Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 13, číslo 10/2011 **15. října**

10/2011

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1340 registrovaných odběratelů)

Obsah :

A. Československé šifry z obdobia 2. svetovej vojny Diel 9., Šifra „Růžena“

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.

9 Šifra „Růžena“

Šifra „Růžena“ je typu SP. Jedná sa o substitúciu a následné pričítanie periodického hesla. Popis tejto šifry je uvedený v knihe [2] (str. 128–129). Šifru „Růžena“ používala napríklad rádiostanica Růžena v operácii Bauxite. Odtiaľ pochádza aj jej pracovný názov. Je veľmi pravdepodobné, že oficiálne označenie tejto šifry bolo niektorým rímskym číslom, podobne ako tomu bolo pri iných ČS šifrách.

9.1 Všeobecný popis a príklad šifrovania depeší

Postup pri šifrovaní touto šifrou ukážeme na príklade textu:

> *Jestliže mně dáte šest řádků napsaných rukou toho nejčestnějšího muže, já v nich najdu něco za co ho budem moct pověsit.*
> *(Kardinál Richelieu)*[1]

Text určený na zašifrovanie sa najskôr previedol do číselnej podoby. Používala sa 49 znaková substitučná tabuľka. Avšak bližšie informácie o nej v [2] nie sú uvedené. Podľa uvedeného príkladu by to mohla byť rovnaká tabuľka ako pri šifre „Marta“, čiže tabuľka 1, uvedená na strane 3. Text najskôr prepíšeme pomocou znakov zo substitučnej tabuľky a špeciálne znaky, ktoré v nej nie sú obsiahnuté, vynecháme. Medzery za špeciálnymi znakmi sa vynechávajú, pretože slová sú oddelené buď medzerou, alebo špeciálnym znakom. V príklade dostaneme text:

[1] Uvedený text je voľný preklad francúzskej verzie: *Deux lignes de la main d'un homme suffisent à faire condamner le plus innocent.*

	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	0	1	2	3	4	5	6	7	8	9

Tabuľka 1: Česká 49 znaková abeceda pre šifry „Marta/Růžena“

```
JESTLIŽE MNĚ DATE ŠEST ŘADKU NAPSANYCH RUKOU TOHO
NEJČESTNEJŠIHO MUŽE,JA V NICH NAJDU NĚCO ZA CO
HO BUDEM MOCT POVĚSIT.
```

O delení textu na kratšie časti sa v [2] explicitene nič nepíše, ale pri danom spôsobe šifrovania, môže tabuľka obsahovať nanajvýš n^2 cifier, kde n je počet znakov hesla. Dlhšie texty sa preto zrejme rozdeľovali. Budeme predpokladať, že v sérii sa jednotlivé časti označovali znakmi určujúcimi nadväznosť podobne ako sa to robilo aj pri väčšine iných šifier. Náš text má, po úprave, aj s medzerami 119 znakov, takže ho rozdelíme na dve časti:

```
JESTLIŽE MNĚ DATE ŠEST ŘADKU NAPSANYCH
RUKOU TOHO NEJČESTNEJŠIHO/A

A/MUŽE,JA V NICH NAJDU NĚCO
ZA CO HO BUDEM MOCT POVĚSIT.
```

Tieto dve časti prevedieme do číselnej podoby podľa substitučnej tabuľky 1, pričom medzery sa nahrádzajú znakmi `5, 6, 7, 8` alebo `9`:

```
13062 32515 12320 65161 70760 50125 06724 06232 58220 10514
26917 01192 30117 30115 21261 41826 62518 10187 17061 30406
23251 70613 24121 01837 01
------------------------------------------------------------
01371 62632 06351 30152 76171 21171 70113 05268 17070 31893
10150 31861 01870 22605 06168 16180 32591 91827 07231 22533
```

Na začiatok prvej depeše sa ako adresovacie znaky pridával deň šifrovania, oddelený od textu bodkou. Číslice dňa sa nekódovali, ale písali sa priamo. Bodka sa podľa substitučnej tabuľky nahradila číslom 33. Ak budeme text šifrovať 23. apríla 1945, tak na začiatok textu pridáme `2333`. Pokiaľ počet

cifier depeše nie je násobkom 5, tak na konci ho náhodne doplníme ciframi 5, 6, 7, 8 alebo 9. V [2] sa uvádza, že sa text dopĺňal nulami a v číselnej podobe depeše sú skutočne doplnené cifry 0, ale to sa zrejme len jedná o svojské pochopenie pojmu „nula“, ktorý má v kryptografii trochu odlišný význam než v matematike. Takže v príklade druhá časť zostane nezmenená a prvú časť doplníme. Dostávame:

```
23331 30623 25151 23206 51617 07605 01250 67240 62325 82201
05142 69170 11923 01173 01152 12614 18266 25181 01871 70613
04062 32517 06132 41210 18370 15968
------------------------------------------------------------
01371 62632 06351 30152 76171 21171 70113 05268 17070 31893
10150 31861 01870 22605 06168 16180 32591 91827 07231 22533
```

Až teraz prichádza na rad heslo, ktoré sa používa na tvorbu dvoch ďalších hesiel, z ktorých prvé určuje umiestnenie začiatku hesla vrámci riadku tabuľky a druhé heslo je samotným kľúčom, ktorý sa pričitáva ku textu depeše. Toto heslo sa podľa [2] tvorilo na základe dátumu šifrovania. Za jeho textovú podobu sa bralo označenie dňa v týždni a cifry označujúce deň v dátume šifrovania a to všetko v nemčine. V príklade šifrujeme depešu 23. apríla 1945, čo bol pondelok. Potom heslo bude *Montag zwei drei* a jeho vyčíslenie bude:

M	O	N	T	A	G	Z	W	E	I	D	R	E	I
8	10	9	12	1	5	14	13	3	6	2	11	4	7

Dĺžka hesla určuje šírku tabuľky. V príklade bude mať preto tabuľka 14 stĺpcov. Teraz ešte z vyčísleného hesla zostrojíme tzv. „druhé heslo“. Toto bude rovnako dlhé ako to prvé, ale v dvojciferných číslach vynecháme desiatkové cifry. Takže v príklade druhé heslo bude:

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

Pôvodne vyčíslené heslo („prvé heslo“) sa používa na očíslovanie stĺpcov tabuľky a bude určovať začiatky druhého hesla v jednotlivých riadkoch tabuľky. Z neho zostrojené „druhé heslo“ sa používa ako kľúč, ktorý sa pričitáva ku textu depeše. Text v číselnej podobe, doplnený už aj o služobné skupiny a nuly, zapisujeme po riadkoch do tabuľky. Cifry budeme zapisovať zľava doprava a zhora nadol. Potom riadky tabuľky očíslujeme, ale budeme ich číslovať zdola nahor. Ďalej pod cifry v každom riadku tabuľky napíšeme cifry kľúča („druhého hesla“). V prvom riadku (dolný riadok tabuľky) začneme písať cifry kľúča od stĺpca s číslom 1 a pokračujeme cyklicky v celom riadku. V druhom riadku začneme písať cifry kľúča od stĺpca s číslom 2 atď.

Následne sčítame cifry textu s ciframi kľúča modulo 10. V príklade dostávame pre prvú depešu tabuľku 2 na strane 6 a pre druhú depešu tabuľku 3 na strane 7.

V tabuľkách si všimnime prvé riadky (dolné riadky tabuliek). Tie sú neúplné. Pán Hanák vo svojom príklade píše kľúč cyklicky, ale len vrámci políčok zaplnených ciframi textu. Ako by sa to asi robilo, ak by text v najspodnejšom riadku tabuľky nesiahal až po stĺpec s poradovým číslom 1, tak ako to je aj v príklade? Ako by sa potom zapisoval kľúč pod cifry textu? Určite by sa dal vymyslieť aj nejaký spôsob zápisu kľúča, ktorý by bol aplikovateľný v podobných situáciach, ale v [2] sa nič také neuvádza. Preto v príklade používame logickejšiu možnosť, a síce to, že kľúč sa zapisuje cyklicky do celého riadku, bez ohľadu na to, ako dlhý je text.

Nakoniec už len zostáva z tabuliek vypísať cifry súčtov a napísať ich v päťmiestnych skupinách:

```
91323 45056 87295 91298 66040 69785 93304 90861 09317 97634
67289 44503 73060 81094 63299 92535 62595 46624 37085 48656
30276 00509 11286 74831 55179 37005
----------------------------------------------------------
81292 16968 27721 22206 09792 68925 03734 42067 38691 78692
31693 60076 44132 36385 49420 20860 24642 45153 28609 21754
```

Ďalej musíme do depeší doplniť služobné údaje. Tieto, podľa informácií z [2], obsahovali dátum šifrovania a číslo depeše. Pokiaľ ide o číslovanie depeší, tak pán Hanák uvádza, že obyčajné depeše sa číslovali od 01 po 69 a zvláštne depeše (overovacie, zabezpečovacie) sa číslovali od 70 po 99. Okrem toho spomína, že časti série sa číslovali od 50 po 99. Nie je z toho zrejmé ako to bolo myslené, a preto informáciu o číslovaní častí série budeme ignorovať a depeše, vrátane častí série, budeme číslovať vzostupne. Služobné údaje boli kódované do dvoch päťmiestnych skupín. Prvá skupina bola na začiatku depeše a poradie druhej skupiny zodpovedalo jednotkám dňa šifrovania. Tieto dve skupiny sa údajne maskovali vzájomným sčítaním – zrejme je myslené sčítanie modulo 10. Tu sa pán Hanák pravdepodobne opäť mýli. Ak by sme skutočne tieto skupiny vzájomne sčítali modulo 10, tak by sme ich nemohli jednoznačne spätne dekódovať. Maskovať sčítaním modulo 10 môžme preto len jednu z dvoch služobných skupín. My budeme maskovať druhú služobnú skupinu, pretože prvá bude obsahovať dátum šifrovania a ten potrebujeme na dešifrovanie a aj na určenie umiestnenia druhej skupiny. V skutočnosti sa to zrejme robilo nejakým rafinovanejším spôsobom, pretože tu uvedený postup je príliš priehľadný. Prvá skupina služobných údajov zostane v otvorenom tvare a zároveň sa pričíta modulo 10 ku druhej skupine. Kedže v príklade šifrujeme depeše 23. deň v mesiaci, služobné skupiny budú prvá

	Čísla stĺpcov													
	8	10	9	12	1	5	14	13	3	6	2	11	4	7
10. riadok	2	3	3	3	1	3	0	6	2	3	2	5	1	5
Kľúč	7	8	0	9	2	1	5	4	3	3	6	2	1	4
Súčet	**9**	**1**	**3**	**2**	**3**	**4**	**5**	**0**	**5**	**6**	**8**	**7**	**2**	**9**
9. riadok	1	2	3	2	0	6	5	1	6	1	7	0	7	6
Kľúč	4	7	8	0	9	2	1	5	4	3	3	6	2	1
Súčet	**5**	**9**	**1**	**2**	**9**	**8**	**6**	**6**	**0**	**4**	**0**	**6**	**9**	**7**
8. riadok	0	5	0	1	2	5	0	6	7	2	4	0	6	2
Kľúč	8	0	9	2	1	5	4	3	3	6	2	1	4	7
Súčet	**8**	**5**	**9**	**3**	**3**	**0**	**4**	**9**	**0**	**8**	**6**	**1**	**0**	**9**
7. riadok	3	2	5	8	2	2	0	1	0	5	1	4	2	6
Kľúč	0	9	2	1	5	4	3	3	6	2	1	4	7	8
Súčet	**3**	**1**	**7**	**9**	**7**	**6**	**3**	**4**	**6**	**7**	**2**	**8**	**9**	**4**
6. riadok	9	1	7	0	1	1	9	2	3	0	1	1	7	3
Kľúč	5	4	3	3	6	2	1	4	7	8	0	9	2	1
Súčet	**4**	**5**	**0**	**3**	**7**	**3**	**0**	**6**	**0**	**8**	**1**	**0**	**9**	**4**
5. riadok	0	1	1	5	2	1	2	6	1	4	1	8	2	6
Kľúč	6	2	1	4	7	8	0	9	2	1	5	4	3	3
Súčet	**6**	**3**	**2**	**9**	**9**	**9**	**2**	**5**	**3**	**5**	**6**	**2**	**5**	**9**
4. riadok	6	2	5	1	8	1	0	1	8	7	1	7	0	6
Kľúč	9	2	1	5	4	3	3	6	2	1	4	7	8	0
Súčet	**5**	**4**	**6**	**6**	**2**	**4**	**3**	**7**	**0**	**8**	**5**	**4**	**8**	**6**
3. riadok	1	3	0	4	0	6	2	3	2	5	1	7	0	6
Kľúč	4	3	3	6	2	1	4	7	8	0	9	2	1	5
Súčet	**5**	**6**	**3**	**0**	**2**	**7**	**6**	**0**	**0**	**5**	**0**	**9**	**1**	**1**
2. riadok	1	3	2	4	1	2	1	0	1	8	3	7	0	1
Kľúč	1	5	4	3	3	6	2	1	4	7	8	0	9	2
Súčet	**2**	**8**	**6**	**7**	**4**	**8**	**3**	**1**	**5**	**5**	**1**	**7**	**9**	**3**
1. riadok	5	9	6	8										
Kľúč	2	1	4	7	8	0	9	2	1	5	4	3	3	6
Súčet	**7**	**0**	**0**	**5**										

