čísla zapisujeme v päťčlenných skupinách. Pokiaľ počet cifier nie je násobok 5, náhodne doplníme potrebný počet cifier označujúcich medzery. V našom príklade ihneď vidno, že v prvej časti sú pridané cifry `7867` a v druhej časti cifry `8667`.

Teraz k číselnej podobe depeše periodicky príčítame posunuté heslo. Súčet robíme obvyklým spôsobom, t.j. modulo 10 (bez prenosu desiatok). Potom prvá časť našej depeše bude mať podobu:

Text:	2	2	1	5	2	0	2	4	1	1	6	1	6	1	1
Heslo:	**2**	**5**	6	1	9	9	1	4	2	2	1	2	2	9	1
Súčet:	4	7	7	6	1	9	3	8	3	3	7	3	8	0	2

Text:	1	3	2	4	1	7	7	1	6	0	6	1	5	2	5
Heslo:	7	2	6	2	3	1	0	2	4	1	5	2	8	3	1
Súčet:	8	5	8	6	4	8	7	3	0	1	1	3	3	5	6

Text:	3	1	0	6	8	2	5	1	6	1	1	1	3	1	6
Heslo:	1	2	0	2	7	4	1	8	2	7	5	1	2	1	1
Súčet:	4	3	0	8	5	6	6	9	8	8	6	2	5	2	7

Text:	1	7	2	5	2	4	3	5	0	1	2	6	2	3	0
Heslo:	3	8	1	6	**2**	**5**	6	1	9	9	1	4	2	2	1
Súčet:	4	5	3	1	4	9	9	6	9	0	3	0	4	5	1

Text:	1	1	3	6	3	0	0	2	0	1	0	2	0	7	1
Heslo:	2	2	9	1	7	2	6	2	3	1	0	2	4	1	5
Súčet:	3	3	2	8	0	2	6	4	3	2	0	4	4	8	6

Text:	4	2	9	7	2	5	2	4	0	6	1	3	3	7	0
Heslo:	2	8	3	1	1	2	0	2	7	4	1	8	2	7	5
Súčet:	6	0	2	8	3	7	2	6	7	0	2	1	5	4	5

Text:	1	7	8	6	7										
Heslo:	1	2	1	1	3										
Súčet:	2	9	9	7	0										

a druhá časť našej depeše bude mať podobu:

Text:	0	1	3	7	1	8	2	1	0	6	0	5	8	2	2
Heslo:	**2**	**5**	6	1	9	9	1	4	2	2	1	2	2	9	1
Súčet:	2	6	9	8	0	7	3	5	2	8	1	7	0	1	3

Text:	1	5	2	0	2	4	1	1	6	1	2	0	6	7	1
Heslo:	7	2	6	2	3	1	0	2	4	1	5	2	8	3	1
Súčet:	8	7	8	2	5	5	1	3	0	2	7	2	4	0	2

Text:	0	1	7	2	0	2	3	1	1	8	1	6	0	6	3
Heslo:	1	2	0	2	7	4	1	8	2	7	5	1	2	1	1
Súčet:	1	3	7	4	7	6	4	9	3	5	6	7	2	7	4

Text:	1	6	2	2	0	1	1	5	0	1	7	2	2	1	5
Heslo:	3	8	1	6	**2**	**5**	6	1	9	9	1	4	2	2	1
Súčet:	4	4	3	8	2	6	7	6	9	0	8	6	4	3	6

Text:	2	0	2	4	3	3	0	3	1	1	0	3	0	6	2
Heslo:	2	2	9	1	7	2	6	2	3	1	0	2	4	1	5
Súčet:	4	2	1	5	0	5	6	5	4	2	0	5	4	7	7

Text:	0	1	7	3	3	2	5	0	5	2	0	8	6	6	7
Heslo:	2	8	3	1	1	2	0	2	7	4	1	8	2	7	5
Súčet:	2	9	0	4	4	4	5	2	2	6	1	6	8	3	2

Toto by už mohol byť konečný tvar zašifrovanej depeše. Ešte ale môžme aplikovať pričítanie ďalšieho periodického heslo, prípadne spätnú substitúciu cifier za znaky medzinárodnej abecedy, prípadne aj oboje. Ukážeme si, ako sú tieto alternatívne možnosti popísané v [2]. Odtiaľ ale nie je zrejmé či sa skutočne aj používali a v akých kombináciach.

Najskôr si popíšeme pričitávanie ďalšieho periodického hesla. Toto heslo sa tvorilo z posunutého hesla, ktoré sme vytvorili a použili už v predošlej časti. Zobralo sa prvých desať vyčíslených znakov posunutého hesla (v našom príklade 25 6 19 9 14 22 12 29 17 26) a v dvojciferných číslach sa vynechali desiatky. V našom príklade dostávame: 5 6 9 9 4 2 2 9 7 6. Takto vytvorené desaťciferné číslo sa použilo ako ďalšie periodické heslo, ktoré sa pričitávalo k už predtým zašifrovanej depeši. Pričitávanie sa uskutočňovalo rovnako ako v predošlej časti, t.j. modulo 10 (bez prenosu desiatok). Potom prvá časť našej depeše bude mať podobu:

Medzivýsledok:	4	7	7	6	1	9	3	8	3	3	7	3	8	0	2
Heslo:	5	6	9	9	4	2	2	9	7	6	5	6	9	9	4
Súčet:	9	3	6	5	5	1	5	7	0	9	2	9	7	9	6

Medzivýsledok:	8	5	8	6	4	8	7	3	0	1	1	3	3	5	6
Heslo:	2	2	9	7	6	5	6	9	9	4	2	2	9	7	6
Súčet:	0	7	7	3	0	3	3	2	9	5	3	5	2	2	2

Medzivýsledok:	4	3	0	8	5	6	6	9	8	8	6	2	5	2	7
Heslo:	5	6	9	9	4	2	2	9	7	6	5	6	9	9	4
Súčet:	9	9	9	7	9	8	8	8	5	4	1	8	4	1	1

Medzivýsledok:	4	5	3	1	4	9	9	6	9	0	3	0	4	5	1
Heslo:	2	2	9	7	6	5	6	9	9	4	2	2	9	7	6
Súčet:	6	7	2	8	0	4	5	5	8	4	5	2	3	2	7

Medzivýsledok:	3	3	2	8	0	2	6	4	3	2	0	4	4	8	6
Heslo:	5	6	9	9	4	2	2	9	7	6	5	6	9	9	4
Súčet:	8	9	1	7	4	4	8	3	0	8	5	0	3	7	0

Medzivýsledok:	6	0	2	8	3	7	2	6	7	0	2	1	5	4	5
Heslo:	2	2	9	7	6	5	6	9	9	4	2	2	9	7	6
Súčet:	8	2	1	5	9	2	8	5	6	4	4	3	4	1	1

Medzivýsledok:	2	9	9	7	0										
Heslo:	5	6	9	9	4										
Súčet:	7	5	8	6	4										

a druhá časť depeše bude mať podobu:

Medzivýsledok:	2	6	9	8	0	7	3	5	2	8	1	7	0	1	3
Heslo:	5	6	9	9	4	2	2	9	7	6	5	6	9	9	4
Súčet:	7	2	8	7	4	9	5	4	9	4	6	3	9	0	7

Medzivýsledok:	8	7	8	2	5	5	1	3	0	2	7	2	4	0	2
Heslo:	2	2	9	7	6	5	6	9	9	4	2	2	9	7	6
Súčet:	0	9	7	9	1	0	7	2	9	6	9	4	3	7	8

Medzivýsledok:	1	3	7	4	7	6	4	9	3	5	6	7	2	7	4
Heslo:	5	6	9	9	4	2	2	9	7	6	5	6	9	9	4
Súčet:	6	9	6	3	1	8	6	8	0	1	1	3	1	6	8

Medzivýsledok:	4	4	3	8	2	6	7	6	9	0	8	6	4	3	6
Heslo:	2	2	9	7	6	5	6	9	9	4	2	2	9	7	6
Súčet:	6	6	2	5	8	1	3	5	8	4	0	8	3	0	2

Medzivýsledok:	4	2	1	5	0	5	6	5	4	2	0	5	4	7	7
Heslo:	5	6	9	9	4	2	2	9	7	6	5	6	9	9	4
Súčet:	9	8	0	4	4	7	8	4	1	8	5	1	3	6	1

Medzivýsledok:	2	9	0	4	4	4	5	2	2	6	1	6	8	3	2
Heslo:	2	2	9	7	6	5	6	9	9	4	2	2	9	7	6
Súčet:	4	1	9	1	0	9	1	1	1	0	3	8	7	0	8

