Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 13, číslo 5/2011 **15.květen**

5/2011

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1350 registrovaných odběratelů)

Obsah :

A. Československé šifry z obdobia 2. svetovej vojny Diel 5., Šifra „Rímska desať“

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.

5 Šifra „Rímska desať“

Šifra „Rímska desať“ bola šifrou typu STP, t.j. najskôr sa robila substitúcia, potom transpozícia a následne sa ešte pričítalo periodické heslo. Túto šifru používala napríklad stanica Barbora v operácii Antimony.

Popis šifry „Rímska desať“ je uvedený v knihe [2] na stranách 121–122. Presnejšie povedané, nejedná sa tam o popis, ale o nekompletný a neokomentovaný príklad šifrovania. Z tohto príkladu sa síce dá získať približná predstava o charaktere šifry, ale mnohé dôležité informácie tam chýbajú a môžme si ich len domýšlať. V popise a príklade šifrovania na tieto chýbajúce časti upozorníme.

5.1 Všeobecný popis a príklad šifrovania depeší

Pri šifrovaní sa najskôr nahradili znaky číslami, potom sa robila transpozícia podobná transpozícii plukovníka Rocheho a následne sa ešte pričítalo periodické heslo. Na príklade teraz popíšeme tieto kroky.

V knihe[2] nie je uvedená substitučná tabuľka, používaná pri nahrádzaní znakov číslami. Podľa príkladu na strane 121 by sa mohlo jednať o tabuľku podobnú tabuľke 1 (Crypto-World 4/2011, str. 3), použitej pri šifre „Rímska deväť“. Rozdiel je v tom, že pri „Rímskej desať“ sa v substitučnej abecede vyskytuje aj písmeno CH ako samostané písmeno s kódom 11. Podľa príkladu uvádzaného v [2] sa pri tejto šifre číslice nešifrovali, ale priamo opisovali. Toto, v podobe ako to uvádza pán Hanák, by bol pomerne veľký problém. Mohli by totiž nastať vážne problémy s nejednoznačnosťou pri dešifrovaní. Tento problém sa dá vyriešiť niekoľkými spôsobmi, žiaden z nich ale nie je v súlade s príkladom pána Hanáka. V jeho príklade depeša síce neobsahuje

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

Tabuľka 1: Česká 49 znaková abeceda pre „Rímsku desať“

čísla, ale pomocou čísel sa označuje nadväznosť častí seriálu depeše. Tieto čísla sú tam vypísané priamo a od textu depeše sú oddelené lomítkom. Možné riešenia problémov s číslami sú nasledovné. Po prvé, čísla môžme v depešiach vypisovať slovne. Po druhé, môžme použiť špeciálny znak, pomocou ktorého adresáta informujeme o prechode zo znakov na čísla a opačne. A napokon, po tretie, môžme rozšíriť substitučnú tabuľku o cifry a tie kódovať rovnako ako ostatné znaky. V našom príklade použijeme posledné spomenuté riešenie, pretože je v súlade s ostatnými používanými šiframi a zdá sa byť preto najpravdepodobnejšie. Nadväznosť jednotlivých častí série budeme označovať písmenami abecedy, rovnako ako sa to robilo aj pri ďalších šifrách. Takže na substitúciu znakov číslami budeme pre šifru „Rímska desať“ používať substitučnú tabuľku 1.

Pri šifrovaní sa používalo týždenné heslo a z neho sa potom tvorilo denné heslo cyklickým posunom. V [2] nie sú uvedené žiadne podrobnosti o pravidlách tvorby hesla, ale dá sa predpokladať, že heslá mali stanovené limity pre minimálnu a maximálnu dĺžku. Rozumné hranice sa zdajú byť 15–20 znakov, pričom medzery a interpunkčné znamienka sa nepočítajú. My si pre náš príklad zvolíme heslo:

Nikto nežije bez viny.

ktorého autorom je Marcus Porcius Cato starší. Toto heslo vyčíslime obvyklým spôsobom podľa použitej substitučnej abecedy, pričom medzery a interpunkčné znamienka vynechávame:

N	I	K	T	O	N	E	Ž	I	J	E	B	E	Z	V	I	N	Y
10	5	9	14	13	11	2	18	6	8	3	1	4	17	15	7	12	16

Týmto sme dostali číselné týždenné heslo. Z neho cyklickým posunom dostaneme denné heslo, pomocou ktorého potom šifrujeme depešu. Opäť sa v [2] neuvádza, podľa čoho sa určuje cyklický posun. Či to bol deň týždňa, deň

mesiaca, dátum šifrovania, vopred dohodnutá postupnosť čísel, iný parameter, prípadne kombinácia týchto parametrov. Toto nie je z príkladu v [2] zrejmé. Pre náš príklad zvolíme za prvý znak denného hesla Ž a odtiaľ potom z vyčíslenia týždenného hesla cyklickým posunom dostaneme denné heslo:

Ž	I	J	E	B	E	Z	V	I	N	Y	N	I	K	T	O	N	E
18	6	8	3	1	4	17	15	7	12	16	10	5	9	14	13	11	2

Ako text na šifrovanie zoberieme latinské príslovie:

> *Kapka hloubí kámen nikoliv silou, ale častým padáním. Podobně se člověk stává učeným ne mocí, ale až po dlouhé době studia.*[1]

Text depeše musíme rozdeliť na kratšie časti tak, aby žiadna z nich, po prevedení do číselnej podoby, nemala viac než $\frac{n(n+1)}{2}$ cifier, kde n je počet znakov hesla. Je to dané spôsobom, akým sa robí transpozícia, pretože transpozičná tabuľka má práve toľko políčok. Takže text zapíšeme pomocou znakov zo substitučnej tabuľky 1, rozdelíme ho na menšie časti a jednotlivé časti seriálu doplníme označením nadväznosti rovnako, ako sme to robili pri iných popisovaných šifrách. V našom príklade dostaneme dve depeše (časti seriálu):

```
KAPKA HLOUBI KAMEN NIKOLIV SILOU,ALE ČASTYM PADANIM.PODOBNĚ SE/A
--------------------------------------------------------------
A/ČLOVĚK STAVA UCENYM NE MOCI,ALE AŽ PO DLOUHE DOBĚ STUDIA.EIŽ
```

Na koniec poslednej časti série píšeme podpisové znaky, v našom príklade EIŽ. Podpisové znaky sú oddelené od textu depeše bodkou a tvoria ich tri znaky, ktoré dostaneme z denného hesla. Je to znak vľavo a vpravo od prvého znaku denného hesla a prvý znak denného hesla. Následne nahradíme znaky číslami, podľa substitučnej tabuľky 1. Za špeciálnymi znakmi medzery, ako obvykle, vynechávame a inde medzery medzi slovami nahrádzame číslami 5, 6, 7, 8 alebo 9. Pri rozdeľovaní depeše na časti dbáme na to, aby jednotlivé časti depeše v číselnom tvare mali rôznu dĺžku. Pokiaľ by sme mali viacero depeší rovnakej dĺžky, šifrovaných tým istým heslom, mohli by sme pri lúštení použiť anagramovú metódu. Ak dĺžka depeše v číselnom tvare nie je násobkom 5, doplníme na koniec depeše potrebný počet cifier predstavujúcich medzery. Naše dve depeše v číselnom tvare budú mať podobu:

```
14011 91401 51015 18260 21261 40116 06177 17121 41815 12278
23121 51826 35011 50690 40123 25301 65190 10501 17121 63319
18051 80217 07623 06370 15986
```