Tabuľka 2: Šifrovacia tabuľka 1. depeše

	Čísla stĺpcov													
	8	10	9	12	1	5	14	13	3	6	2	11	4	7
8. riadok	0	1	3	7	1	6	2	6	3	2	0	6	3	5
Kľúč	8	0	9	2	1	5	4	3	3	6	2	1	4	7
Súčet	**8**	**1**	**2**	**9**	**2**	**1**	**6**	**9**	**6**	**8**	**2**	**7**	**7**	**2**
7. riadok	1	3	0	1	5	2	7	6	1	7	1	2	1	1
Kľúč	0	9	2	1	5	4	3	3	6	2	1	4	7	8
Súčet	**1**	**2**	**2**	**2**	**0**	**6**	**0**	**9**	**7**	**9**	**2**	**6**	**8**	**9**
6. riadok	7	1	7	0	1	1	3	0	5	2	6	8	1	7
Kľúč	5	4	3	3	6	2	1	4	7	8	0	9	2	1
Súčet	**2**	**5**	**0**	**3**	**7**	**3**	**4**	**4**	**2**	**0**	**6**	**7**	**3**	**8**
5. riadok	0	7	0	3	1	8	9	3	1	0	1	5	0	3
Kľúč	6	2	1	4	7	8	0	9	2	1	5	4	3	3
Súčet	**6**	**9**	**1**	**7**	**8**	**6**	**9**	**2**	**3**	**1**	**6**	**9**	**3**	**6**
4. riadok	1	8	6	1	0	1	8	7	0	2	2	6	0	5
Kľúč	9	2	1	5	4	3	3	6	2	1	4	7	8	0
Súčet	**0**	**0**	**7**	**6**	**4**	**4**	**1**	**3**	**2**	**3**	**6**	**3**	**8**	**5**
3. riadok	0	6	1	6	8	1	6	1	8	0	3	2	5	9
Kľúč	4	3	3	6	2	1	4	7	8	0	9	2	1	5
Súčet	**4**	**9**	**4**	**2**	**0**	**2**	**0**	**8**	**6**	**0**	**2**	**4**	**6**	**4**
2. riadok	1	9	1	8	2	7	0	7	2	3	1	2	2	5
Kľúč	1	5	4	3	3	6	2	1	4	7	8	0	9	2
Súčet	**2**	**4**	**5**	**1**	**5**	**3**	**2**	**8**	**6**	**0**	**9**	**2**	**1**	**7**
1. riadok	3	3												
Kľúč	2	1	4	7	8	0	9	2	1	5	4	3	3	6
Súčet	**5**	**4**												

Tabuľka 3: Šifrovacia tabuľka 2. depeše

a tretia skupina depeše. Nech prvá depeša má poradové číslo 03. Potom druhá bude mať poradové číslo 04. Nezamaskované služobné skupiny depeší potom budú `23047 03297` a `23042 04167`. Dátum šifrovania je 23. apríla a je to zakódované prvými štyrmi ciframi prvej skupiny. Piata cifra tejto skupiny je doplnená náhodne. Prvé dve cifry druhej skupiny sú poradové číslo depeše a ďalšie tri cifry sú doplnené náhodne. Ak teraz zamaskujeme druhé skupiny, tak dostávame: `23047 26234` a `23042 27109`. Po doplnení služobných údajov do depeší dostávame:

```
23047 91323 26234 45056 87295 91298 66040 69785 93304 90861
09317 97634 67289 44503 73060 81094 63299 92535 62595 46624
37085 48656 30276 00509 11286 74831 55179 37005
------------------------------------------------------------
23042 81292 27109 16968 27721 22206 09792 68925 03734 42067
38691 78692 31693 60076 44132 36385 49420 20860 24642 45153
28609 21754
```

Depeše sa zrejme vysielali bez návestia, pretože dátum šifrovania bol skrytý v služobných údajoch. Preto sa zrejme na začiatok depeše pre kontrolu úplnosti pridávala len informácia o počte jej skupín (dĺžke).V príklade dostávame depeše:

```
28 GR
23047 91323 26234 45056 87295 91298 66040 69785 93304 90861
09317 97634 67289 44503 73060 81094 63299 92535 62595 46624
37085 48656 30276 00509 11286 74831 55179 37005
------------------------------------------------------------
22 GR
23042 81292 27109 16968 27721 22206 09792 68925 03734 42067
38691 78692 31693 60076 44132 36385 49420 20860 24642 45153
28609 21754
```

ktoré sú týmto pripravené na odoslanie.

9.2 Postup pri šifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii text na šifrovanie.

b. Je daný dátum šifrovania. Na základe dátumu sa tvoria heslá.

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

Potom šifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Pri šifrovaní sa používajú dve heslá – tzv. „prvé heslo“ a „druhé heslo“. Prvé heslo sa tvorí na základe dátumu šifrovania a druhé heslo sa tvorí z prvého. Ako heslo v textovej podobe zoberieme označenie dňa v týždni a cifry označujúce deň v dátume šifrovania a to všetko v nemčine.