Nakoniec si ukážeme ešte spätnú substitúciu cifier za znaky medzinárodnej abecedy, ktorá sa alternatívne mohla robiť. Na túto substitúciu sa využívala tabuľka s desiatimi stĺpcami, do ktorej sa zapísala medzinárodná

abeceda (v poslednom riadku zostali posledné štyri stĺpce prázdne). Na vytvorenie tejto tabuľky sa používalo rovnaké heslo, aké sa použilo aj na vytvorenie číselných periodických hesiel. Toto heslo sa zapísalo do riadkov tabuľky zľava doprava a zhora nadol, pričom opakujúce sa znaky sa vynechávali a interpunkčné znamienka sa nepísali. Do zvyšku tabuľky sa zapísali nepoužité písmená abecedy v lexikografickom poradí. V našom príklade bolo znenie hesla: *Čas je múdrejší zo všetkých radcov* a substitučná tabuľka bude mať podobu:

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

Ako vidno, jedná sa o homofónnu substitúciu. Cifry `1, 2, 3, 4, 5` a `6` budú mať tri a cifry `7, 8, 9` a `0` budú mať dve rôzne vyjadrenia pomocou znakov medzinárodnej abecedy. Po substitúcii bude mať prvá časť našej depeše podobu:

Cifry:	9	3	6	5	5	1	5	7	0	9	2	9	7	9	6
Text:	R	S	M	E	K	C	W	U	I	F	A	R	H	F	Y

Cifry:	0	7	7	3	0	3	3	2	9	5	3	5	2	2	2
Text:	G	U	H	V	I	P	S	O	R	E	V	K	N	A	O

Cifry:	9	9	9	7	9	8	8	8	5	4	1	8	4	1	1
Text:	F	R	F	U	R	D	B	D	W	J	Z	B	T	L	C

Cifry:	6	7	2	8	0	4	5	5	8	4	5	2	3	2	7
Text:	X	H	N	D	G	Q	E	K	B	J	W	A	P	O	U

Cifry:	8	9	1	7	4	4	8	3	0	8	5	0	3	7	0
Text:	D	F	Z	H	T	Q	B	S	I	D	E	G	V	U	I

Cifry:	8	2	1	5	9	2	8	5	6	4	4	3	4	1	1
Text:	B	N	L	K	R	A	D	W	M	J	T	P	Q	C	Z

Cifry:	7	5	8	6	4										
Text:	H	E	B	Y	J										

a druhá časť našej depeše bude mať podobu:

Cifry:	7	2	8	7	4	9	5	4	9	4	6	3	9	0	7
Text:	U	A	D	H	J	R	E	T	F	Q	M	S	R	I	U

Cifry:	0	9	7	9	1	0	7	2	9	6	9	4	3	7	8
Text:	G	F	H	R	C	I	U	O	F	Y	R	J	V	H	B

Cifry:	6	9	6	3	1	8	6	8	0	1	1	3	1	6	8
Text:	X	F	M	P	Z	D	Y	B	G	L	C	S	Z	X	D

Cifry:	6	6	2	5	8	1	3	5	8	4	0	8	3	0	2
Text:	M	Y	N	K	B	L	V	W	D	T	I	B	P	G	A

Cifry:	9	8	0	4	4	7	8	4	1	8	5	1	3	6	1
Text:	R	D	I	Q	J	U	B	T	C	D	E	Z	S	X	L

Cifry:	4	1	9	1	0	9	1	1	1	0	3	8	7	0	8
Text:	Q	C	F	Z	G	R	L	C	Z	I	V	B	H	G	D

Toto je kompletný popis šifrovania aj s alternatívnym pričítaním ďalšieho periodického hesla a spätnou substitúciou za znaky medzinárodnej abecedy.

Pri tejto šifre sa služobné údaje depeší, ako sú číslo depeše, počet päťmiestných skupín príslušnej časti, dátum šifrovania, prvé dve cifry posunutého hesla a dátum a čas nasledujúcej relácie, skrývali v prvých a posledných štyroch päťmiestnych skupinách (v číselnej, prípadne znakovej podobe, podľa spôsobu šifrovania). Depeše sa tak zdanlivo odosielali bez záhlavia. Takto sa to spomína v [2], avšak spôsob kódovania týchto údajov sa tam neuvádza. Z informácií tam spomenutých, sa dá iba predpokladať, že posledné štyri skupiny depeše boli zrkadlovým obrazom prvých štyroch skupín. Toto už samo o sebe lúštiteľom napovedá, že sa bude s najväčšou pravdepodobnosťou jednať práve o služobné údaje depeše. Výnimku by predstavovala len spätná substitúcia depeše za znaky medzinárodnej abecedy, kedy by sa rovnaké cifry reprezentovali na začiatku a na konci depeše rôznymi znakmi. **Keďže mi nie je známy spôsob kódovania týchto údajov, pre účely nášho príkladu si vymyslím niečo veľmi jednoduchého. V praxi zrejme tieto údaje boli maskované a nie použité priamo, ako v tomto príklade.** Potrebujeme zakódovať nasledovných sedem informácií:

- **Číslo telegramu** – použijeme štyri cifry `cccc`.
- **Spôsob šifrovania** – potrebujeme adresátovi indikovať, či depeša bola zašifrovaná jedným, alebo dvoma periodickými heslami. Na to nám stačí jedna cifra **e**. Nepárne číslo bude znamenať šifrovanie jedným a párne číslo dvoma periodickými heslami. Spôsob šifrovania sa v [2]

medzi služobnými údajmi neuvádza, ale ak sa používali alternatívne formy šifrovania, bolo by logické ich nejakým spôsobom aj indikovať adresátovi.

- **Počet päťmiestnych skupín** – keďže sa depeše zrejme delili na kratšie časti, použijeme tri cifry `ppp`. Nie je ale jasné, či sa počet skupín počítal spolu so skupinami obsahujúcimi služobné údaje, alebo bez nich. V našom príklade budeme počet skupín udávať aj so služobnými údajmi.
- **Dátum šifrovania** – stačí kódovať deň. Rok a mesiac sa zrejme nebudú príliš líšiť od dátumu prijatia depeše. Takže použijeme dve cifry `dd`.
- **Prvé dve cifry posunutého hesla** – tu potrebujeme dve cifry `hh`.
- **Dátum nasledujúcej relácie** – použijeme štyri cifry `MMDD` označujúce mesiac a deň.
- **Čas nasledujúcej relácie** – použijeme štyri cifry `tttt` udávajúce hodiny a minúty vo formáte bežne používanom v anglosaských krajinách.

Takže naše prvé štyri skupiny depeše budú mať podobu:

```
cccce pppdd hhMMD Dtttt
```

a posledné štyri skupiny depeše budú ich zrkadlovým obrazom. Ak budeme predpokladať, že čísla prvej a druhej časti našej depeše sú 316, 317, depeše šifrujeme 9. deň v mesiaci len pomocou prvého periodického hesla a dátum a čas najbližšej relácie sú 13. augusta o 18^{00}, tak potom prvé štyri skupiny prvej a druhej časti depeše v našom príklade budú mať podobu:

```
03163 02709 25081 31800
03171 02609 25081 31800
```

a posledné štyri skupiny prvej a druhej časti depeše v našom príklade budú mať podobu:

```
00813 18052 90720 36130
00813 18052 90620 17130
```

Potom definitívny tvar prvej a druhej časti našej depeše, aj so služobnými údajmi, bude:

```
03163 02709 25081 31800 47761 93833 73802 85864 87301 13356
43085 66988 62527 45314 99690 30451 33280 26432 04486 60283
72670 21545 29970 00813 18052 90720 36130
------------------------------------------------------------
03171 02609 25081 31800 26980 73528 17013 87825 51302 72402
13747 64935 67274 44382 67690 86436 42150 56542 05477 29044
45226 16832 00813 18052 90620 17130
```

Použili sme šifrovanie len pričítaním prvého periodického hesla z nášho príkladu. Tieto depeše sú už pripravené na odoslanie.

Podobne definitívny znakový tvar prvej a druhej časti depeše, aj so služobnými údajmi, bude:

```
ISCMA IAUGR OEIDZ VLBGI RSMEK CWUIF ARHFY GUHVI PSORE VKNAO
FRFUR DBDWJ ZBTLC XHNDG QEKBJ WAPOU DFZHT QBSID EGVUI BNLKR
ADWMJ TPQCZ HEBYJ IGBLV ZDIEO RGUAI AMCSI
-----------------------------------------------------------
ISCUJ IAMGR OEIDZ VLBGI UADHJ RETFQ MSRIU GFHRC IUOFY RJVHB
XFMPZ DYBGL CSZXD MYNKB LVWDT IBPGA RDIQJ UBTCD EZSXL QCFZG
RLCZI VBHGD IGBLV ZDIEO RGMAI JUCSI
```

Teraz sme použili šifrovanie pričítaním prvého aj druhého periodického hesla a spätnú substitúciu za znaky medzinárodnej abecedy z nášho príkladu a tieto depeše sú už pripravené na odoslanie.