[1] Pôvodná verzia v latinčine: *Gutta cavat lapidem, non vi, sed saepe cadendo. Sic homo fit doctus, non vi, sed saepe studendo.*

```
01370 41518 27071 47232 50127 01826 03061 73016 91706 51618
03123 50115 06601 32719 18805 15182 61006 90518 02075 23252
60512 01330 61232
```

Prvá časť mala 121 cifier, takže sme na jej koniec doplnili cifry `5986`. Druhá časť depeše má 115 cifier a nebolo potrebné nič dopĺňať. Pokiaľ vieme ako sa robí nahrádzanie znakov číslami, doplnené cifry ľahko spoznáme.

Následne depeše v číselnej podobe zapíšeme do tabuliek pomocou ktorých realizujeme transpozíciu. Ak bola dĺžka hesla (počet znakov) n, transpozičná tabuľka bude mať rozmer $n \times n$. Jej stĺpce budú očíslované pomocou týždenného hesla a riadky budú očíslované pomocou denného hesla. Do každého riadku tabuľky, z hora nadol, zapíšeme práve toľko cifier depeše, koľko určuje hodnota denného hesla pre príslušný riadok. V našom príklade tieto tabuľky budú mať nasledovný tvar:

10	**5**	**9**	**14**	**13**	**11**	**2**	**18**	**6**	**8**	**3**	**1**	**4**	**17**	**15**	**7**	**12**	**16**	
1	4	0	1	1	9	1	4	0	1	5	1	0	1	5	1	8	2	**18**
6	0	2	1	2	6													**6**
1	4	0	1	1	6	0	6											**8**
1	7	7																**3**
1																		**1**
7	1	2	1															**4**
4	1	8	1	5	1	2	2	7	8	2	3	1	2	1	5	1		**17**
8	2	6	3	5	0	1	1	5	0	6	9	0	4	0				**15**
1	2	3	2	5	3	0												**7**
1	6	5	1	9	0	1	0	5	0	1	1							**12**
7	1	2	1	6	3	3	1	9	1	8	0	5	1	8	0			**16**
2	1	7	0	7	6	2	3	0	6									**10**
3	7	0	1	5														**5**
9	8	6																**9**
																		14
																		13
																		11
																		2

10	**5**	**9**	**14**	**13**	**11**	**2**	**18**	**6**	**8**	**3**	**1**	**4**	**17**	**15**	**7**	**12**	**16**	
0	1	3	7	0	4	1	5	1	8	2	7	0	7	1	4	7	2	**18**
3	2	5	0	1	2													**6**
7	0	1	8	2	6	0	3											**8**
0	6	1																**3**
7																		**1**
3	0	1	6															**4**
9	1	7	0	6	5	1	6	1	8	0	3	1	2	3	5	0		**17**
1	1	5	0	6	6	0	1	3	2	7	1	9	1	8				**15**
8	0	5	1	5	1	8												**7**
2	6	1	0	0	6	9	0	5	1	8	0							**12**
2	0	7	5	2	3	2	5	2	6	0	5	1	2	0	1			**16**
3	3	0	6	1	2	3	2											**10**
																		5
																		9
																		14
																		13
																		11
																		2

Ako vidno, obe tabuľky sú neúplné. Pre správne dešifrovanie depeše potrebuje adresát poznať jej dĺžku, aby vedel ako dlhé sú jednotlivé stĺpce tabuľky. Preto je nutné dĺžku depeše indikovať medzi služobnými údajmi. K tvorbe služobných údajov depeše sa ešte dostaneme neskôr. Teraz dokončíme popis procesu šifrovania.

Depešu v číselnej podobe máme zapísanú v transpozičnej tabuľke. Jednotlivé cifry z tabuľky budeme čítať a vypisovať po stĺpcoch zhora nadol, v poradí určenom týždenným heslom. Cifry zapisujeme v päťmiestnych skupinách. Naše dve depeše po transpozícií budú mať podobu:

```
13910 10210 13252 61801 05404 71122 61178 07559 01501 80016
02072 86352 70616 11174 81172 39966 10303 68112 15559 67511
11132 11015 10821 24146 21013

-----------------------------------------------------------

73105 10108 92320 78001 91120 60110 60311 35245 18821 63511
17551 70037 07391 82234 26561 63270 01266 50217 08600 10561
38027 21253 61052
```

Napokon ešte pod cifry, ktoré sme dostali transpozíciou, podpíšeme periodicky denné heslo a sčítame modulo 10, t.j. bez prenosu desiatok. Tým je šifrovanie ukončené. Prvá depeša bude mať podobu:

```
Cifry:  13910 10210 13252 61801 05404 71122 61178 07559 01501
Heslo:  18683 14171 57121 61059 14131 12186 83141 71571 21610
-------------------------------------------------------------
Depeša: 21593 24381 60373 22850 19535 93208 44219 78020 22111

Cifry:  80016 02072 86352 70616 11174 81172 39966 10303 68112
Heslo:  59141 31121 86831 41715 71216 10591 41311 21868 31417
-------------------------------------------------------------
Depeša: 39157 33193 62183 11321 82380 91663 70277 31161 99529

Cifry:  15559 67511 11132 11015 10821 24146 21013
Heslo:  15712 16105 91413 11218 68314 17157 12161
-----------------------------------------------
Depeša: 20261 73616 02545 22223 78135 31293 33174
```

a druhá depeša bude mať pododu:

```
Cifry:  73105 10108 92320 78001 91120 60110 60311 35245 18821
Heslo:  18683 14171 57121 61059 14131 12186 83141 71571 21610
-----------------------------------------------------------
Depeša: 81788 24279 49441 39050 05251 72296 43452 06716 39431

Cifry:  63511 17551 70037 07391 82234 26561 63270 01266 50217
Heslo:  59141 31121 86831 41715 71216 10591 41311 21868 31417
-----------------------------------------------------------
Depeša: 12652 48672 56868 48006 53440 36052 04581 22024 81624

Cifry:  08600 10561 38027 21253 61052
Heslo:  15712 16105 91413 11218 68314
-----------------------------------
Depeša: 13312 26666 29430 32461 29366
```