2. Textové heslo vyčíslime obvyklým spôsobom podľa substitučnej abecedy. Heslo je síce v nemčine, ale substitučná tabuľka obsahuje aj písmeno `CH`, na čo si treba dať pozor! Takto dostaneme prvé heslo. Druhé heslo dostaneme z prvého tak, že v jeho vyčíslenej podobe z dvojciferných čísel vynecháme desiatkové cifry.

3. 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. Pri tejto šifre používame tú istú substitučnú tabuľku ako pri šifre „Marta“.

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

5. Tabuľka, do ktorej budeme text zapisovať, má n^2 políčok, kde n je počet písmen hesla. Text rozdelíme na časti tak, aby tieto aj so znakmi označujúcimi nadväznosť častí a adresovacími znakmi na začiatku textu (4 cifry – uvádza sa ďalej), mali nanajvýš n^2 cifier.

6. 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, znak `/` a na konci textu znak `/` a písmeno identické s písmenom označujúcim nasledovnú časť textu. Písmená na označovanie častí berieme podľa abecedy. Prvá časť má označenie len na konci a posledná časť len na začiatku.

7. Podľa tabuľky 1 nahradíme znaky depeše dvojciferným číslami. Medzery medzi slovami nahrádzame jednociferným číslami `5, 6, 7, 8` alebo `9`.

8. Na začiatok prvej časti depeše sa ako adresovacie znaky dávalo číslo označujúce deň šifrovania, oddelené od textu bodkou. Číslo označujúce

deň sa nekódovalo, ale písalo sa priamo. Bodka sa nahradila ciframi `33` podľa substitučnej tabuľky.

9. Ak počet cifier depeše nie je násobkom 5, tak na jej koniec náhodným spôsobom doplníme potrebný počet cifier `5, 6, 7, 8` alebo `9`.

10. Depešu zapíšeme po riadkoch do tabuľky s n stĺpcami a nanajvýš n riadkami, kde n je dĺžka hesla. Stĺpce tabuľky sú očíslované prvým heslom. Cifry depeše zapisujeme zľava doprava a zhora nadol. Vyplnené riadky tabuľky potom očíslujeme, ale číslujeme ich zdola nahor. Čiže poradové číslo 1 má najspodnejší vyplnený riadok tabuľky.

11. Pod jednotlivé riadky tabuľky zapisujeme cyklicky druhé heslo. Postupujeme tak, že heslo v i-tom riadku tabuľky začíname písať v stĺpci, ktorého poradové číslo je i a postupujeme cyklicky smerom doprava.

12. V riadkoch tabuľky sčítame cifry depeše s ciframi kľúča modulo 10. Potom výsledok tohto súčtu vypíšeme z tabulky po riadkoch, zľava doprava, zhora nadol a cifry zapisujeme v päťmiestnych skupinách.

13. Zostrojíme dve päťmiestne skupiny služobných údajov. Tieto budú obsahovať dátum šifrovania a číslo depeše. **Nevieme nič o tom ako sa v skutočnosti tieto služobné údaje kódovali, takže popisovaný postup je vymyslený pre potreby príkladu.** Dátum šifrovania a číslo depeše zapíšeme v tvare `ddmmx ccxxx`, kde `dd` a `mm` označujú deň a mesiac šifrovania, `cc` je číslo depeše a `x` označuje ľubovoľnú cifru. Obyčajné depeše sa číslovali od 01 po 69. Zvláštne depeše sa číslovali od 70 po 99. Cifry prvej skupiny z `ddmmx ccxxx` pričítame ku cifrám druhej skupiny modulo 10 a samotná prvá skupina zostane tak ako je. Prvá skupina sa umiestňuje na začiatok depeše a umiestnenie druhej skupiny zodpovedá jednotkám z dňa šifrovania.

14. Na začiatok depeše pridáme ešte návestie v tvare `xx GR`, kde `xx` je počet päťmiestnych skupín depeše. Týmto je šifrovanie depeše ukončené a depeša je pripravená na odoslanie.

9.3 Postup pri dešifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii kompletný text zašifrovanej depeše.

Potom dešifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Na základe návestia overíme kompletnosť depeše (počet cifier) a vynecháme návestie depeše, ktoré už nebudeme potrebovať.

2. Prvé štyri cifry prvej skupiny sú dátumom šifrovania. Z neho určíme umiestnenie druhej služobnej skupiny. Jej poradie zodpovedá jednotkám dňa šifrovania. Prvú služobnú skupinu odčítame od druhej modulo 10 a z druhej služobnej skupiny potom určíme poradové číslo depeše. Potom obe služobné skupiny vynecháme, pretože ich už nebudeme potrebovať.

3. Podľa dátumu šifrovania zostrojíme „prvé heslo“ a „druhé heslo“. Ako heslo v textovej podobe zoberieme označenie dňa v týždni a cifry označujúce deň v dátume šifrovania a to všetko v nemčine.

4. Textové heslo vyčíslime obvyklým spôsobom podľa abecedy zo substitučnej tabuľky 1. Heslo je síce v nemčine, ale substitučná tabuľka obsahuje aj písmeno `CH`, na čo si treba dať pozor! Takto dostaneme prvé heslo.

5. Druhé heslo dostaneme z prvého tak, že v jeho vyčíslenej podobe z dvojciferných čísel vynecháme desiatkové cifry.

6. Cifry depeše zapíšeme do tabuľky s n stĺpcami, kde n je dĺžka hesla. Stĺpce tabuľky sú očíslované prvým heslom. Cifry depeše zapisujeme po riadkoch zľava doprava a zhora nadol. Vyplnené riadky tabuľky potom očíslujeme, ale číslujeme ich zdola nahor. Čiže poradové číslo 1 má najspodnejší vyplnený riadok tabuľky.

7. Pod jednotlivé riadky tabuľky zapisujeme cyklicky druhé heslo. Postupujeme tak, že heslo v i-tom riadku tabuľky začíname písať v stĺpci, ktorého poradové číslo je i a postupujeme cyklicky smerom doprava.