V tomto príklade je úmyselná chyba v tom, že pri substitúcii cifier za znaky medzinárodnej abecedy sme pri služobných údajoch (prvé a posledné štyri skupiny depeše) nevyužili homofónnosť spätnej substitúcie čísel za znaky. Preto sú posledné štyri skupiny zrkadlovým obrazom prvých štyroch skupín, čo lúštiteľom zjednoduší prácu. Tomuto sa dalo zabrániť „rozumnejšiou“ substitúciou.

4.2 Postup pri šifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii text na šifrovanie.

b. Máme približne tridsať znakov dlhé heslo.

c. Máme číslo depeše. Budeme prepokladať, že depeše sa číslujú vzostupne, takže každá ďalšia depeša bude mať toto číslo o 1 väčšie než predchádzajúca.

d. Je daný dátum šifrovania (uvádza sa v služobných údajoch).

e. Sú dané dátum a čas nasledujúcej relácie (uvádzajú sa v služobných údajoch).

Potom šifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Zoberieme heslo a jeho znaky vyčíslime obvyklým spôsobom. Medzery a interpunkčné znamienka sa nevyčíslujú a znaky vyčíslujeme v poradí podľa substitučnej tabuľky 1 (str. 3).

2. Zvolíme posunutie hesla pre danú depešu. Bolo by žiaduce každú depešu šifrovať s iným posunutím hesla. Toto posunutie sa indikuje priamo v služobných údajoch depeše (viď ďalej). Posunutie sa určuje znakom hesla, ktorý potom berieme ako prvý znak a ostatné znaky sa cyklicky posúvajú. Podľa toho sa potom posunie aj vyčíslenie hesla, z predošlého bodu.

3. Podľa posunutia hesla vytvoríme podpis depeše. Tento je trojznakový a tvoríme ho tak, že vezmeme prvý znak posunutého hesla a dva znaky pred ním, alebo dva znaky za ním. Podpis pridávame na koniec textu, ktorý sa chystáme šifrovať a od textu ho oddeľuje bodka.

4. Text, ktorý ideme šifrovať, prepíšeme len pomocou znakov obsiahnutých v substitučnej tabuľke 1 (str. 3), čiže nahradíme písmená a vynecháme špeciálne znaky, ktoré sa v substitučnej tabuľke nevyskytujú.

5. Pokiaľ sa medzi slovami textu nachádza niektorý zo špeciálnych znakov obsiahnutých v substitučnej tabuľke, za týmto znakom sa medzera vynecháva.

6. Text rozdelíme na časti približne 100 znakov dlhé tak, aby každá časť vždy končila kompletným slovom.

7. Na koniec prvej časti pridáme, kvôli nadväznosti dielov, znaky `/A`. Na začiatok druhej časti pridáme `A/`, na koniec druhej časti pridáme `/B` atď. Každá časť textu (okrem prvej a poslednej) bude mať na začiatku písmeno identické s koncovým písmenom predošlej časti a lomítko. Na konci textu lomítko a písmeno identické s písmenom označujúcim nasledovnú časť textu. Písmena na označovanie častí berieme podľa abecedy. Prvá časť má označenie len na konci a posledná časť len na začiatku.

8. Každú časť textu šifrujeme zvlášť a každá časť textu tvorí samostatnú depešu. Ďalší popis sa bude týkať šifrovania jednotlivých častí.

9. Znaky v texte nahradíme podľa tabuľky 1 (str. 3) dvojciferným číslami. Medzery v texte sa nahrádzajú ciframi `6, 7` alebo `8`.

10. Postupnosť čísel, ktorú sme dostali rozdelíme na skupiny po 5 cifier. Pokiaľ počet cifier, nie je násobkom 5, tak náhodne doplníme chýbajúce cifry, číslami `6, 7` alebo `8`.

11. Pod cifry depeše periodicky podpíšeme cifry posunutého hesla.

12. Sčítame cifry depeše s ciframi hesla modulo 10, t.j. súčet bez prenosu desiatok. Týmto môžme šifrovanie ukončiť, alebo pokračujeme nasledovnými dvoma bodmi:

    (a) Vytvoríme druhé, 10-ciferné, periodické heslo tak, že zoberieme prvých desať znakov posunutého hesla a ich vyčíslenia. Z týchto čísel vynecháme desiatky a dostaneme desaťciferné číslo.

    (b) Podpíšeme druhé periodické heslo pod cifry depeše z bodu 12 a spravíme súčet cifier depeše a cifier druhého hesla modulo 10.

13. Vytvoríme služobné záhlavie. Toto pozostáva zo štyroch päťčlenných skupín. **Nie je známe, ako sa záhlavie tvorilo v skutočnosti. Tu popisovaný postup je vymyslený len pre potreby nášho príkladu!**

    (a) Prvé štyri cifry udávajú číslo depeše.

    (b) Piata cifra indikuje prešifrovanie druhým periodickým heslom. Pokiaľ je táto cifra nepárna, pričítalo sa len jedno periodické heslo, ak je párna, pričítali sa dve periodické heslá.

    (c) Ďalšie 3 cifry depeše udávajú počet päťčlenných skupín spolu so služobnými údajmi. To znamená počet skupín depeše z bodu 12 zväčšený o 8 (štyri služobné skupiny na začiatku a štyri zrkadlovo obrátené skupiny na konci depeše).

    (d) Nasledujúce 2 cifry udávajú deň šifrovania depeše.

    (e) Ďalšie 2 cifry budú prvé dve cifry posunutého hesla.

    (f) Nasledujú 4 cifry udávajúce mesiac a deň nasledujúcej relácie.

    (g) Posledné 4 cifry udávajú čas nasledujúcej relácie.

    Týmto sme vytvorili štyri päťčlenné skupiny služobného záhlavia, ktoré píšeme na začiatok depeše a zrkadlovo obrátené ho pridáme aj na koniec depeše.

14. Predošlým bodom môžme skončiť a depeša je pripravená na odoslanie, prípadne pokračujeme ďalšími bodmi.

15. Zostrojíme substitučnú tabuľku 3x10. Stĺpce označíme číslami 1, 2, 3, 4, 5, 6, 7, 8, 9, 0 a do riadkov zľava doprava a zhora nadol zapíšeme 26 znakov medzinárodnej abecedy v poradí určenom šifrovacím heslom obvyklým spôsobom.

16. Zameníme cifry depeše z bodu 13 za znaky medzinárodnej abecedy podľa substitučnej tabuľky z predošlého bodu. Pritom v maximálnej miere využívame homofónnosť tejto substitúcie. Takto dostaneme definitívny tvar depeše.

4.3 Postup pri dešifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii kompletný text zašifrovanej depeše.

b. Máme k dispozícii šifrovacie heslo.

Potom dešifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Pokiaľ je depeša v znakovej podobe, t.j. zapísaná pomocou znakov medzinárodnej abecedy, najskôr ju prevedieme na číselný tvar. Zostrojíme substitučnú tabuľku 3x10. Stĺpce označíme číslami 1, 2, 3, 4, 5, 6, 7, 8, 9, 0 a do riadkov zľava doprava a zhora nadol zapíšeme 26 znakov medzinárodnej abecedy v poradí určenom šifrovacím heslom obvyklým spôsobom. Potom pomocou tejto substitučnej tabuľky prevedieme znaky na čísla.

2. Posledné štyri skupiny depeše musia byť zrkadlovým obrazom prvých štyroch skupín. Tieto obsahujú služobné údaje. Zistíme z nich číslo depeše, spôsob šifrovania depeše, počet päťmiestnych skupín depeše, dátum šifrovania, prvé dve cifry posunutého hesla a dátum a čas nasledujúcej relácie. Pre ďalšie dešifrovanie sú podstatné spôsob šifrovania depeše a prvé dve cifry posunutého hesla. Ostatné údaje majú len kontrolný a informatívny charakter.

3. Prvé a posledné štyri skupiny depeše môžme vynechať, pretože ich už nebudeme potrebovať.

4. Zoberieme heslo a jeho znaky vyčíslime obvyklým spôsobom. Medzery a interpunkčné znamienka sa nevyčíslujú. Znaky vyčíslujeme v poradí podľa substitučnej tabuľky 1 (str. 3).

5. Prvé dve cifry posunutého hesla poznáme. Posunieme teda vyčíslené heslo tak, aby sa začínalo týmito ciframi.

6. Ak bola depeša šifrovaná dvoma periodickými heslami, potom:

(a) Vytvoríme druhé, 10-ciferné, periodické heslo tak, že zoberieme prvých desať znakov posunutého hesla a ich vyčíslenia. Z týchto čísel vynecháme desiatky a dostaneme desaťciferné číslo.