Týmto je proces šifrovania ukončený a zostáva len pridať služobné údaje. Tie sa pridávali na koniec depeše ako tri päťmiestne skupiny a maskovali sa pomocou prvých troch skupín zašifrovanej depeše. V [2] opäť nie sú uvedené žiadne detaily. Veľmi vágne sa tam spomína, že posledné tri skupiny obsahovali „varovnú nulu a údaje o nasledujúcej relácii“. Pojem „varovná nula“ sa spomína aj v iných knihách o československých šifrách z druhej svetovej vojny. Odosielateľ depeše umiestnením cifry `0` na vopred dohodnuté miesto depeše (zrejme v služobných údajoch) oznamoval adresátovi, že pracuje pod nátlakom. V uvedenom príklade v [2] sú nuly dve, takže si môžme len domýšlať, ktorá z nich je „varovná“. Podobne aj to, ako sa kódovali údaje o nasledujúcej relácii, je len dohad. V našom príklade použijeme rovnaké relačné údaje ako sú uvedené v [2] a pokúsime sa interpretovať ich význam. Relačné údaje budú `27 11 30`. Keďže to majú byť údaje o nasledujúcej relácii, `27` pravdepodobne znamená 27. deň mesiaca a `11 30` bude asi označovať čas nasledujúcej relácie 11^{30}. Každá z týchto šiestich cifier sa kódovala ako ľubovoľne zvolený súčet dvoch cifier modulo 10, ktorého výsledkom je príslušná cifra. Za zakódované prvé dve cifry (v našom príklade `27`) sa pridávala jedna náhodná cifra. To bolo pravdepodobne miesto, kam sa umiestňovala „varovná nula“. Čiže ak posledná cifra prvej skupiny bola `0`, adresátovi to signalizovalo, že odosielateľ pracuje pod nátlakom. A na koniec tretej skupiny sa dávali náhodne dve cifry. Takto dostaneme tri päťmiestne skupiny. Pod ne zapíšeme prvé tri skupiny zašifrovanej depeše a sčítame modulo 10. Takže v našom príklade budú mať tri skupiny služobných údajov prvej depeše podobu:

Relačné údaje:	2		7			1		1		3	0				
Zvolené cifry:	7	5	9	8	**0**	6	5	8	3	6	7	5	5	1	4
Prvé 3 skupiny:	2	1	5	9	3	2	4	3	8	1	6	0	3	7	3
Depeša:	9	6	4	7	3	8	9	1	1	7	3	5	8	8	7

Ako vidno, použili sme „varovnú nulu“. Je to posledná cifra prvej skupiny pri zvolených cifrách (druhý riadok) a je zapísaná tučným fontom.
Tri skupiny služobných údajov druhej depeše podobu:

Relačné údaje:	2		7			1		1		3	0				
Zvolené cifry:	6	6	5	2	**3**	4	7	2	9	5	8	2	8	5	3
Prvé 3 skupiny:	8	1	7	8	8	2	4	2	7	9	4	9	4	4	1
Depeša:	4	7	2	0	1	6	1	4	6	4	2	1	2	9	4

Tu sme nedali „varovnú nulu“, ale len preto, aby sme ilustrovali tvorbu služobných údajov bez nej. V praxi by sa samozrejme varovná nula buď dávala do všetkých častí seriálu, alebo do žiadnej. Podľa toho, či odosielateľ pracoval, alebo nepracoval pod nátlakom.

V popise tejto šifry sa v [2] nikde neuvádzajú informácie o záhlaví a o tom, aké údaje v ňom boli obsiahnuté. Keďže ale pre dešifrovanie je potrebné poznať dĺžku depeše, bolo by veľmi žiaduce, aby záhlavie obsahovalo informáciu o počte cifier depeše. Okrem toho je pravdepodobné, že záhlavie obsahovalo aj poradové číslo depeše a možno aj dátum šifrovania. Ak teda k depešiam pridáme aj služobné údaje a záhlavie, dostaneme konečný tvar depeší:

```
017-140-14
21593 24381 60373 22850 19535 93208 44219 78020 22111 39157
33193 62183 11321 82380 91663 70277 31161 99529 20261 73616
02545 22223 78135 31293 33174 96473 89117 35887
------------------------------------------------------------


018-130-14
81788 24279 49441 39050 05251 72296 43452 06716 39431 12652
48672 56868 48006 53440 36052 04581 22024 81624 13312 26666
29430 32461 29366 47201 61464 21294
```

pripravený na odoslanie. Záhlavie depeše je v tvare `xxx-yyy-zz`, kde `xxx` je poradové číslo depeše, `yyy` je počet cifier depeše a `zz` je deň šifrovania depeše.

5.2 Postup pri šifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii text na šifrovanie.

b. Máme 15–20 znakov dlhé týždenné heslo.

c. Máme určený prvý znak denného hesla, ktoré sa z týždenného hesla dostane cyklickým posunom.

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

e. Je daný dátum šifrovania (uvádza sa v záhlaví).

f. Máme dátum a čas nasledovnej relácie (pre služobné údaje).

Potom šifrovanie depeše prebieha 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. Týždenné heslo aj s jeho vyčíslením cyklicky posunieme tak, aby sa začínalo určeným znakom denného hesla.

3. Podľa posunutia hesla vytvoríme podpis depeše. Tento je trojznakový a tvoríme ho tak, že vezmeme jeden znak vľavo, jeden znak vpravo od prvého znaku denného hesla a prvý znak denného hesla. Podpis pridávame na koniec šifrovaného textu 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 abecede nevyskytujú.

5. Pokiaľ sa medzi slovami textu nachádza niektorý zo špeciálnych znakov obsiahnutých v substitučnej abecede, vynecháva sa za ním medzera.

6. Text rozdelíme na kratšie časti tak, aby každá časť končila kompletným slovom a žiadna časť po prepise do číselnej podoby nebola dlhšia než $\frac{n(n+1)}{2}$ cifier, kde n je počet znakov hesla. Pri rozdeľovaní dávame pozor na to, aby žiadne dve časti nemali rovnakú dĺžku.

7. Na koniec prvej časti pridáme, kvôli nadväznosti dielov, `/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 a 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) dvojcifernými číslami. Medzery v texte sa nahrádzajú ciframi `5, 6, 7, 8` alebo `9`.

10. Postupnosť čísel, ktorú sme dostali rozdelíme na skupiny po 5 cifier. Pokiaľ počet cifier nie je násobkom 5, náhodne doplníme chýbajúce cifry číslami `5, 6, 7, 8` alebo `9`.

11. Cifry depeše zapisujeme do tabuľky rozmeru $n \times n$ zľava doprava a zhora nadol. Stĺpce transpozičnej tabuľky sú očíslované týždenným heslom zľava doprava, riadky sú očíslované denným heslom zhora nadol. Do každého riadku tabuľky zapíšeme práve toľko cifier, koľko určuje hodnota denného hesla pre príslušný riadok.

12. Cifry depeše vypisujeme z transpozičnej tabuľky zhora nadol po stĺpcoch, v poradí určenom týždenným heslom. Cifry zapisujeme do päťmiestnych skupín.

13. Pod cifry depeše periodicky podpíšeme cifry denného hesla.

14. Sčítame cifry depeše s ciframi denného hesla modulo 10, t.j. bez prenosu desiatok.

15. Vytvoríme tri päťmiestne skupiny služobných údajov. **Nevieme ako sa v skutočnosti tvorili skupiny služobných údajov. Tu popisovaný postup je vymyslený na základe neokomentovaného príkladu z [2] !** Služobné údaje pravdepodobne obsahovali deň mesiaca, hodinu a minútu nasledujúcej relácie a „varovnú nulu“ pre prípad, že odosieľateľ pracoval pod nátlakom.