8. V riadkoch tabuľky odčítame od cifier depeše cifry kľúča modulo 10. Výsledok rozdielu vypíšeme z tabuľky po riadkoch, zľava doprava, zhora nadol. Tým dostaneme text depeše v číselnom tvare.

9. Na začiatku prvej časti depeše sú adresovacie znaky, pozostávajúce z dňa šifrovania a bodky. Číslo označujúce deň šifrovania je v otvorenom tvare a bodka je kódovaná ako `33`. Deň šifrovania poznáme, takže prvú časť a adresovacie znaky nájdeme ľahko a môžme ich po kontrole vynechať.

10. Podľa tabuľky 1 nahradíme čísla znakmi. Tie sú kódované dvojciferným číslami. Pokiaľ by na mieste desiatok bola cifra `5, 6, 7, 8` alebo `9`,

jedná sa o medzeru a tá je kódovaná jednociferne. Potom ešte doplníme medzery za špeciálne znaky v texte a dostávame pôvodný text depeše.

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

9.4 Lúštenie

Pri tejto šifre síce pričitávame k textu depeše heslo, ale nie periodicky. Heslo je v jednotlivých riadkoch tabuľky cyklicky posunuté. Nemôžme preto mechanicky použiť Kasiského metódu na zistenie dĺžky periódy a hesla. Avšak v prípade série nám v zodpovedajúcich si riadkoch jednotlivých častí, vznikajú úseky šifrované rovnakým periodickým heslom. V prípade ak máme sériu s veľkým počtom častí, čo nebola žiadna zvláštnosť, tak môžme celú časť brať ako jedno opakovanie hesla, čiže uvažovali by sme heslo dĺžky n^2. Na dostatočne dlhé série by potom bola aplikovateľná aj Kasiského metóda. Lúštenie tejto šifry je pracnejšie než lúštenie iných šifier typu SP, ale je stále realizovateľné. Prípadne sa dajú využiť ďalšie postranné informácie, ktoré boli lúštiteľom k dispozícii, keďže spravodajci z Londýna mali dobrý zvyk oznamovať popis nových šifier rádiom v depešiach zašifrovaných starými šiframi.

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. Podzimní Soutěž v luštění 2011 zahájena

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

Vážení čtenáři, **23. 10. 2010** bude zahájena tradiční **podzimní soutěž v luštění (jednoduchých) šifrových textů o ceny – *Soutěž v luštění 2011***. Pro nově registrované čtenáře uvádím, že obdobné soutěže pořádal náš e-zin již od roku 2000 a doporučuji se s minulými příklady a jejich řešením seznámit (http://crypto-world.info/souteze.php).

PRAVIDLA

Soutěž začne zveřejněním prvních úloh 23.10.2011 a skončí v listopadu 2011 (přesný den bude uveden dodatečně). Zúčastnit soutěže se může pouze odběratel e-zinu Crypto-World.

Vstup na stránku soutěže bude přes domovskou stránku Crypto-Worldu - ikona **Soutěže** nebo přímým voláním soutěžní stránky (http://soutez2011.crypto-world/).

Při registraci musí řešitel zadat kód soutěže 2011, který mu byl zaslán společně s výzvou k soutěži (při rozeslání informací ke stažení tohoto čísla e-zinu). Kód soutěže 2011 bude zaslán i všem nově registrovaným odběratelům e-zinu Crypto-World, kteří se během soutěže k jeho odběru přihlásí.

Soutěžící při registraci zadá své uživatelské jméno (login) a autentizační heslo pro opětovné přihlášení a dále e-mail, na který mu je zasílán e-zin Crypto-World. Tento e-mail se dále na stránce nezobrazuje a je pro ostatní návštěvníky soutěže nedostupný. Slouží k odesílání pokynů a informací soutěžícím a k ověření, že uživatel je registrovaným odběratelem e-zinu.

Soutěžní úlohy budou i letos zpřístupněny v nepravidelných etapách.

K některým úlohám budou zveřejněny dodatečné nápovědy, které umožní jejich vyluštění resp. jejich dešifraci. Nápovědy budou zveřejňovány v sekci Crypto-NEWS: http://crypto-world.info/news/index.php?sekce=c .

Za vyřešení úlohy se připisují soutěžícímu body. Registrovaný řešitel zadává své odpovědi přes www rozhraní (vždy velkými písmeny)!

Zadává se "klíčové" slovo z vyluštěného textu, pomoc s výběrem klíčového slova bude uvedena v nápovědi, která bude zveřejněna v Crypto-NEWS. Odpověď bude automaticky vyhodnocena a řešitel se ihned dozví, zda odpověděl správně nebo ne.

Příklad vyhledání a zadání klíčového slova z úlohy:
Řešitel vyluští zadanou úlohu a získá např. tento otevřený text:

KDE ZACNOU PALIT KNIHY TAM NAKONEC BUDOU LIDI UPALOVAT XX
(Kde začnou pálit knihy, tam nakonec budou lidi upalovat.)

Klíčovým slovem, kterým řešitel prokáže, že úlohu vyřešil je jedno ze slov otevřeného textu. Aby luštitel nemusel zkoušet všechna slova, slouží k jeho určení vždy nějaká jednoduchá nápověda.
Pokud bude v nápovědě např. uvedeno *CO ?* je klíčové slovo odpověď na tuto otázku dle kontextu úlohy. V tomto případě slovo KNIHY.
Pokud bude uvedeno *(4)* je klíčové slovo KNIHY, neboť je čtvrtým slovem získaného textu.
Pokud bude v nápovědě uvedeno *K2*, je klíčové slovo druhým slovem textu, které začíná na písmeno K. Klíčovým slovem je tedy opět slovo KNIHY atd.

Na stránce soutěže bude zveřejňován aktuální průběh soutěže. U každého řešitele bude v celkovém žebříčku uveden počet jeho dosažených bodů a lze se také podívat i na pořadí úloh, ve kterém je soutěžící vyřešil.

O pořadí soutěžících rozhoduje celkový počet dosažených bodů, v případě rovnosti bodů je rozhodující, kdo dosáhl tohoto počtu bodů dříve!

V případě, že soutěžící ještě nezískali žádné body, jsou uvedeni podle pořadí registrace.