(b) Podpíšeme druhé periodické heslo pod cifry depeše a spravíme rozdiel cifier depeše a cifier druhého hesla modulo 10, t.j. bez prenosu desiatok.

7. Pod cifry depeše, prípadne medzivýsledku z predošlého bodu, podpíšeme prvé periodické heslo a spravíme rozdiel cifier depeše a cifier prvého hesla modulo 10.

8. Z konca depeše vynecháme náhodne pridané cifry. Tieto spoznáme podľa toho, že na miestach desiatok majú len cifry `6, 7` alebo `8`.

9. Podľa substitučnej tabuľky 1 (str. 3) zameníme čísla depeše za znaky. Znaky sú kódované dvojcifernými číslami. Pokiaľ by sa na mieste desiatok vyskytovala cifra `6, 7` alebo `8`, tak sa jedná o medzeru a tá je kódovaná len jednou cifrou.

10. Doplníme medzery za špeciálne znaky v texte. Týmto sme dostali pôvodný text depeše.

11. Pokiaľ sa jedná o seriál, tak text zostavíme v správnom poradí podľa označenia na začiatku a konci jednotlivých častí seriálu.

4.4 Lúštenie

Pokiaľ ide o lúštenie tejto šifry, v jej základnej podobe je to šifra typu SP a platí o nej presne to isté, čo bolo spomenuté pri lúštení šifry „rímska osem“ v predošlej časti seriálu (Crypto-World 3/2011). Čiže najskôr odhadneme dĺžku periodického hesla (napríklad Kasiského metódou), potom pomocou útoku na predpokladaný text odhalíme toto heslo a následne musíme ešte vyriešiť jednoduchú substitúciu. Preto v prípade tejto šifry bolo lúštenie, v porovnaní so šifrou „rímska osem“, o čosi zjednodušené tým, že substitúcia nebola homofónna, ale len jednoduchá. Naviac, služobné údaje sa zapisovali ako prvé a posledné štyri skupiny depeše, pričom posledné štyri skupiny boli zrkadlovým obrazom prvých štyroch skupín. Pokiaľ sa nerobila spätná substitúcia čísiel za znaky a nevyužila sa jej homofónnosť, dali sa tieto služobné skupiny veľmi ľahko rospoznať.

Pokiaľ sa použilo prešifrovanie pričítaním ďalšieho periodického hesla, na bezpečnosti šifry a jej lúštení sa zmenilo len málo. Varianty SP a SPP sú

z hľadiska bezpečnosti a lúštenia vo svojom princípe ekvivalentné. Pričítanie dvoch periodických hesiel sa dá nahradiť pričítaním jediného periodického hesla. Pri vhodnej voľbe pôvodných dvoch hesiel bude dĺžka výsledného hesla rovná súčinu dĺžok pôvodných dvoch hesiel, čo v ideálnom prípade bude vyžadovať podstatne viac zašifrovaného textu na analýzu. Takáto vhodná voľba dvoch periodických hesiel ale nie je pri šifre „rímska deväť“ zabezpečená. Takže toto prešifrovanie pričítaním ďalšieho periodického hesla bolo v podstate zbytočné. Spôsobovalo iba komplikácie šifrantom a dešifrantom, zvyšovalo pravdepodobnosť spravenia chyby a nutnosť opakovaného posielania depeše.

Prešifrovanie spätnou substitúciou čísel za písmená medzinárodnej abecedy obsahovalo homofónnu substitúciu, ktorá prácu lúštiteľov mierne skomplikovala. Samozrejme len za predpokladu, že sa správne využila homofónnosť spätnej substitúcie. To však, aspoň podľa mne dostupných informácii, opäť nebolo ničím zabezpečené. Nijako podstatne to ale bezpečnosť šifry nezvýšilo. Lúštenie homofónnych substitúcii bolo známe dávno pred 2. svetovou vojnou. Pri odchytení dostatočného množstva depeší sa dali využiť štatistické metódy. Naviac z dostupných zdrojov nie je zrejmé, či sa toto prešifrovanie vôbec v praxi používalo.

Okrem toho pri zostavovaní tabuľky pre spätnú substitúciu sa používalo rovnaké heslo ako pre konštrukciu oboch periodických hesiel. Preto pokiaľ už lúštitelia poznali princíp tejto šifry z predošlých depeší a podarilo sa im rekonštruovať tabuľku spätnej substitúcie, tak mali rovno aj obe periodické heslá.

Literatúra

[1] Grošek Otokar, Vojvoda Milan, Zajac Pavol: Klasické šifry
STU v Bratislave, 2007

[2] Hanák Vítězslav: Muži a radiostanice tajné války
Elli Print, 2002

[3] Janeček Jiří: Gentlemani (ne)čtou cizí dopisy
Books Bonus A, 1998

[4] Janeček Jiří: Odhalená tajemství šifrovacích klíčů minulosti
Naše vojsko, 1994

[5] Janeček Jiří: Válka šifer – výhry a prohry československé vojenské rozvědky (1939–1945)
Votobia, 2001

B. Rotorový šifrátor Fialka M-125
Úvod k seriálu

Eugen Antal & Matúš Jókay, Kaivt FEI, STU v Bratislave
(antal.87@gmail.com , matus.jokay@stuba.sk)

Fialka je rotorový šifrovací stroj, vytvorený sovietskou armádou. Prvýkrát bol uvedený do používania okolo roku 1965. Dizajn a fungovanie Fialky je založené na podobnom princípe ako Enigma (používaná nemeckou armádou počas druhej svetovej vojny), aj keď s mnohými vylepšeniami. Oficiálne označenie stroja je **M-125**, **Fialka** je meno šifrovacej procedúry.[1] Stroj používa niekoľko rotorov na substitúciu znaku napísaného na klávesnici. Obsahuje mechanické ako aj elektronické časti.

Odlišné verzie Fialky sa objavili v bývalom Československu, na území východného Nemecka a v Poľsku.[6] Po páde Sovietskeho zväzu vydali príkaz na pozbieranie a zničenie vydaných strojov, čo bolo súčasťou zmluvy, ktorá hovorila len o zápožičke. Zachránilo sa len málo kusov. Z toho dôvodu je skúmanie Fialky v dnešnej dobe veľmi náročné. Popis tohto stroja bol donedávna utajený a nejasný. Prvý podrobný popis zverejnili až v roku 2006.

Seriál o rotorovom šifrátore Fialka M-125 sme kvôli rozsahu, a tiež pre lepšiu prehľadnosť, rozdelili na niekoľko častí. V prvej sa zaoberáme opisom šifrovacieho algoritmu Fialka a schémou šifrovacieho stroja Fialka M-125. Aj keď sme sa snažili čitateľovi priblížiť fungovanie šifry a šifrátora čo najjednoduchším spôsobom, nie vždy sa dalo vyhnúť aspoň čiastočným formalizmom. Označovanie jednotlivých častí, funkcií a symbolov vychádza z označenia bežne používaného v literatúre, zaoberajúcej sa klasickými šiframi (viď napríklad [7], [8]).

Druhá časť je zameraná na porovnanie viacerých rotorových šifier (viď napríklad [9]), ako Enigma, Hagelin, Siemens... V porovnaní sa zameriavame na odlišnosti funkcií mechanicko-elektronických súčiastok, na zhody a prípadné rozdiely v konceptoch (de)šifrovacích systémov.

V tretej časti seriálu predstavíme čitateľom niekoľko pohľadov na štatistické vlastnosti šifrovacieho systému Fialka. Aj keď sa už veľa autorov venovalo automatizovanej kryptoanalýze klasických šifrovacích systémov (viac informácií na túto tému viď napríklad [10]), zatiaľ sa nepodarilo aplikovať postupy automatického lúštenia na rotorové šifry typu Fialka. Málo odborníkov venuje pozornosť týmto systémom (keďže sú už dávno nahradené modernými šifrovacími systémami). O to zaujímavejšie môžu byť predstavené výsledky skúmania niektorých vybraných charakteristík šifry Fialka.

Na záver prinesieme krátku informáciu o výkonnostných parametroch implementácie šifrátora Fialka M-125 na súčasných počítačoch. Ukážeme efektivitu šifrátora v porovnaní so súčasným šifrovacím štandardom. Taktiež spomenieme možnosti aplikácie a využitia klasických kryptosystémov typu Fialka v súčasnom svete digitálnej informácie.