    (a) Relačné údaje pozostávajú zo šiestich cifier: `dd hh mm`. Prvé dve cifry určujú deň mesiaca, druhé dve cifry hodinu a tretia dvojica cifier minútu nasledujúcej relácie.

(b) Každú zo šiestich cifier relačných údajov rozpíšeme ako ľubovoľný súčet dvoch cifier modulo 10, ktorého výsledkom je príslušná cifra. Napríklad 3 môžme rozpísať ako $(4+9) \bmod 10$ alebo $(6+7) \bmod 10$ a pod. Takto dostaneme 12 cifier.

(c) Za prvé štyri cifry z predošlého bodu zapíšeme ľubovoľnú cifru. Táto cifra má funkciu „varovnej nuly“. Pokiaľ teda odosielateľ pracuje pod nátlakom, zapíše na toto miesto nulu. Inak tam napíšeme ľubovoľnú cifru rôznu od nuly.

(d) Takto sme dostali postupnosť 13-tich cifier. Na jej koniec pripíšeme dve ľubovoľné cifry a dostávame 15 cifier, čiže tri päťmiestne skupiny.

(e) Pod tri päťmiestne skupiny z predošlého bodu podpíšeme prvé tri skupiny zašifrovanej depeše a sčítame modulo 10. Tým dostaneme tri päťmiestne skupiny služobných údajov, ktoré pridáme na koniec zašifrovanej depeše.

16. Na začiatok depeše pridáme ešte návestie v tvare `xxx-yyy-zz`, kde `xxx` je poradové číslo depeše, `yyy` je počet cifier depeše a `zz` je deň šifrovania depeše. Týmto je šifrovanie depeše ukončené.

5.3 Postup pri dešifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii kompletný text zašifrovanej depeše.

b. Máme týždenné heslo.

c. Máme určený prvý znak denného hesla, ktoré sa z týždenného hesla dostane cyklickým posunom.

Potom dešifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Na základe návestia overíme kompletnosť depeše (počet cifier).

2. Vynecháme návestie depeše, ktoré už nebudeme potrebovať.

3. Pod posledné tri skupiny depeše podpíšeme prvé tri skupiny depeše a odpočítame modulo 10. Tým dostaneme tri skupiny zakódovaných služobných údajov. Posledné dve cifry môžme vynechať, pretože boli náhodne pridané a sú tam len na doplnenie počtu cifier do 15. Zakódované služobné údaje pozostávajú z 13-tich cifier, ktoré budeme ďalej zpracovávať:

(a) Prvú a druhú dvojicu cifier zakódovaných služobných údajov sčítame modulo 10. Tým dostaneme dve cifry označujúce deň mesiaca nasledujúcej relácie.

(b) Piata cifra má funkciu „varovnej nuly“. Pokiaľ je táto cifra nula, tak to znamená, že odosieľateľ pracoval pod nátlakom. Inak je táto cifra len do počtu.

(c) Súčet modulo 10 ďalších dvoch dvojíc cifier dá dve cifry určujúce hodinu nasledujúcej relácie.

(d) Súčet modulo 10 posledných dvoch dvojíc cifier dá dve cifry určujúce minútu nasledujúcej relácie.

4. Služobné údaje už máme zpracované, takže posledné tri skupiny depeše vynecháme, pretože ich už nebudeme potrebovať.

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

6. Týždenné heslo aj s jeho vyčíslením cyklicky posunieme tak, aby sa začínalo určeným znakom denného hesla.

7. Periodicky podpíšeme denné heslo pod cifry depeše a spravíme rozdiel cifier depeše a cifier denného hesla modulo 10, t.j. bez prenosu desiatok.

8. Cifry depeše zapisujeme do tabuľky rozmeru $n \times n$. Stĺpce transpozičnej tabuľky sú očíslované týždenným heslom zľava doprava, riadky sú očíslované denným heslom zhora nadol. V každom riadku tabuľky bude práve toľko cifier, koľko určuje hodnota denného hesla pre príslušný riadok. Dĺžku depeše (počet cifier) poznáme, takže vieme, koľko riadkov tabuľky bude obsadených a ktoré stĺpce posledného použitého riadku budú kratšie. Cifry do tabuľky zapisujeme zhora nadol po stĺpcoch, v poradí určenom týždenným heslom.

9. Cifry depeše vypisujeme z transpozičnej tabuľky po riadkoch zľava doprava a zhora nadol.

10. Z konca depeše vynecháme náhodne pridané cifry. Tieto spoznáme podľa toho, že na miestach desiatok majú cifry `5, 6, 7, 8` alebo `9`.

11. Podľa substitučnej tabuľky 1 (str. 3) nahradíme čísla depeše znakmi. Znaky sú kódované dvojcifernými číslami. Pokiaľ sa na mieste desiatok vyskytuje cifra `5, 6, 7, 8` alebo `9`, jedná sa o medzeru a tá je kódovaná len jednou cifrou.

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

13. Pokiaľ sa jedná o sériu, text zostavíme v správnom poradí podľa označenia na začiatku a konci jednotlivých častí.

5.4 Lúštenie

Lúštenie šifry „Rímska desať“ je náročnejšie, než lúštenie doteraz popisovaných šifier. Okrem toho, že transpozičná tabuľka má rôzne dlhé riadky, tak pri transpozícii sa „roztrhajú“ dvojciferné čísla predstavujúce znaky. To samo o sebe ešte nie je veľký problém (ako sa ukázalo pri lúštení šifry STT), ale naviac sa k výsledku transpozície pričítalo periodické heslo. V takomto prípade je prakticky nereálne použitie Kasiského metódy na odhalenie periodického hesla. Museli by byť splnené veľmi špeciálne podmienky, ktoré sa v praxi nedajú očakávať.

Napriek uvedenému, táto šifra nie je nerozlúštiteľná a bola počas vojny lúštená. Asi najťažšou časťou lúštenia bolo nájdenie správnych dĺžok riadkov transpozičnej tabuľky. Substitučné tabuľky českých znakov boli už lúštiteľom známe z predošlých šifier, takže substitúcia predstavovala v tomto prípade tú ľahšiu časť úlohy. Okrem toho je možné na šifru útočiť aj na základe očakávaného textu (začiatky a konce depeší, označenie nadväznosti častí seriálu a pod.) a využívali sa aj chyby šifrantov ako boli napríklad rovnako dlhé depeše šifrované tým istým heslom.