Ceny a loga sponzorů

1.cena

Pro vítěze celé soutěže je i letos připravena tradiční hlavní cena - bezplatná účast na mezinárodním **kryptologickém workshopu Mikulášská kryptobesídka** http://mkb.buslab.org/ , který se koná 1.- 2.prosince v Praze. Pořadatelé 11.ročníku Trusted Network Solutions (http://www.kernun.cz/) a BUSLab (http://www.buslab.org/) hradí za vítěze registrační poplatek a srdečně zvou vítěze na tuto velmi zajímavou akci.

Další odměnou pro vítěze je pak ještě **rok web hostingu zdarma** (multihost/ftp/web), který věnuje firma HEXAGEEK http://www.hexageek.com/ .

2.cena

Rok hostingu zdarma (multihost/ftp/web) a dále **registrace domény zdarma** (dle výběru CZ nebo SK). Věnuje firma HEXAGEEK http://www.hexageek.com/ .

HEXAGEEK

3.cena

Rok hostingu zdarma (multihost/ftp/web) a **dále registrace domény zdarma** (dle výběru CZ nebo SK). Věnuje firma HEXAGEEK http://www.hexageek.com/ .

Ceny pro 3 náhodně vylosované úspěšné řešitele

(losuje ze všech řešitelů, kteří splní limit 15ti bodů)

1.vylosovaný: kniha P.Vondruška: Kryptologie, šifrování a tajná písma , edice OKO, nakladatelství Albatros, 2006, věnuje autor http://crypto-world.info/oko/index.php .

2.vylosovaný: registrace domény zdarma (dle výběru CZ nebo SK), věnuje firma HEXAGEEK http://www.hexageek.com/ .

3.vylosovaný: registrace domény zdarma (dle výběru CZ nebo SK), věnuje firma HEXAGEEK http://www.hexageek.com/ .

HEXAGEEK

Soutěžícím již teď přeji pěknou zábavu a úspěšné vyřešení všech úloh!

C. Crypto-Wars I.

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

Vždy, když Dr. Peter Hayek nastoupil do časoprostorového výtahu a vložil do otvoru svoji kartu s nahranou stáží, se cítil velmi vzrušeně. I po dvaceti letech služby si stále nemohl zvyknout na to, že je vyslán do minulosti, aby zachránil svět. Přesněji, aby zachránil stabilitu světa a nedošlo ke změně, která by měla za následek zničení Ultima Paradise. Tedy světa, který byl vybudován jako stabilní svět v roce 9011 po narození Krista.

Pamatuje si stále velmi živě na svoji prvou cestu před dvaceti jedna lety, kdy nastoupil do výtahu ve společnosti toho „potrhlého matematika“, který jej vyhledal a nabídl mu velmi zajímavou práci, kde prý bude moci využít své schopnosti luštit klasické šifry. Matematik za ním přišel dva dny po té, co vyhrál prestižní světovou soutěž v luštění, aby mu nabídl zajímavou práci. Povečeřeli spolu a pak se od něj dozvěděl velké tajemství o cestování časem a o společenských fluktuacích v časoprostoru. Nejdříve přisuzoval jeho vyprávění jisté potrhlosti v jeho chování, které se projevovalo ve velké roztržitosti a neustálé roztěkanosti a velmi, velmi podivnému chování, kdy neustále sledoval okolí a před každou jednoduchou aktivitou přemýšlel, jakoby to pro něj bylo něco nového. Dále pak jeho vyprávění připisoval chutnému těžkému portskému vínu. V závěru večera, pravděpodobně pod vlivem toho, že v posledních měsících, kdy se mu vůbec nedařilo a stíhala jej jedna osudová rána za druhou (po smrti rodičů jej opustila jeho dívka) se rozhodl, že s ním zajde do hotelu, kde mu slíbil matematik předat přihlášku do nové práce.

V hotelu Alcron prošli společně kolem recepce, vstoupili do běžného výtahu a když se dveře zavřely, vytáhl jeho podivný průvodce nějaký balíček, který připevnil na stěnu výtahu a pak vyndal ze své náprsní kapsy kartu a přiložil ji k balíčku. Proboha snad to není bomba! Jenže výbuch nenastal, ale stalo se něco jiného. Vnitřek výtahu se jako mávnutím kouzelného proutku změnil a najednou se octli v prostoru, který výtah připomínal, ale byl jiný než ten, do kterého vstoupili. Změnil se materiál, vše bylo z nějakého zvláštního plastu. Původní panel s tlačítky zmizel a místo něj se objevil displej velikosti asi 10x10 cm, ve kterém bylo číslo 2011 a pod ním další dlouhá řada čísel. Jeho průvodce se k němu obrátil a řekl: „Milý Petře, vím, že budeš s novou prací souhlasit, a proto tě odvezu přímo do naší centrály, která leží daleko v budoucnosti a je uzavřena ve speciálním časoprostorovém vaku.“ Pak vyndal z kapsy jinou čipovou kartu a přiložil ji k displeji. Na displeji se začala rychle měnit čísla 2011 / 2012 / 2013/ ..... Čísla v druhém řádku se měnila tak rychle, že prakticky tvořila jen světelnou čárku. Po několika málo minutách se „výtah“ zastavil a najednou se objevily dveře.

Oba z výtahu vystoupili a ocitli se v místnosti se skleněnou kopulí a se spoustou zelených velkých rostlin. Vnímal, že se kolem pohybují lidé, kteří jsou oblečeni do šatů ze zvláštní přiléhavé, lesklé látky. Zmateně se kolem sebe rozhlížel a hledal vysvětlení toho, co se to vlastně stalo? Přece nebude věřit těm povídačkám svého podnapilého průvodce, že se ocitli v daleké budoucnosti!

Ale bylo to tak. Petr se dostal do výcvikového střediska SGW (ochránců světa). Trvalo to asi 3 měsíce, než se částečně vyrovnal s tím, co se stalo a než pochopil a vstřebal základní informace. Petr měl možnost se ptát a ptát a na své dotazy dostával odpovědi. Byl ve výcviku a bylo potřeba, aby byl připraven. Základní důraz výcviku byl kladen právě na to, aby nový adept na strážce pochopil, kdo je, co je jeho úkolem, proč vzniklo toto výcvikové středisko, proč instituce Strážců světa vznikla, proč byl vybrán, co bude dělat, proč to nejde dělat jinak, paradoxy času a prostoru.