Literatúra

[1], [6], [7], [8], [9], [10] – viz následující článek

C. Rotorový šifrátor Fialka M-125
Diel 1., Popis šifrátora

Eugen Antal & Matúš Jókay, Kaivt FEI, STU v Bratislave
(antal.87@gmail.com , matus.jokay@stuba.sk)

Šifrovací stroj Fialka na prvý pohľad vyzerá ako obyčajný písací stroj. Vo vnútri však skrýva pokročilý šifrovací mechanizmus, vďaka ktorému sa zaradil medzi vrcholné kryptografické stroje po druhej svetovej vojne.

Pôvodná verzia Fialky bola implementovaná strojom M-125-xx. Tento typ stroja bol navrhnutý pre sovietskú armádu (klávesnica používala len cyriliku). Neskoršie verzie M-125-3xx boli rozšírené o niekoľko vylepšení a boli vybavené klávesnicou, ktorá obsahovala aj písmená latinskej abecedy. [1]

Obr. 1. Pohľad na Fialku M-125-3MP2 (prevzaté z [4]).

1 Rotory

Fialka používa desať jedinečných rotorov, označených prvými desiatimi písmenami cyriliky, vsadených na hriadeľ. Každý rotor má 30 kontaktov, na jednej strane prepojených príslušnou substitúciou a niekoľko blokovacích pinov. Je tu 30 možných pozícií blokovacích pinov na každom rotore. Každý pin je priradený k jednému písmenu na vonkajšej hrane. Prítomnosť alebo neprítomnosť pinu ovláda krokovanie rotora Fialky. Blokovacie piny zabraňujú ďalšiemu rotoru v pohybe.

Existujú dva typy rotorov: pevné a nastaviteľné. Pôvodne vydali Fialku s desiatimi pevnými rotormi. Každý rotor mal 30 kontaktov s premenlivým počtom blokovacích pinov.[1]

Obr. 2. Sada rotorov Fialky (prevzaté z [2]).

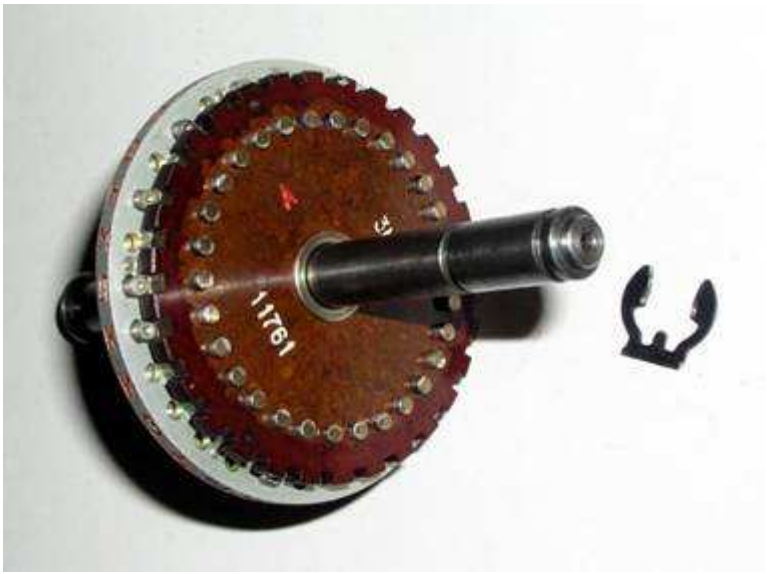
V [5] autori tvrdia, že Fialka mohla pracovať s 8 alebo 10 rotormi, ale P. Reuvers v [1] popiera existenciu verzie s 8 rotormi, a označuje toto tvrdenie za nepravdivé. Zatiaľ nie sú verejne známe oficiálne dokumenty, ktoré by potvrdili alebo popreli existenciu verzie s 8 rotormi.

1.1 Pevné rotory (PROTON-1)

Na Fialke s pevnými rotormi sa mohli uskutočniť (podobne ako na Enigme) nasledujúce nastavenia:

- Zmena poradia rotorov (10! pre 10 rotorov)
- Natočenie rotora do pozície - zmena začiatočného znaku (30^{10} pre 30 možných posunov na každom rotore)

Teda celkový počet nastaviteľných kľúčov na rotoroch je 10! x 30^{10}.



Obr. 3. Rotor označený s „A“ nastavený na hriadeľ (prevzaté z [2]).

1.2 Nastaviteľné rotory (PROTON-2)

V roku 1978 boli pevné rotory vymenené za nastaviteľné. [6] Tento typ rotorov sa označuje aj ako PROTON-2. [1] V základnom nastavení každý nastaviteľný rotor fungoval ako pevný s rovnakým označením. Oproti pevným rotorom bolo možné navyše nastaviť:

- Posun vonkajšieho kruhu (t.j. blokovacích pinov a aj kontaktov na vonkajšom kruhu)
- Preloženie jadra z jednotlivých rotorov do iného rotora (jadro obsahuje prepojenie kontaktov)
- Zmena strany jadra
- Zmena znaku na jadre jednotlivých rotorov (natočenie jadra)

Obr. 4. Rozobratý nastaviteľný rotor (prevzaté z [3]).

2 Prepojenie rotorov

Boli nájdené tri rôzne série rotorov, ktoré sa líšili v prepojeniach ako aj v pozíciách blokovacích pinov. Rôzne krajiny používali rôzne série.[1] Z troch sérií boli zatiaľ identifikované len dve:
3K – použité v Poľsku
6K – použité v Československu [3]

Prepojenie rotorov bolo dopredu určené zvlášť pre každú sériu. Tieto prepojenia, ako aj prítomnosť blokovacích pinov na jednotlivých pozíciách môžu byť znázornené v prepojovacích tabuľkách. Z prepojovacej tabuľky pomocou znaku vstupujúceho na rotor a z označenia rotora môžeme určiť výstupný znak. Pre jednoduchšiu prácu použijeme aj číselné označenie písmen.

latinský znak	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
cyrilský znak	Б	И	С	В	У	А	П	Р	Ш	О	Л	Д	Ь	Т	Щ
číselné označenie	2	9	17	3	19	1	15	16	24	14	11	5	27	18	25
latinský znak	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**2**	**5**	**7**	**8**
cyrilský znak	З	Х	К	Ы	Е	Г	М	Ц	Ч	Я	Н	Й	Ж	Ф	Ю
číselné označenie	8	21	10	26	6	4	12	22	23	29	13	30	7	20	28

Tab. 1. a) Latinská abeceda, jej ekvivalent (na Fialke) v cyrilike a číselné označenie .

Poznámka: Fialka používala 30 písmen cyriliky, kým predošlá tabuľka obsahuje len 26 písmen latinskej abecedy. Zvyšné 4 písmená cyriliky sú nahradené číslami 2,5,7 a 8. Táto tabuľka je kompatibilná s klávesnicou, ktorá sa používala v bývalom Československu a v Poľsku.

cyrilský znak	**А**	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**К**	**Л**	**М**	**Н**	**О**	**П**
latinský znak	F	A	D	U	L	T	5	P	B	R	K	V	Z	J	G
číselné označenie	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
cyrilský znak	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ы**	**Ь**	**Ю**	**Я**	**Й**
latinský znak	H	C	N	E	7	Q	W	X	I	O	S	M	8	Y	2
číselné označenie	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Tab. 1. b) Písmená na vonkajšej strane rotora (miesto kontaktov) a ich číselné označenie pri natočení rotorov (čísla sú znížené o 1 oproti pôvodnej hodnote kvôli výpočtom).

Ďalej sa v tabuľkách používa číselné označenie z Tab.1.a)

3K SERIES

Wheel		Contact																												
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
		А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ю	Я	Й
1	А	23	22	3	7	4	8	16	6	10	20	15	17	24	9	30	12	25	11	1	28	27	5	29	26	2	18	21	14	13	19
2	Б	5	24	20	2	6	21	26	7	18	4	17	23	15	19	10	30	13	28	29	11	9	25	1	14	22	8	27	5	12	16
3	В	20	5	7	15	21	27	4	1	22	17	23	13	30	6	26	10	16	14	19	18	29	24	3	12	9	11	2	28	8	25
4	Г	16	21	28	11	27	3	15	12	24	30	9	17	4	20	25	8	1	29	19	18	14	10	5	23	26	7	6	22	2	13
5	Д	18	15	1	22	19	16	29	8	17	4	3	14	6	30	23	5	26	13	25	10	12	21	27	20	7	11	24	9	2	28
6	Е	9	14	13	20	24	8	2	6	5	19	11	28	30	3	18	15	7	25	16	1	12	23	27	29	17	10	21	4	22	26
7	Ж	7	9	5	26	6	4	19	3	8	28	22	12	21	24	23	10	13	1	16	29	2	25	27	15	18	11	14	17	30	20
8	З	29	27	15	13	8	2	25	12	6	23	9	18	24	1	14	21	17	10	3	11	22	7	16	4	19	26	5	30	28	20
9	И	5	19	2	27	20	26	7	11	16	18	3	13	4	23	28	21	6	24	29	30	15	17	9	12	8	22	25	10	1	14
10	К	20	24	8	25	19	1	17	5	15	27	9	12	22	10	18	3	16	30	4	14	7	23	11	2	29	26	28	21	6	13

Tab. 2. Prepojovacia tabuľka série rotorov 3K (prevzaté z [1]).

