Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 13, číslo 1/2011 **15. leden 2011**

1/2011

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1355 registrovaných odběratelů)

Obsah :

A. Československé šifry z obdobia 2. svetovej vojny
Úvod k seriálu

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

V rokoch 1939 až 1945 československá exilová vláda v Londýne, komunikovala so svojimi zahraničnými expozitúrami a domácimi agentami prevažne prostredníctvom rádia. Svoje depeše samozrejme šifrovala, avšak plk. Moravec z londýnskej rozviedky, nechal jediného profesionálneho vojenského kryptológa, Josefa Růžka, v protektoráte. Dôsledkom toho bolo, že používané šifry boli veľmi nízkej kvality. Naviac sa londýnska centrála dopúšťala aj mnohých kryptografických prehreškov, takže nemci počas vojny československé šifry bez vážnejších problémov lúštili. Kryptoanalýza a postupy lúštenia prevažnej väčšiny použitých šifier boli známe a v literatúre popísané už počas 1. svetovej vojny, prípadne aj skôr. Celkovo bolo československou exilovou vládou v Londýne počas vojny používaných vyše 50 rôznych šifier. Boli to všetko ručné šifry zostavené ako rôzne kombinácie substitúcie (S), transpozície (T), prípadne pričítania periodického hesla (P). Takéto šifry sa preto niekedy zvyknú označovať ako STP šifry.

Cieľom tohto seriálu je zosumarizovať známe fakty o československých šifrách používaných počas 2. svetovej vojny. Bežne dostupné informácie o týchto šifrách sa nachádzajú v niekoľkých knihách a skriptách uvedených na konci každej časti, v použitej literatúre. Najdôležitejšie pramene sú knihy pána Janečku. V nich popisované šifry sú podrobne zdokumentované a ku všetkým je uvedený aj náčrt kryptoanalýzy, alebo priamo postup kryptoanalýzy aj s príkladom lúštenia. Žiaľ pán Janečnek vo svojich knihách popisuje len zopár najdôležitejších typov šifier, ktoré tvoria len malú časť z ich celkového počtu. V knihe pána Hanáka je popis šifier skôr poslabší a s viacerými chybami, ale na druhej strane je tam zoznam až desiatich používaných šifier. V nasledujúcom texte bude postupne popisovaných jedenásť šifier. Informácie o týchto šifrách pochádzajú z uvedenej literatúry a vo veľmi malej miere aj z internetových zdrojov. Žiaľ ani popis týchto jedenástich šifier nie je úplne kompletný. Samotný postup šifrovania je síce kompletne popísaný, ale v niekoľkých prípadoch mi chýbajú informácie napr. o zostavovaní služobného záhlavia depeší, rozdeľovaní depeší na časti a pod. Preto som si pre potreby popisu šifier niektoré chýbajúce časti „vymyslel“ tak, aby sa dali pomocou uvedeného popisu zašifrovať a dešifrovať depeše. Na tieto mnou doplnené (neautentické) časti popisu šifier samozrejme v texte upozorňujem, takže by nemalo dôjsť k nedorozumeniam.

B. Československé šifry z obdobia 2. svetovej vojny Diel 1., Šifra TTS

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, tak všetky tieto informácie s radosťou uvítam.

1 Šifra TTS

Túto šifru používala exilová vláda v Londýne na spojenie s domácim odbojom po veľmi dlhý čas na začiatku vojny. Používal ju aj štábny kapitán Morávek. Popis tejto šifry, ako aj popis jej lúštenia, môžme nájsť v [3] (str. 49–60) a ešte podrobnejší popis lúštenia v [5] (str. 253–268). Jednalo sa o dvojitú tabuľkovú transpozíciu a následnú substitúciu znakov za dvojice čísel.

1.1 Všeobecný popis a príklad šifrovania depeší

Postup šifrovania je veľmi jednoduchý. Nasledovný popis vychádza z [3] (str. 49–50). Transpozičné heslá sa vyberali z dohodnutých kníh a šifrovanie záviselo od dňa, v ktorom bolo robené. Pre výber základu textu hesla bolo stanovených 12, prípadne, v niektorých iných variantoch, 17 znakov. Pre jednotlivé dni v mesiaci boli stanovené dĺžky transpozičných hesiel a posun substitučnej abecedy zoznamom. Zoznam mohol vyzerať napríklad takto:

`1-18-21 ; 2-14-17 ... 13-15-19 ... 30-16-19 ; 31-18-15`

V číselných trojiciach prvé číslo znamená deň šifrovania, druhé a tretie čísla určujú dĺžky hesiel prvej a druhej transpozičnej tabuľky. Na finálnu substitúciu sa zväčša používala neúplná, 45 znaková česká abeceda, doplnená o číslice 0 až 9 a štyri špeciálne znaky. Táto substitučná abeceda, vo svojej základnej podobe, je uvedená v tabuľke 1 na str. 4. V [5] na str. 257 je uvedená mierne odlišná substitučná abeceda, v ktorej je namiesto znaku ? uvedený znak : a v [2] sú uvedené iné, mierne odlišné, abecedy. Je teda pravdepodobné, že sa postupne použité abecedy podľa potreby modifikovali. Pri šifrovaní sa znaky v substitučnej tabuľke cyklicky posúvali tak, že písmeno

	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	.	?	-	/	1	2	3	4
4	5	6	7	8	9	0				

Tabuľka 1: Česká 45 znaková abeceda v základnej podobe

`A` malo hodnotu zodpovedajúcu dňu šifrovania. Tabuľka 1, tak ako je uvedená, by sa teda používala na substitúciu 1. deň v mesiaci.