Petr si postupně sestavoval mozaiku informací, která mu měla pomoci vše pochopit. Zpočátku si při své pečlivosti a také ze strachu, zda nešílí nebo již nezešílel, řadu věcí psal, aby se k nim mohl vracet a hledal v tom, zda to má nějaký smysl.

Ze všech poznámek se mu postupně vyklubal tento nový pohled na svět:
Cestování časem a časoprostorem je možné. Vše se děje najednou. Tak jako chodíme dveřmi z místnosti do místnosti, tak můžeme vstupovat z jednoho bodu v čase a prostoru do jiného. Omezení je dáno pouze energií. Zatímco cestování časem ve stejném bodě prostoru je energeticky zvládnutelné, tak cestování v prostoru ve stejném čase je energeticky náročné. Lidé se mění, ale povahově jsou to pořád zvířata. Pro své ego, moc a majetek jsou ochotni udělat cokoliv a to i tehdy, když tím poruší obecný princip morálky. Jak běžela staletí a tisíciletí (pardon jak běží vedle sebe), tak se stalo, že v jednom bodě časoprostoru přišli na způsob, jak ovládnout pohyb v čase. To však mělo za následek, že se našla skupina lidí, která se rozhodla toto využít ve svůj přímý či nepřímý prospěch a lidé ze skupiny začali cestovat v čase za účelem změny minulosti. To, co nastalo, byl tak hrozný zmatek, že vyústil v neustálé změny dějin, které měly za následek změnu budoucnosti a to zcela nepředvídanou, vedlo to však k tomu, že kolem roku 9000 se skupina lidí rozhodla, že taková anarchie není možná a hlavně může vést k definitivnímu zničení lidstva bez možnosti nápravy. Nepochopil sice řadu souvislostí, kauzalit a determinismů v dalším vysvětlení, ale oficiální historie byla adeptům vyložena takto:

- v roce 9011 vznikla rovnováha lidstva – tzv. Ultima Paradise
- aby úmyslné nebo neúmyslné změny minulosti neměly negativní vliv na vytvoření tohoto zářného cíle a stavu lidstva, je s okamžitou platností zakázáno cestovat do minulosti (až na výjimky uvedené dále)
- vědci sestavili dějiny lidstva a tyto dějiny se nesmí změnit, neboť by to mohlo mít za následek to, že Ultima Paradise nevznikne
- to, že je možné cestovat časem, plyne z obecné teorie relativity propojené s kvantovou teorií, teorií neurčitosti a teorií tachyonů (částice rychlejší než světlo)
- malá změna v historii může, ale nemusí mít za následek změnu různé intenzity s různým dopadem v jiném čase
- dějiny jsou to, co lidé z jiného času vědí o čase předchozím
- mimo prostor Země ve velmi těžko energeticky vzdálené části vesmíru vznikla časová kapka, která má speciální energetický tunel do Ultima Paradise, v časové kapce je výcvikové středisko Strážců času, analyticko-historické oddělení a zásahová jednotka vycvičených strážců času
- důvodem je, že při změně dějin se sice může stát, že se významně změní známé dějiny a dokonce i zmizí Ultima Paradise, ale časová kapka touto změnou není dotčena a analyticko-historické oddělení navrhne takové změny, úpravy, které vedou k tomu, že se objeví opět Ultima Paradise a dalšími změnami dokončí to, že se dějiny dostanou do souladu s popsaným a známým stavem
- dějiny se někdy mění zcela nečekaně a bez zásahu zvenčí a to na základě vnitřních energetických fluktuací, které plynou z teorie neurčitosti, z hlediska pozorovatele v daném časoprostoru se nějaká událost prostě stane, ale podle dějin se stát neměla (nebo opačně)
- jako příklad bylo Petrovi uvedeno toto: „Podívejte se, třeba ve vaší specializaci. Nějaký luštitel má před sebou zašifrovanou zprávu. Pokud ji vyluští, má to za následek např. vítězství v bitvě a tím třeba v celé válce. Jenže právě díky časové fluktuaci se může stát, že se mu zprávu nepodaří vyluštit. To může mít za následek, že se změní významným způsobem následné dějiny. Třeba díky tomu ale zmizí i Ultima Paradise. V tom okamžiku zasáhne naše jednotka strážců času.“
- Petr se naivně zeptal, jak to jednotka udělá? Vtrhne tam s novodobou technikou a pomůže bitvu vyhrát nebo tak nějak? Přednášející jen zdvihl obočí. Jistěže ne. To by mělo za následek, že zmínky o pomoci by se objevily v dalších dějinách. Protože ale o nich nevíme, znamená to, že nastat v tomto rozsahu nesmí. Nesmíme změnit známé dějiny. Můžeme však dotyčnému v tomto případě pomoci zprávu vyluštit. Pokud to uděláme

vhodným způsobem, který nebude dále v dějinách zachycen, tak se nám naše dílo podařilo a důsledkem bude, že se vše v čase vrátí do původního stavu a tedy včetně vzniku Ultima Paradise.