6K SERIES

Wheel		Contact																												
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
		А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ю	Я	Й
1	А	13	22	8	18	20	12	28	4	15	27	3	5	16	14	23	26	1	25	17	11	30	10	24	7	6	21	29	2	9	19
2	Б	20	8	5	15	4	28	21	1	24	13	29	12	14	23	25	7	9	30	27	3	11	18	17	19	22	10	2	26	6	16
3	В	29	11	4	22	24	16	18	2	23	3	17	8	20	5	28	12	15	26	30	7	21	19	13	10	27	25	9	1	14	6
4	Г	4	12	19	29	24	23	7	30	15	1	20	14	18	2	16	27	10	25	17	28	6	21	11	8	22	5	9	3	26	13
5	Д	18	2	15	7	20	28	8	13	23	12	19	27	4	24	10	14	11	6	30	3	17	26	22	1	29	25	16	21	5	9
6	Е	16	4	14	24	23	19	30	3	1	8	27	13	9	5	29	10	15	26	22	7	25	17	20	11	2	6	21	28	18	12
7	Ж	26	23	7	5	13	8	24	30	29	20	22	9	12	10	25	16	3	21	19	18	4	1	28	27	6	2	15	17	11	14
8	З	16	22	14	30	24	15	17	20	4	7	27	12	6	13	25	21	1	5	26	8	11	23	29	28	3	18	10	19	2	9
9	И	12	1	17	29	6	4	7	11	15	3	21	25	9	26	30	13	22	20	10	24	27	14	28	23	2	5	19	18	16	8
10	К	9	21	8	16	25	5	20	22	4	27	14	19	1	15	30	2	10	17	7	24	12	18	29	3	23	6	13	28	26	11

Tab. 3. Prepojovacia tabuľka série rotorov 6K (prevzaté z [1]).

V ľavej časti tabuľky sú pod sebou očíslované rotory. V hornej časti zase kontakty - použitá abeceda v poradí.

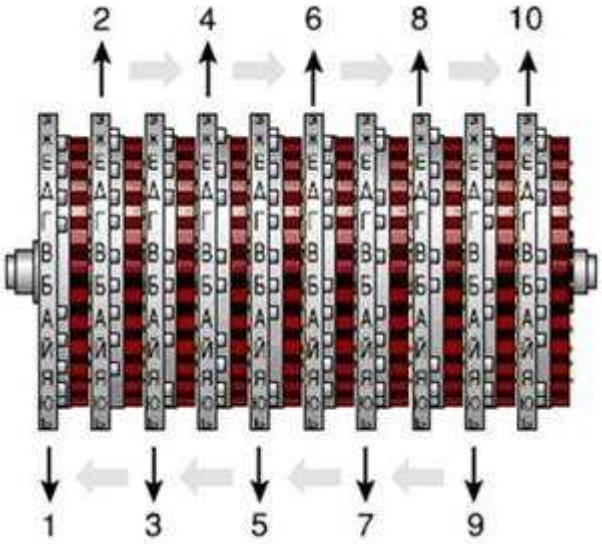
Príklad na používanie tabuľky:
V tabuľke 6K (Tab. 3.) príde na rotor označený „10“ vstup na kontakt označený „3“, takže z tohoto rotora vystupuje znak „8“. Ako vidíme, pole označujúce výstup je farebne zvýraznené. Znamená to, že na danom rotore je na danom mieste blokovací pin. Prítomnosť

pinu ovláda pohyb nasledujúcich rotorov, čo je vysvetlené v nasledujúcej časti.

3 Krokovanie rotorov

S každým znakom zadaným cez klávesnicu sa rotory vo vnútri Fialky nastavia na novú pozíciu. To zabezpečí nové prepojenie rotorov pre každý ďalší znak vstupu. Fialka používa striedavý krokovací mechanizmus. To znamená, že na pohyb rotorov sa používajú dve mechanicky nezávislé časti. Preto rotor nikdy neovplyvní pohyb susedného rotora. Rotor je však spojený s rotorom ob jeden ďalej. Priľahlé rotory sa pohybujú v opačnom smere. Keď sa jeden rotor pohybuje v smere hodinových ručičiek, potom susedný rotor sa pohybuje proti smeru hodinových ručičiek.[1]

Rotory v poradí (vloženia do stroja) zľava označme symbolmi od 1 do 10. Toto označenie rotorov je treba odlišovať od číselného označenia (menovky) jednotlivých rotorov.



Obr. 5. Označené rotory Fialky a smer ich pohybu (prevzaté z [1]).

Rotory označené párnym číslom sa otáčajú nezávisle od nepárnych. Prakticky sa jedná o dva nezávislé pohyby rotorov. Keď uvažujeme pripojenie klávesnice na strane rotora číslo 1, párne rotory sa od neho vzďaľujú. Rotor č. 2 má špeciálnu vlastnosť, je rýchly. To znamená, že sa pohybuje pri každom stlačení klávesy. Každým stlačením klávesnice sa bude otáčať rotor č. 2 a posúvať rotor č. 4, ktorý potom posúva rotor č. 6 atď.

Všetky rotory napravo od blokovacieho pinu na rotore nebudú krokované. Krokovací mechanizmus sa nachádza na opačnej strane rotorov než aktuálne nastavený znak, preto v prepojovacej tabuľke musíme hľadať prítomnosť blokovacích pinov na pozíciách o pár znakov posunutých. V prípade párnych rotorov má posunutie veľkosť 17 znakov v smere hodinových ručičiek. V prípade nepárnych rotorov sa jedná o posunutie o 20 znakov v smere hodinových ručičiek. Na nastaviteľných rotoroch nastavenie kruhu posunie umiestnenie blokovacích pinov, preto pozíciu pinov hľadáme na tejto pozícií: „aktuálne natočenie rotora(λ) + 20 miest pre párne (alebo 17 miest pre nepárne) + natočenie kruhu(σ)“.

Pri pohľade zhora, sa nepárne rotory pohybujú smerom ku klávesnici. Rotory sú poháňané sprava, takže v tomto prípade je tým rýchlym rotor č. 9. On posúva rotor č. 7, ktorý zase pohybuje rotorom č. 5 atď., až je nakoniec posúvaný i rotor č. 1. Blokovací pin opäť zabráni krokovaniu rotorov vľavo od neho. [1]

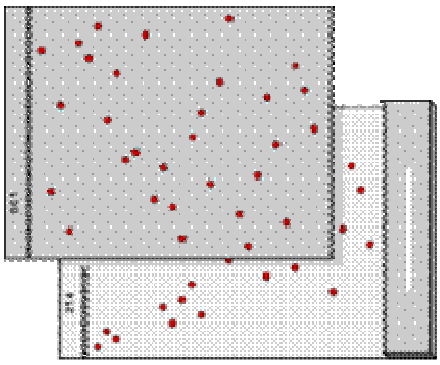
4 Čítačka karty

Medzi klávesnicou a čítačkou karty sú kontakty prepojené nasledovne:

Keyboard → Card Reader																												
А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Ю	Я	Й
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
17	25	30	14	26	21	6	19	1	15	29	20	4	28	24	2	22	23	18	12	7	5	27	8	10	9	16	13	11	3

Tab. 4. Substitúcia znaku medzi klávesnicou a čítačkou karty (prevzaté z [1]).

Čítačka karty (karta) je v podstate jedna matica s 30 riadkami a 30 stĺpcami, ktorá dovoľuje vzájomnú výmenu dvojíc písmen. Vložená karta musí obsahovať presne jedno prepojenie na každú kombináciu stĺpec-riadok. V prípade absencie karty sa vkladal do stroja kovový trojuholník, pri ktorom bolo identické zobrazenie vstupného znaku. [1]



Obr. 6. Karta s prepojeniami, ktorá sa vkladala do čítačky karty (prevzaté z [1]).

Používanie karty bolo súčasťou denného nastavenia Fialky. Na karte je možno nastaviť 30! rôznych prepojení, preto množina kľúčov s používaním karty pre fixné rotory je:
$30! \times 10! \times 30^{10}$**.**

5 Vstupný disk

Pri pravej strane sady rotorov je fixne pripevnený bakelitový disk. Jeho úlohou je odovzdať signál, prichádzajúci od čítačky karty a klávesnice, pravému krajnému rotoru. Vstupný disk tvorí spojenie nehybných a pohyblivých častí Fialky. [1]

Medzi čítačkou karty a vstupným diskom sú kontakty prepojené nasledovne:

Card Reader → Entry Disc																												
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
28	14	20	24	2	16	1	10	21	11	17	13	19	30	5	6	8	15	23	25	27	18	3	29	26	12	22	7	9	4

Tab. 5. Substitúcia znaku na vstupnom disku (prevzaté z [1]).