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. Vzpomínky a poznámky čtenáře k tématu Fialka M-125 Jeroným Knížek (knizek@centrum.cz)

Někdy kolem r. 1963 jsem se zúčastnil v Komorním Hrádku u Chocerad krátkého soustředění asi 20 Náč. 8. odd. svazků ČSLA, kde nám pplk. Robert Sobol z ŠO GŠ poprvé ukázal dva kódovací stroje Fialka a měli jsme pomoci GŠ řešit jeho organizační strukturu a využití v ČSLA. Tam jsme se dověděli základní data stroje. Měl jenom azbuku a jedno nevýměnné typové kolečko, sadu 10 disků a nastavovací kartu 30x30. Dalo se psát i ve skupinách na dlp pásku a snad perforovat i číst 5 stopou DP. Už nepamatuji způsob dálkové korespondence, snad přes starý dálnopis Siemens psaním ve skupinách či telefonem (spojaři přece ještě všude neměli vysílače a děrovače pásky a my na svazcích už měli nový ŠD1 pro přímé dlps spojení, (ten byl zanedlouho nahražen stroji ŠD3). Přídavků 322 byl nedostatek, upravil jsem si proto k tomu vysílač německý a dobře mi sloužil u 1. td i při cvičeních v poli. Několikrát jsem svým polním pracovištěm V3S zajišťoval na cvičeních i GŠ.

Potom GŠ objednal menší dodávku již zdokonalených strojů, které měly i latinskou abecedu a zorganizoval vyškolení několika desítek šifrantů v rozborce, údržbě a seřizování Fialky, kterého jsem se v Komorním Hrádku zúčastnil. Viděl jsem tam, jak někteří kolegové si navzájem povyměňovali klávesnice aj. Pamatuji, že jsme při nastavování otáčeli i kontaktní kroužky uvnitř disků podle tabulky (o tom se autor článku nezmiňuje, snad toto nastavování ani nezná). Název sad disků PROTON se objevil až později snad r. 1976. Tehdy už jsem sloužil 2 roky na GŠ a měly se objednat další dodávky Fialek a s tím i disků PROTON pro případ skutečného polního nasazení ČSLA. Přeložil jsem veškerou sovětskou dokumentaci včetně seznamu součástek a náhradních dílů, zpracoval české příručky, jakož i formuláře pro provádění oprav atd. Dost jsem se natrápil jak zajistit změnu typů na typovém kolečku, aby bylo možno navzájem korespondovat se všemi armádami VS, což vyžadovalo i zásah do uspořádání abeced na klávesnici a několik výměnných typových koleček. Na klávesnici jsem doplnil písmena s háčky tuším v horní řadě a písmeno A jsem musel dát doprostřed spodní řady. Němcům z NDR stačilo původní rozložení latinky, pro jedničku a nulu užívali písmena I a O. Nakonec se mi to podařilo a stroje byly podle toho pro ČSLA vyrobeny a dodány. Byly již upraveny pro vysílání a příjem po dálnopisné lince či nepřímo předáním označených děr. pásek k odeslání jinou cestou. Péči o Fialku ode mne převzal asi r. 1977 pplk. Šoltész (a skupina mat. zásobování).

V Novém městě nad V. bylo postupně vyškoleno několik set obsluh Fialky a ta byla nasazena na stupni divize – pluk, dále u topografů, dělostřelců a leteckého zásobování. Sám jsem učil v několika takových kurzech. Tehdy, kdy ještě pošt. spoje neměly vyřešené takové spojení, voj. spoj. výzkum nám k Fialce vymyslel způsob vysílání dlps. zpráv po telefonní lince, což bylo prakticky vyzkoušeno. Nakonec ale vše bylo uspořádáno jinak; v té době bylo více využíváno ZASů, důležitější zprávy šly přes šifrstroje ŠD3 aj. Pokud vím, k nasazení ostrých disků PROTON nikdy nedošlo (měly jimi být vybaveny jen některé prvosledové svazky).

Je to už mnoho let a detaily si už nejsem zcela jist…

C. Rotorový šifrátor Fialka M-125
Diel 2., Porovnanie s viacerými rotorovými šifrátormi

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

1 Okolnosti vzniku šifrátora Fialka

Ako bolo spomenuté v predošlom článku, Fialka bola prvýkrát zavedená do používania okolo roku 1965. Vďaka utajovaniu informácií sa dlhú dobu predpokladalo, že sovietska armáda nemala detailné informácie o Enigme. Avšak nápadná podobnosť Fialky s Enigmou bola dostatočným dôvodom myslieť si, že sovieti mali podrobný popis Enigmy. Pri tvorbe zohľadňovali aj nedostatky Enigmy a pokúsili sa o ich nápravu. Inšpirácia Enigmou bola podložená príbehom, ktorý bol zverejnený v roku 1999. Tento príbeh odhalil študenta, ruského špióna Johna Cairncrossa, ktorý pracoval na projektoch prelomenia nemeckých šifier v Bletchley Parku v Anglicku. [1]

2 Základná koncepcia rotorových šifrátorov

Spochybnená bezpečnosť šifier s malou periódou opakovaných znakov viedla k využitiu kľúčov, ktoré sa menia pri šifrovaní každého znaku. Rozvíjanie tejto myšlienky viedlo k návrhu nových typov šifier. Do jednej skupiny patria aj rotorové šifrátory (v týchto šifrátoroch sa k i-temu znaku x_i otvoreného textu priraďuje znak y_i pomocou permutácie π a kľúčov k_i, λ_i v tvare $y_i=\pi(x_i+k_i)-\lambda_i$). Výpočet sa realizuje pomocou elektromechanického princípu. [2]

Myšlienkou rotorového šifrátora sa zaoberali aj mnohí konštruktéri, ako napríklad Američan Edward Hebern a Holanďan Hugo Alexander Koch. Patent nakoniec odkúpil nemecký inžinier Scherbius, a v roku 1924 predstavil svoj vlastný fungujúci stroj, ktorý nazval Enigma. [4] Enigma zohrala významnú úlohu počas druhej svetovej vojny, v ktorej bola používaná Nemeckou armádou.

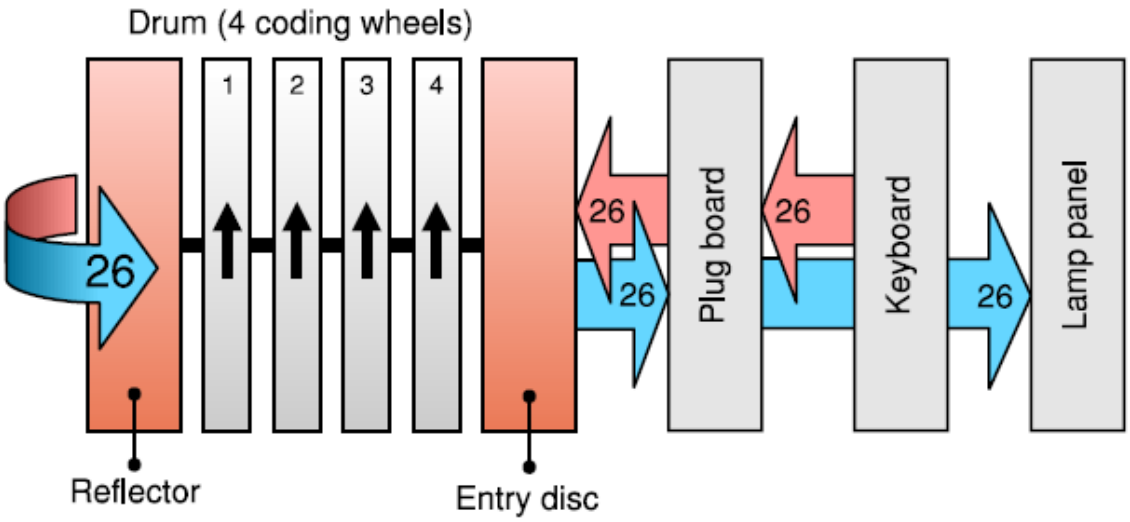
Z hľadiska konštrukcie prebieha šifrovanie na rotorových šifrátoroch nasledovným spôsobom:

- Vstupom celého zariadenia je mechanická klávesnica. Po každom stlačení klávesy sa vyšle elektrický signál z klávesnice cez príslušné elektrické vedenie a prepojenia až na výstup šifrátora. Treba si uvedomiť, že sa jedná o jediný elektrický obvod, v ktorom rôzne permutácie znamenajú rôzne prepojenia kontaktov na rôznych miestach. Výsledná zmena vstupu sa prejaví až pri výstupe. Z tohto hľadiska jednému vstupu prislúcha vždy len jeden výstup, pričom sa toto prepojenie môže zmeniť v každom kroku (t.j. po každom stlačení klávesy).

- Výstupný, už zašifrovaný znak môže byť reprezentovaný rôznymi spôsobmi. V prípade Enigmy sa po zašifrovaní daného vstupu rozsvietila jedna z lámp na svetelnom paneli. Každá lampa reprezentovala príslušný výsledný znak. Táto metóda nie je najefektívnejšia, pretože spomaľuje celú šifrovaciu procedúru a zvyšuje možnosť vnesenia chyby obsluhou.

  V prípade Fialky sa výstupný znak tlačil na papierový pásik [1] podobným spôsobom, ako sa tlačia znaky na písacích strojoch. Bola implementovaná aj možnosť reprezentovať znaky vlastnými symbolmi, a to namiesto tradičných tlačených písmen postupnosťami dier rôznych veľkostí.

3 Fialka vs. Enigma

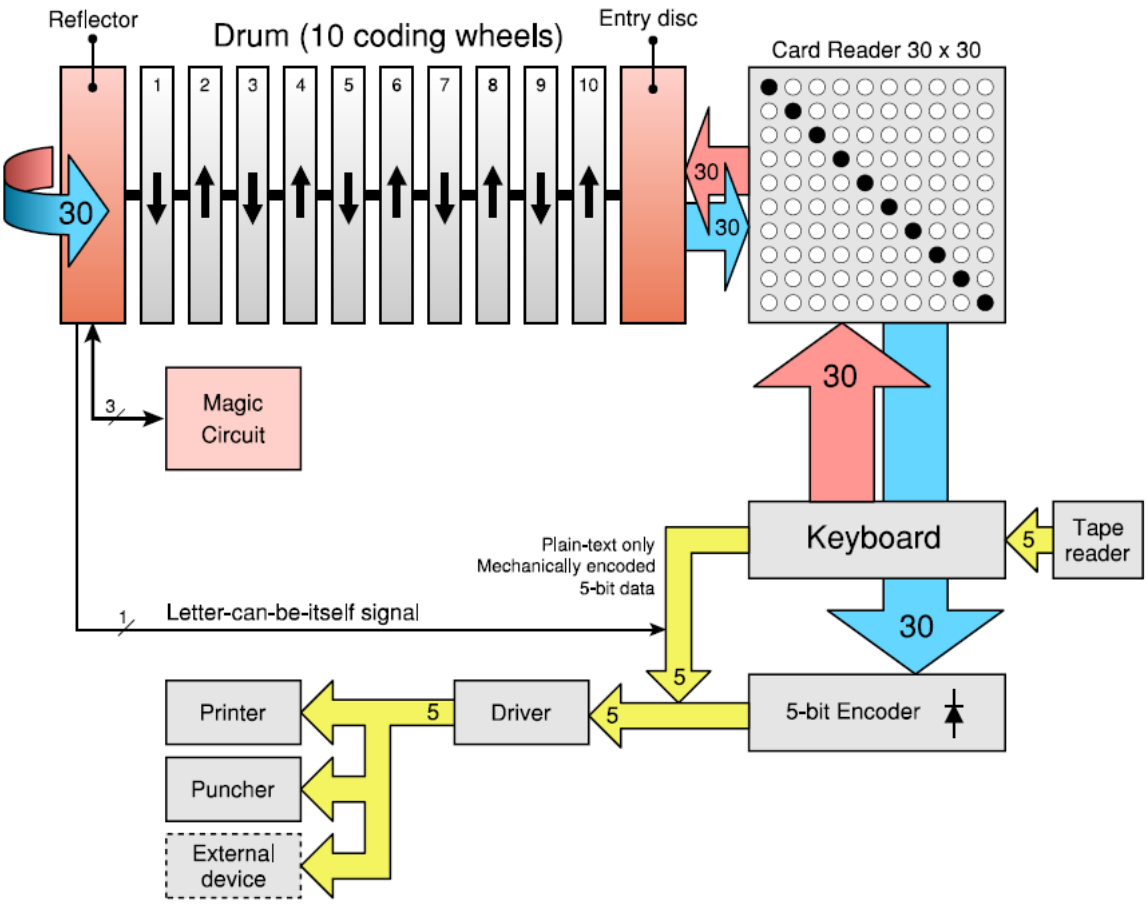


Obr. 1. Blokový diagram Enigmy (prevzaté z [1])

Jadro Enigmy pozostáva zo súpravy pohybujúcich sa rotorov, ktoré sa nachádzajú medzi vstupným diskom (na obrázku označenom ako Entry disc) a reflektorom (Reflector). Enigma používa ako vstup klávesnicu (Keyboard), a ako výstup lampový panel (Lamp panel). Klávesnica má 26 kláves. Pri stlačení klávesy je vyslaný elektrický prúd z klávesnice cez súpravu šifrovacích zariadení. Signál najprv prejde cez prepojovací panel (plug board). Jedná sa o mechanizmus, ktorý definuje vzájomnú zámenu dvojíc písmen. Signál z panelu je poslaný na vstupný disk, ktorý pošle signál pravému rotoru (tento rotor identifikujeme číslom 4), ten pošle signál tretiemu atď., až k reflektoru, ktorý je na ľavej strane. Vo vnútri reflektoru je každý kontakt prepojený s ďalším kontaktom (spolu 13 párov kontaktov), ktorý efektívne vracia prúd naspäť do súpravy rotorov. Prúd prejde všetkými štyrmi rotormi (tentokrát opačným smerom), vstupným diskom a prepojovacím panelom až na svetelný panel, na ktorom sa rozsvieti jedna z 26 lámp.