- Aha, rozumím. Jsem tedy zde pro případ, že bude potřeba vyluštit nějakou klasickou šifru a napovědět luštitelům v daném čase a prostoru nebo ji místo nic vyluštit a předat. To chápu, ale proč já? To nemáte někoho z dalších století a tisíciletích lepšího? Velitel výcviku se usmál a řekl: „Petře, nepodceňujte se! Již sto let po datu Vašeho narození se používaly pouze binární šifry a dvěstě let po Vašem narození kvantové šifry. Prostě zkušenosti s luštěním klasických šifer již vaši následovníci nemají. Navíc znáte dějiny od roku cca 0 n.letopočtu do roku 2011 a tedy právě dějiny období, kdy se tyto šifry používaly. Máte představu, jak lidé v dané době žili, jak se oblékali, víte co jedli a máte základní jazykovou vybavenost.. Prostě pro toto období a pro tuto činnost jste vhodným strážcem. Čili při výběru kandidátů pro nějakou činnost dáváme vždy přednost pro kandidáty z vrcholu daného období. Máme zde všechny možné specializace, které se hodí pro speciální úkoly, které naše jednotky strážců času plní.
- Znovu opakuji, v dějinách je mnoho a mnoho událostí, které nejsou nikde zaznamenány a tedy se o nich neví a jejich dopad tedy může, ale nemusí mít vliv na dějiny. Zde tedy máme velké možnosti a můžeme nasadit prakticky libovolnou techniku a prostředky; když se o tom neobjeví záznam a naše dějiny se nezmění, pak se zásah povedl.
- Analyticko-historické oddělení provedlo vždy před zásahem podrobný rozbor a navrhlo vhodný způsob nápravy. Zásah po provedení pečlivě vyhodnotilo a pokud se o něm neobjevil někde v budoucnosti záznam, byl úspěšný.
- Mezi strážci se vyprávěly neuvěřitelné příběhy. Jeden ze strážců neustále například dokola popisoval svůj nejzajímavější úkol. Skutečná matka Leonarda da Vinciho – Caterina - byla otrokyně pocházející z Východu. Otci Leonarda ji věnoval jeden florentský šlechtic. S ní měl mít Piero da Vinci syna Leonarda. Jenže v té době Piero - Leonardův otec - žil v manželství s jinou ženou. Ta velmi hlídala jeho večerní návštěvy u Cateriny. Prakticky k ní přicházel na lože velmi málo. To mělo za následek jednu z fluktuací v čase. Caterina neotěhotněla a právoplatná manželka Piera da Vinci u manžela prosadila, že Caterinu prodal svému příteli. Tím se ovšem stalo, že se Leonardo da Vinci nenarodil. To však byla tak významná historická událost, že to změnilo celé dějiny světa. Nezbylo než zasáhnout. Řešení bylo více, ale nakonec se našlo to nejjednodušší. Jeden ze strážců dostal za úkol navštívit rodinu da Vinci jako mladý kupec a zde přespat. Podařilo se mu navázat kontakt s Caterinou a dokonce ji v noci navštívit. Strážce tu noc s ní zplodil syna. Ta se

samozřejmě nikdy nepřiznala. Piero da Vinci si myslel, že je otec chlapce on a měl z otěhotnění Cateriny radost. Nátlakům své právoplatné manželky odolal a Caterinu u sebe ponechal a o chlapce, který se narodil, se řádně postaral a do smrti věřil, že je to jeho syn. V tomto platném čase se na svět dostal geniální Leonardo da Vinci díky zásahu z daleké budoucnosti.. Strážce se při vyprávění tohoto příběhu rozhlédl a řekl: „Jak by nebyl Leonardo geniální, vždyť byl po mně!“

Po úvodním kurzu absolvoval Petr jednoroční kurz sebeovládání, psychologie, historie a jazykovědy. To jej poměrně bavilo a bez velkých problémů kurz absolvoval.
Následoval 6-ti měsíční kurz, ve kterém se seznámil s různými technologiemi, kterými strážci disponují a mohou je na základě rozhodnutí analyticko-historického oddělení použít.
Pak absolvoval 5 jednodenních návštěv v různých časových obdobích. Naučil se tak prakticky ovládat technologii cestování časem a získal potřebný stupeň profesního sebevědomí a umění se pohybovat mezi lidmi jiného věku.

Celá jeho příprava byla uzavřena jednoměsíční dovolenou na začátku třetihor. Koupal se v teplém šelfovém moři, chodil na vycházky a obdivoval panenskou třetihorní přírodu, lovil, rybařil.
Po návratu z dovolené byl pozván na vedení analyticko-historického oddělení a zde mu byl předán diplom o absolvování a odznak strážce – zlatou hvězdu se zeleným smaragdem a s vyrytým jménem a jednoznačným identifikačním kódem, který byl vytvořen jako otisk jeho DNA. Peterovi byla přečtena rozsáhlá přísaha a on vyslovil nahlas: „Tak přísahám“.
Tak se stal Dr. Peter Hayek jedním ze strážců času se speciální profesí luštitel klasických šifer.
Peter trávil svůj volný čas v knihovně a hltal zde dějiny lidstva. Dějiny, které pro něj byly budoucností, jej nesmírně zajímaly. Divil se, že lidstvo dělalo stále stejné chyby, ale současně obdivoval, že vždy v těch těžkých chvílích se našel nějaký vůdce – vizionář a řada poctivých lidí, kteří tyto vize dokázali realizovat.
A pak nastal ten den, na který byl připravován a na který čekal. Byl nasazen do své prvé akce. Na historicko-analytickém odboru mu podrobně vysvětlili, co se stalo a jak se očekává, že by náprava mohla proběhnout. Byl seznámen s tím, co vše se o daném časovém okamžiku a osobách ví a tedy co by během řešení svého úkolu neměl porušit. Pak Dr. Peter Hayek dostal naprogramovanou kartu s nahranou stáží, popřáli mu mnoho štěstí a pak nastoupil do časoprostorového výtahu na svoji prvou akci.

D. O čem jsme psali v říjnu 2000 – 2010

Crypto-World 10/2001

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)
(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

Crypto-World 10/2002

Crypto-World 10/2003

Crypto-World 10/2004

Příloha : J.Pinkava - Hashovací funkce v roce 2004 , hash_2004.pdf

Crypto-World 10/2005

Příloha : Další informace k článku V.Klímy - prilohy.zip (53 kB)
(Obsahuje: Žádost a podpisy odborníků, Návrh Šámal, Návrh Smejkal, Návrh VK_IURE, překlad části úmluvy, průvodní dopis vk_iure, link psp, stenozáznam jednání PSP, tisk zpráva ČTK)

Crypto-World 10/2006

Příloha: doprovodné materiály k Soutěži v luštění 2006 - vystava.pdf , epilog.pdf

Crypto-World 10/2007

Crypto-World 10/2008

Příloha: simulátor historického šifrátoru Lorenz SZ 40- lorenz.zip.enp

Crypto-World 10/2009

Crypto-World 10/2010

E. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem 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 Vlastimil Klíma Tomáš Rosa Dušan Drábik
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Jaroslav Pinkava
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/
Dušan Drábik	Dusan.Drabik@o2bs.com ,	
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