Medzi vstupným diskom a susedným rotorom je posun kontaktov, a to z toho dôvodu, že kontakty sú na vstupnom disku inak číslované (+3 pri smere zo vstupného disku na rotor a -3 pri opačnom smere).

6 Reflektor

Na ľavej strane sady rotorov je fixne pripevnený bakelitový disk, kteorý sa používa na odrazenie signálu naspäť do rotorov. Tým sa dosahuje reciprocita celej operácie šifrovania podobne, ako to bolo v Enigme. Oproti nej je však jeden rozdiel – znak môže byť zakódovaný sám na seba (v prípade Enigmy to nebolo možné, čo bola jedna z jej hlavných chýb).

26 kontaktov je prepojených do párov medzi sebou (tým tvoria cykly dĺžky 2). Jeden kontakt (označený číslom 13) je prepojený sám na seba, v dôsledku čoho sa s pravdepodobnosťou 1:30 znak zašifruje sám na seba. Zvyšné 3 kontakty už nie je možné spárovať ako predošlé, preto sú prepojené všetky tri medzi sebou a musia sa interpretovať inak pri šifrovaní a inak pri dešifrovaní (kontakty tvoria cyklus dĺžky 3).

Pozn.: Aj v tomto prípade sú kontakty posunuté ako to bolo aj v prípade vstupného disku.

	Reflector in Coding mode (3)																												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Coding (3)	23	6	20	28	14	2	12	17	22	11	10	7	13	5	29	18	8	24	27	3	25	9	1	16	21	30	19	4	15	26
Decoding (P)	23	6	20	28	14	2	12	17	22	11	10	7	13	5	29	24	8	16	27	3	25	9	1	18	21	30	19	4	15	26
Plain text (O)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Tab. 6. Substitúcie na reflektore vo všetkých módoch činnosti (prevzaté z [1]).

X	1	2	3	4	5	6	7	8	9
Y	23	6	20	28	14	2	12	17	22
X	10	11	12	13	14	15	17	19	20
Y	11	10	7	13	5	29	8	27	3
X	21	22	23	25	26	27	28	29	30
Y	25	9	1	21	30	19	4	15	26

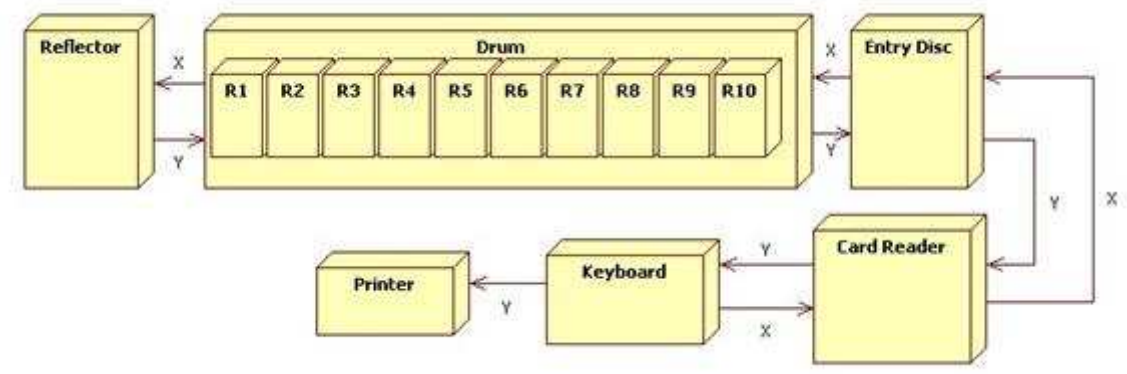
Tab. 7. Substitúcie na reflektore
(X - vstup, Y - výstup).

X	16	18	24
Y	18	24	16

Tab. 8. Substitúcie na reflektore
(X - vstup, Y - výstup).

7 Šifrátor Fialka M-125-xx

7.1 Schéma



Obr. 7. Blokový diagram Fialky M-125-xx (X - vstup, Y - výstup)

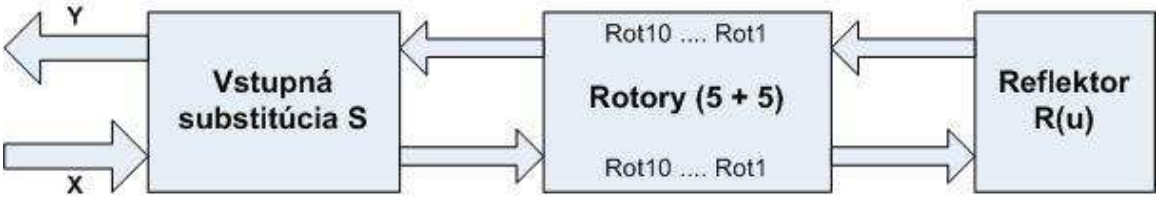
Vstupom šifrovacieho stroja je klávesnica, ktorá má 30 kláves. Pri stlačení klávesy je vyslaný elektrický prúd z klávesnice do súpravy šifrovacích zariadení. Najprv sa však aplikuje substitúcia znaku na klávesnici. Signál potom prejde cez čítačku kariet, čo umožní vzájomnú výmenu dvojíc písmen. Signál z čítačky kariet je poslaný na vstupný disk, kde sa aplikuje ďalšia substitúcia znaku. Vstupný disk pošle signál ďalej desiatemu rotoru, ten deviatemu, ten ôsmemu atď., až kým signál nedorazí k reflektoru, ktorý je úplne vľavo. Na reflektore je aplikovaná ďalšia substitúcia. Následne je signál vrátený späť cez súpravu rotorov na vstupný disk a čítačku kariet až na klávesnicu. Na odrazený signál sú aplikované inverzné substitúcie. Na výstup sa vytlačí zašifrovaný znak, potom nasleduje krokovanie rotorov. [1]

Stroj je možné používať v nasledujúcich troch módoch:

O – ako písací stroj
P – na rozšifrovanie správy
3 – na zašifrovanie správy

Do stroja bolo možné vložiť rotory typu PROTON-1 aj PROTON-2.

7.2 Matematický model



Obr. 8. Schéma šifrátora Fialka M-125-xx (X - vstup, Y - výstup).

V prvom rade je potrebné zmeniť vstupujúci (cyrilský/latinský) znak **X** na jeho číselné označenie z Tab. 1.a).

- Vstupná substitúcia je daná vzťahom:
  $S = S_3S_2S_1(x)$ (1), s nasledovným významom symbolov:
  S_1 – pevne zabudované prepojenie klávesnice (viď Tab. 4.)
  S_2 – čítačka karty (zakódovaná v karte, voliteľná podľa knihy denných kľúčov; pri absencii karty je identické zobrazenie)
  S_3 – pevne zabudované prepojenie vstupného disku (viď Tab. 5.)

Kvôli posunutiu medzi kontaktmi vstupného disku a pravého krajného rotora sa musí pridať hodnotu 3 k vystupujúcemu znaku zo vstupnej substitúcie *S*. Pri inverznej substitúcie sa táto hodnota odpočítava od vstupujúceho znaku.

- Substitúcia rotorov:

Rot_i (ρ_{10}) ... Rot_i (ρ_1) je dané z nastavení rotorov a z Tab. 2. alebo z Tab. 3. – závisí to od zvolenej série a typu rotorov. Rot_i označuje menovku vloženého rotora, ρ_{10} je pravý krajný rotor a ρ_1 je ľavý krajný rotor.

Substitúcia rotorov typu PROTON-1 (pevne daná):
Substitúciu jednotlivými rotormi Rot_i (ρ_j) (rotor s menovkou **i** na **j** – tom mieste podľa vloženia do stroja) môžeme definovať nasledovne:

1. Pridaj aktuálnu pozíciu (natočenie) rotora λ_i

2. Aplikuj substitúciu S_4 z tabuľky prepojenia rotorov (buď Tab. 2. alebo Tab. 3., podľa zvolenej série rotorov – 3K alebo 6K)
3. Odrátaj aktuálnu pozíciu rotora λ_i

Teda pre Rot_i platí: $\rho_i = S_4(x+\lambda_i) - \lambda_i \bmod 30$ (2)

Poznámka:
1. λ je číselné označenie z Tab.1.b),
2. inverzná substitúcia rotorov ρ_i^{-1} je identická pôvodnej substitúcie ρ_i s výnimkou, že je v 2. kroku aplikovaná inverzná substitúcia z tabuľky prepojenia rotorov.