Výhodou používania reflektora je reciprocita operácie. Inými slovami, celý proces sa dá obrátiť. Na rozšifrovanie správy musí byť dešifrovacie zariadenie nastavené presne tak, ako je šifrovacie zariadenie. Táto metóda však má jednu nevýhodu: žiaden symbol vstupnej abecedy nemôže byť zašifrovaný sám na seba.

Dizajn Fialky je veľmi podobný Enigme, avšak Fialka má množstvo doplnkov. V prvom rade prepojovací panel Enigmy bol nahradený čítačkou kariet, ktorá značne zjednodušovala nastavovaciu procedúru. Fialka používa 10 rotorov a pokročilý krokovací mechanizmus. Podobne ako v Enigme, aj vo Fialke je použitý reflektor na vrátenie prúdu späť do sady rotorov. Oproti Enigme je namiesto svetelného panelu použitá ako výstupné zariadenie tlačiareň. Ďalším vylepšením Fialky je možnosť identického zobrazenia – t.j. zašifrovania ľubovoľného symbolu vstupnej abecedy na seba samého.



Obr. 2. Blokový diagram Fialky M-125-xx (prevzaté z [1])

Klávesnica Fialky má 30 kláves. Stlačením klávesy sa vyšle elektrický prúd (signál) na čítačku kariet, ktorá sa správa presne tak, ako prepojovací panel na Enigme. Z čítačky kariet ide signál na vstupný disk, ktorý ho podá ďalej na súpravu rotorov. Na konci šifrovacieho zariadenia je signál vrátený späť do súpravy rotorov cez vstupný disk a čítačku kariet až na klávesnicu. Za klávesnicou sa nachádza matica diód, ktorá konvertuje výstupný znak šifrátora na kód o dĺžke 5 bitov. Tento kód je podobný 5 bitovému Baudotovmu kódu. 5 bitové údaje z tohto kódera sú použité na riadenie tlačiarne a dierovača. Klávesnica obsahuje okrem riadenia jedného z 30 spínačov aj 5 bitový mechanický kódovač, ktorý produkuje digitálny kód bežného textového originálu. Tento kód je používaný, keď je Fialka nastavená ako štandardný ďalekopis (v bežnom textovom móde). Avšak 5 bitový kód bežného textu môže byť použitý aj ako výstup šifrátora pri identickom zobrazení. Toto správanie je riadené špeciálnym kontaktom na reflektore. Keď sa tento konkrétny kontakt na reflektore zopne, signál sa neposiela späť na rotory, ale použije sa 5 bitový kód originálneho písmena. Pravdepodobnosť toho, že znak bude zakódovaný sám na seba, je 1:30.

Ďalšie 3 vodiče z reflektora definujú tzv. magický obvod (magic circuit). Jedná sa o vzájomné prepojenie trojice symbolov. Toto zapojenie čiastočne zbavuje Fialku reciprocity. Zvyšných 26 kontaktov na reflektore je podobne ako v Enigme spárovaných a jeden znak (trinásty) sa šifruje sám na seba. [4]

3.1 Jednotlivé vylepšenia Fialky oproti Enigmy

- Aby sa zvýšila odolnosť šifry voči útoku hrubou silou, rozsah priestoru kľúčov sa oproti Enigme zvýšil. Namiesto 4 rotorov používaných v Enigme Fialka ich používa 10. Počet možných počiatočných nastavení (t.j. rozsah priestoru kľúčov) pomocou týchto rotorov je $10! \times 30^{10}$. Faktoriál popisuje počet možných poradí rotorov a výraz 30^{10} reprezentuje 30 možných počiatočných natočení na každom rotore.

- Rotory na Enigme sa otáčajú pomaly a v jednom smere. V prípade Fialky sa priľahlé rotory otáčajú rýchlo a opačným smerom. Okrem toho otáčanie rotora závisí od prítomnosti blokovacieho pinu.

- Výstupom Enigmy je svetelný panel. Fialka používa tlačiareň a dierovač, čiže je menšia pravdepodobnosť výskytu chyby spôsobenej zlyhaním obsluhy.

- Aby Enigma nestratila reciprocitu, môžu byť na reflektore len cykly dĺžky dva (vzájomné prepojenie dvoch kontaktov). Nevýhodou tejto konštrukcie je to, že znak nemôže byť zašifrovaný sám na seba.

- V prípade Fialky je na reflektor pridaný jeden cyklus dĺžky 3, čo umožňuje symbolu, aby bol zašifrovaný sám na seba s pravdepodobnosťou 1/30. Avšak tento cyklus spôsobuje stratu reciprocity. Preto je nutné na dešifrovanie používať iný mód, ako na zašifrovanie.

Príklad [4] [1]:

Majme nasledujúce kontakty pre cyklus dĺžky tri: 1 – 2 – 3.

V šifrovacom móde môže byť prepojenie 1-2, 2-3, 3-1.

V prípade dešifrovanie je to prepojenie v opačnom smere, t.j. 2-1, 3-2, 1-3.

4 Fialka vs. Hagelin

Tento typ rotorového šifrátora sa prvýkrát objavil v roku 1925 vo Švédsku ako vynález Borisa Hagelina. Prvá verzia stroja sa označovala B-21. Do používania bola zavedená v tom istom roku, keď švédska armáda chcela nakúpiť šifrovacie stroje Enigma. Hagelin však ponúkol svoj stroj ako alternatívu a nakoniec sa švédska armáda priklonila k modelu B-21. Fyzicky sa B-21 podobala na Enigmu, ale fungovala inak a v tej dobe bola považovaná za bezpečnejšiu než Enigma. Podobne ako Enigma, obsahovala rotory. Pôvodne bol počet rotorov 2, ale Hagelin tento návrh vylepšil pridaním dvoch pinových rotorov ku každému šifrovaciemu rotoru. Šifrovacie rotory boli zafixované, nemohli sa meniť.

Obr. 3. Hagelin B-21(prevzaté z [5])

Podobne ako Enigma, fungovala na baterky a ako výstup používala svetelný panel. Z právnych dôvodov (Enigma bola už v tej dobe patentovaná) sa preto Hagelin rozhodol použiť úplne iný princíp šifrovania. Šifrovacie rotory nepoužil na substitúciu znaku, ale na poprehadzovanie matice 5x5 (t.j. transpozíciu). Počet prvkov matice obmedzil množinu použiteľných symbolov na 25 (písmená abecedy s vynechaným W). Ďalším rozdielom oproti Enigme bolo riadenie nepravidelného krokovania šifrovacích rotorov riadeného pinovými

rotormi. Podľa Hagelina táto technika znižovala predvídateľnosť výstupu. Tento jeho názor bol vyvrátený v roku 1931, keď bola šifra prelomená za necelých 24 hodín. [5]

Fialka používa striedavý krokovací mechanizmus. Nepravidelné otáčanie rotorov je zabezpečené blokovacími pinmi umiestnenými na rotoroch. Zdá sa, že práve tento prvok Fialky bol inšpirovaný Hagelinovým pinovým rotorom.

4.1 Jednotlivé vylepšenia Fialky oproti Hagelinu (B-21)

- Fialka používala 10 rotorov namiesto 2 šifrovacích (v prípade Hagelinu).

- Rotory na Hageline sa otáčajú nepravidelne v jednom smere a sú riadené pinovými rotormi. Vo Fialke sa otáčajú nepravidelne v dvoch smeroch a sú riadené blokovacími pinmi umiestnenými priamo na šifrovacích rotoroch.

- Výstupom Hagelinu je svetelný panel (v neskorších modeloch bol nahradený tlačiarňou). Filaka používala od začiatku tlačiareň a dierovač.

- Hagelin, podobne ako Enigma, nepodporuje zašifrovanie znaku na seba samého.

5 Fialka vs. Siemens T-52

Pravdepodobne najznámejším šifrovacím strojom firmy Siemens sa stal šifrátor T-52, označovaný aj ak „Geheimschreiber“. Tento šifrátor používalo velenie nemeckého vojska počas druhej svetovej vojny. Po vojne vyvinul Siemens ďalšie šifrovacie stroje odvodené od Vernamovej šifry [6].

Stroj T-52 patril v časoch 2. svetovej vojny medzi najsilnejšie. Šifrovacia procedúra bola odvodená od Vernamovej šifry. Každý vstupný znak bol prevedený do 5 bitovej reprezentácie. Toto 5 bitové slovo vstupovalo do binárnej operácie spolu s ďalším 5 bitovým slovom, ktoré bolo vygenerované. Generátor týchto pseudo-náhodných čísel bol založený na mechanickom princípe rotorov a pinov.

Na kódovanie vstupného znaku sa používal buď Baudotov kód alebo nejaká jeho odvodenina. Šifrátor T-52 obsahoval 10 rotorov. Každý z piatich bitov vstupného znaku bol podrobený funkcii XOR so súčtom troch výstupov z rotorov a následne boli príslušné bity vstupného znaku preklápané. Preklopenie záviselo od súčtu iných troch vývodov z rotorov. Trojice

pinov, ktoré riadili operáciu XOR alebo zmenu bitov, boli voliteľné pomocou prepínacieho panelu. Zdá sa, že inšpiráciu bitovej reprezentácie vstupu čerpali tvorcovia Fialky práve od firmy Siemens.

Obr. 4. Siemens T-52 (prevzaté z [6]).

Bolo vyvinutých viacero verzií šifrátora. T-52a sa od verzie T-52b líšila iba v tom, že neskoršia verzia potláčala elektrický šum. Nasledujúce verzie vylepšili šifrovaciu procedúru, predovšetkým riadenie otáčania rotorov [8].

Prvá verzia stroja bola rozlúštená Annou Beurlingovou za dva týždne v máji 1940 iba za pomoci pera a papiera. Z 500000 správ bolo približne 350000 rozlúštených. V roku 1942 bol šifrátor T-52 vylepšený, ale opätovne prelomený. Až jeho tretie vylepšenie v polovici roku 1943 bolo natoľko úspešné, že zamedzilo dešifrovaniu správ nelegitímnym príjemcom.

Ako sme už spomenuli, šifrátor T-52 pozostával z desiatich rotorov, označovaných písmenami abecedy od A. Jednotlivé rotory nemali rovnakú veľkosť. Výstup rotorov riadil ich posun v nasledujúcom kroku, a taktiež slúžil na generovanie prúdového kľúča, ktorým sa šifroval vstupný text. Krokovanie rotorov bolo zvolené tak, aby sa vždy posunulo aspoň 5 z celkového počtu 10 rotorov [7].

Simulátor tohto šifrovacieho stroja možno nájsť a vyskúšať na internetovej stránke http://cryptocellar.org/simula/t52/.

6 Porovnanie

V nasledujúcej tabuľke sa nachádza porovnanie a zhrnutie základných rozdielov medzi vyššie uvedenými šifrátormi:

Názov	**Enigma**	**Fialka**	**Hagelin**	**T-52**
Počet rotorov	3-4	10	2	10
Pomocné rotory	nie	nie	áno	nie
Otáčanie rotorov	pravidelné	nepravidelné, riadené bloko-vacími pinmi	nepravidelné, riadené pinový-mi rotormi	nepravidelné
Smer otáčania	1	2	1	1
Výstup	svetelný panel	tlačiareň, diero-vač	svetelný panel, tlačiareň	tlačiareň
Seba-zašifrovanie znaku	nie	áno	nie	---
Typ šifrovací operácie	substitúcia	substitúcia	transpozícia	XOR
Úspešné útoky	áno	nie	áno	áno

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] O. GROŠEK, M.VOJVODA, P. ZAJAC: Klasické šifry. STU Bratislava, 2007. ISBN 80-227-2653-5

[3] http://en.wikipedia.org/wiki/Rotor_machine

[4] E. ANTAL: Porovnanie rotorových šifrátorov Enigma a Fialka M-125, Bakalárska práca, FEI STU Bratislava 2009

[5] http://cryptomuseum.com/crypto/hagelin/b21/index.htm

[6] http://rijmenants.awardspace.com/en/focus.htm

[7] http://www.quadibloc.com/crypto/te0302.htm

[8] http://www.rutherfordjournal.org/article010106.html

D. Call for Papers Mikulášská kryptobesídka

1. – 2. prosinec 2011, Praha
http://mkb.buslab.org

Základní informace

Mikulášská kryptobesídka přichází letos již v 11. ročníku. 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 *1. prosince 2011* a (b) půldne prezentací příspěvků a diskusí v pátek *2. prosince 2011*. Pro workshop jsou domluveny zvané příspěvky:

- Chris Mitchell (Royal Holloway, UK): *New architectures for identity management - removing barriers to adoption*.
- Graham Steel (INRIA, Francie): *Attacking and Fixing PKCS#11 Security Tokens*.
- Viktor Fischer (Jean Monnet University Saint-Etienne, Francie): *Recent Advances in Random Numbers Generation for Cryptography*.
- Pavel Vondruška (Telefónica O2 Czech Republic): *Šifry používané československými osobnostmi*.
- Jozef Kollár (SvF STU v Bratislave, SR): *Československé šifry z obdobia 2. svetovej vojny*.

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 se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

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 PDF a to tak, aby na uvedenou adresu přišly nejpozději do *3. října 2011*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2011 – 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 *31. října*. Příspěvek pro sborník workshopu pak musí být dodán do *14. listopadu*.

Důležité termíny

Návrhy příspěvků:	3. října 2011
Oznámení o přijetí/odmítnutí:	31. října 2011
Příspěvky pro sborník:	14. listopadu 2011
Konání MKB 2010:	1. – 2. prosince 2011

Mediální partneři

Programový výbor

Dan Cvrček, Smart Architects, UK
Vlastimil Klíma, KNZ, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Tomáš Rosa, Raiffeisenbank a UK, ČR
Luděk Smolík, Siegen, SRN
Martin Stanek, UK, Bratislava, SR
Petr Švenda, FI MU, Brno, ČR

E. O čem jsme psali v květnu 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