Substitúcia rotorov typu PROTON-2 (nastaviteľná substitúcia):

Substitúciu jednotlivými rotormi Rot_i (ρ_j) (rotor s menovkou **i** na **j** – tom mieste podľa vloženia do stroja) môžeme definovať nasledovne:

1. Pridaj aktuálnu pozíciu (natočenie) rotora λ_i
2. Pridaj nastavenie kruhu (natočenie vonkajšieho kruhu, t.j. rozdiel medzi vonkajším kruhom a jadrom) rotora σ_i
3. Odrátaj nastavenie jadra (natočenie vnútornej časti – jadra) rotora τ_i
4. Aplikuj substitúciu $S_4(x)$ z tabuľky prepojenia rotorov (buď Tab. 2. alebo Tab. 3., podľa zvolenej série rotorov – 3K alebo 6K)
5. Pridaj nastavenie jadra rotora τ_i
6. Odrátaj nastavenie kruhu rotora σ_i
7. Odrátaj aktuálnu pozíciu rotora λ_i

Teda pre Rot_i platí: $\rho_i = S_4(x + \lambda_i + \sigma_i - \tau_i) + \tau_i - \sigma_i - \lambda_i \bmod 30$ (3)

Poznámka:
1. λ, τ, σ sú číselné označenia z Tab.1.b)
2. Nastaviteľné rotory s $\boldsymbol{\sigma} = 0$, $\boldsymbol{\tau} = 0$ a s nezmeneným jadrom (menovka jadra = menovka rotora, viditeľná je strana jadra s označením 1) sú spätne kompatibilné s pevnými rotormi s rovnakým označením (rovnakou menovkou).
3. Pri vložení jadra v pôvodnej polohe strany (strana s označením 1 je viditeľná), substitúcia v 4. kroku je aplikovaná z tabuľky prepojenia. Inverzná substitúcia rotorov ρ_i^{-1} je identická pôvodnej ρ_i s výnimkou, že je v 4. kroku aplikovaná inverzná substitúcia z tabuľky prepojenia rotorov.
4. Pri vložení jadra z opačnej strany (strana s označením 2 je viditeľná), substitúcia v 4. kroku je aplikovaná zo zrkadlovej tabuľky prepojenia. Inverzná substitúcia rotorov ρ_i^{-1} je identická pôvodnej ρ_i s výnimkou, že je v 4. kroku aplikovaná inverzná substitúcia zo zrkadlovej tabuľky prepojenia rotorov.
5. Pri zmene jadra sa na jednotlivých rotoroch aplikuje substitúcia z tabuľky prepojenia podľa označenia vloženého jadra, a nie rotora, lebo základné prepojenie obsahuje jadro. Pri pevných rotoroch boli jadrá fixne zabudované (menovka jadra sa rovnala menovke rotora).

- Substitúcia na reflektore:

$$R(u)=\begin{cases} pre\ u\neq 16,18,24: S_5(u),\ kde\ S_5\ je\ dané\ Tab.\ 7. \\ pre\ u=16,18,24\ (zašifrovanie): S_6(u),\ kde\ S_6\ je\ dané\ Tab.\ 8. \\ pre\ u=16,18,24\ (dešifrovanie): S_6^2(u),\ kde\ S_6\ je\ dané\ Tab.\ 8. \end{cases} \quad (4)$$

Kvôli posunutiu medzi kontaktmi reflektora a ľavého krajného rotora musíme odrátať -3 od vstupujúceho znaku na reflektor a pridať +3 k znaku, ktorý vystupuje z reflektora.

Výsledná šifrovacia funkcia môže byť zapísaná ako:

$$y = S_1^{-1}S_2^{-1}S_3^{-1}(-3)\rho_{10}^{-1}\ldots\rho_1^{-1}(+3)R(u)(-3)\rho_1\ldots\rho_{10}(+3)S_3S_2S_1(x) \quad (5)$$

Následne je potrebné zmeniť vystupujúce číslo späť na (cyrilský/latinský) znak z Tab.1.a).

Literatúra

[1] P. REUVERS, M. SIMONS: Codename Fialka, 2005 ISBN 978-90-79991-01-3 Dostupné na http://www.xat.nl/fialka/man/index.htm

[2] T. PERERA: Fialka museum, 2005. http://tomperera.com/enigma/mfmn.htm

[3] T. PERERA, D. HAMER: Enigma museum. http://w1tp.com/enigma/mfialka.htm

[4] http://www.sscnet.ucla.edu/geog/gessler/collections/crypto-fialka.htm

[5] http://jproc.ca/crypto/russian_m125_fialka.html

[6] http://www.ilord.com/fialka.html

[7] Grošek, Otokar – Vojvoda, Milan – Zajac, Pavol: Klasické šifry. - Bratislava : STU v Bratislave, 2007. - 214 p. - ISBN 978-80-227-2653-5

[8] Grošek, Otokar – Vojvoda, Milan – Zanechal, Marcel – Zajac, Pavol: Základy kryptografie. – Bratislava : STU v Bratislava, 2006. - ISBN 80-227-2415-7

[9] http://www.cryptomuseum.com/crypto/index.htm

[10] Grošek, Otokar - Zajac, Pavol: Automated cryptanalysis of classical ciphers. In: J. R. Rabunal Dopico, J. Dorado De La Calle, A. Pazos Sierra (Eds.): Encyclopedia of Artificial Intelligence, 2009, ISBN: 978-1-59904-849-9. pp. 186-191

D. Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC

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

Problematika infrastruktury veřejných klíčů (PKI)

Kurz seznámí účastníky s principy fungování PKI z různých aspektů. Účastník se seznámí se základními principy asymetrických šifer, s prací s certifikáty, fungováním certifikačních autorit, s požadavky zákona o elektronickém podpisu na různé subjekty a aplikací tohoto zákona v praxi, bude seznámen s technickým a legislativním pohledem na důvěru v certifikáty a přehledem různých druhů útoků na PKI (od praktických po teoretické). Součástí budou některé jednoduché praktické dovednosti – zejména práce s certifikáty (generování, export, import, podpis) a práce s CRL.

Datum	Čas	Lektor	Volná místa	Přihlásit
11.-12.05.2011	09:00–17:00	Pavel Vondruška	XX	

http://www.nic.cz/akademie/course/15/detail/

Pozor – zájemci z řad registrovaných čtenářů e-zinu Crypto-World mají možnost získat 50% slevu. Postup: zájemce požádá e-mailem (ezin@crypto-world.info) o zaslání slevového kódu (kupónu). Tento jedinečný kód mu zajistí uplatnění slevy PŘI REGISTRACI.

Garant: **Pavel Vondruška**

Cena

Základní cena: 4 000,00 Kč
Základní cena včetně DPH: 4 800,00 Kč
Čtenář Crypto-Worldu **50% sleva**

Cíl kurzu

Po absolvování kurzu bude účastník:

- rozumět principu asymetrických šifer
- znát základní informace k budování PKI a CA
- znát vybrané aspekty zákona o el. podpisu (typy certifikátů, podpisů, certifikačních autorit atd.)
- umět vygenerovat certifikát a zacházet s ním a příslušným soukromým klíčem
- pochopit princip důvěry v PKI a certifikáty
- mít základní přehled o možných útocích na PKI a použité šifry

Osnova

1. Základní pojmy asymetrické kryptografie
   - filozofie
   - algoritmy
   - podpisové schéma

2. Zákon o elektronickém podpisu č.227/2000 Sb.
   - stručné opakování základních pojmů
   - typy podpisů (elektronický podpis, zaručený elektronický podpis, elektronická značka)
   - typy poskytovatelů (kvalifikovaný, akreditovaný)
   - typy certifikátů (obyčejný, kvalifikovaný, systémový kvalifikovaný certifikát

3. Certifikační autority
   - přehledy poskytovatelů (ČR, SR)
   - jak pracují a co jej jejich úkolem

4. Praktické ukázky I.
   - certifikáty
   - úložiště
   - CRL
   - nastavení systému

5. Důvěra v elektronické podpisy
   - vystavitel
   - nastavení
   - certifikační cesta
   - technická důvěra x legislativa

6. Praktické ukázky II.
   - podpis Entrust, Adobe
   - podpis MS prostředí

7. Elektronická fakturace, archivace, ISDS

8. Otázky bezpečnosti elektronických podpisů

9. Obecné otázky bezpečnosti
   - Bezpečnost RSA
   - Bezpečnost hashovacích funkcí

http://www.nic.cz/akademie/course/15/detail/

E. O čem jsme psali v dubnu 2000 – 2010

F. 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 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 e-ziny, 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:	Vlastimil Klíma
	Pavel Vondruška
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
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@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.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