Ak sa šifroval dlhší text, tak tento sa rozdelovaľ na depeše dĺžky zhruba 50 znakov[1], pričom každá depeša končila vždy celým slovom. Aby sa zabezpečila nadväznosť depeší, každá depeša seriálu začínala a končila znakom lomítko (`/`) a písmenom príslušného dielu (`A, B, C,...`). Prvý diel teda končil znakmi `/A`, druhý diel sa začínal znakmi `A/`, končil znakmi `/B` atď. Pri rozdeľovaní depeší šifrovaných rovnakými heslami bolo treba dbať na to, aby diely nemali rovnakú dĺžku. Na toto sa počas vojny veľmi často zabúdalo a to významne uľahčilo prácu lúštiteľom.

Text, ktorý sa chystáme zašifrovať, sa zapisoval len pomocou znakov substitučnej abecedy, t.j. `Á` sa nahradilo pomocou `A`, `Ď` pomocou `D` atď. Slová sa oddeľovali buď pomlčkou, alebo niektorým iným špeciálnym znakom. Čiže ak v texte bola medzi slovami len medzera, tak sa táto nahradila pomlčkou. Pokiaľ medzi slovami bola bodka (napr. koniec vety), tak sa nasledujúca medzera vynechala. Podobne sa za znakmi `?` a `/` nepísala extra medzera.

Ak by sme sa teda dohodli, že na tvorbu hesiel použijeme knihu Simona Singha: *Kniha kódů a šifer*, (Dokořán, 2003) a text budeme šifrovať 13. deň v mesiaci, tak postup bude nasledovný. Na 13. strane, na začiatku 13. riadku, vyberieme prvých 12 znakov ako základ hesla prvej transpozičnej tabuľky. Sú to znaky: `KLADÁM PŘÍBĚH`. Potom ďalších 12 znakov ako základ hesla druhej transpozičnej tabuľky. To budú znaky: `Y O POLITICKÝC`. Medzery sa do počtu znakov nerátajú. Zoznam dĺžok transpozičných hesiel určuje na 13. deň mesiaca dĺžky hesiel pre prvú a druhú transpozičnú tabuľku 15, resp. 19 znakov. Vybraných 12 znakov predĺžime na potrebnú dĺžku tak, že zopakujeme potrebný počet znakov zo začiatku vybraného úseku. Potom zapíšeme tieto znaky bez medzier a len pomocou znakov použitej substitučnej abecedy, t.j.

[1]Podľa ukážky autentických depeší z 11. 6. 1941, uvedených v knihe [5] na str. 254, sa delili správy aj na dlhšie časti. Niektoré z uvedených depeší majú aj viac než 100 znakov.

napríklad namiesto Á píšeme A, atď. Nakoniec obe transpozičné heslá vyčíslime obvyklým spôsobom a opäť podľa poradia znakov použitej substitučnej abecedy. V našom príklade dostaneme:

K	L	A	D	A	M	P	Ř	I	B	Ě	H	K	L	A
9	11	1	5	2	13	14	15	8	4	6	7	10	12	3

Tabuľka 2: Heslo prvej transpozičnej tabuľky a jeho vyčíslenie

Y	O	P	O	L	I	T	I	C	K	Y	C	Y	O	P	O	L	I	T
17	9	13	10	7	3	15	4	1	6	18	2	19	11	14	12	8	5	16

Tabuľka 3: Heslo druhej transpozičnej tabuľky a jeho vyčíslenie

Máme teda obe transpozičné heslá a ich vyčíslenie a môžme pristúpiť k šifrovaniu textu. Ako príklad použijeme citát od Senecu:

> *Poznáš, že neexistuje nic, oč by se nepokusila lidská odvaha, a i ty sám se staneš divákem i jedním z těch, kdo se pokoušejí o velké věci.*
>
> *Seneca*[2]

Tento text je na jednu depešu príliš dlhý (113 znakov bez medzier, čiarok a bodky). Preto ho rozdelíme do troch depeší. Medzery nahradíme pomlčkami (resp. na konci vety bodkou), použijeme len znaky substitučnej abecedy a na konce a začiatky depeší pridáme označenie nadväznosti dielov:

```
POZNAŠ-ŽE-NEEXISTUJE-NIC-OČ-BY-SE-NEPOKUSILA-LIDSKA/A

A/ODVAHA-A-I-TY-SAM-SE-STANEŠ-DIVAKEM-I-JEDNIM-Z-TĚCH/B

B/KTO-SE-POKOUŠEJI-O-VELKE-VĚCI.SENECA
```

Každú z týchto troch depeší teraz trasponujeme podľa prvej, tabuľky, potom podľa druhej tabuľky a následne spravíme substitúciu. Keďže šifrujeme 13. deň v mesiaci, na finálnu substitúciu použijeme posunutú substitučnú tabuľku uvedenú na str. 6.

[2]Pôvodná verzia v latinčine: *Videbis nihil humanae audaciae intemptatum erisque et spectator et ipse pars magna conantium. Seneca (Marc.18,7)*

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

Tabuľka 4: Česká 45 znaková abeceda pre 13. deň mesiaca

Takže najskôr zapíšeme všetky tri čiastkové depeše do prvej transpozičnej tabuľky, pričom v hornom riadku tabuľky je vyčíslenie transpozičného hesla. Text sa do tabuliek píše po riadkoch zľava doprava a zhora nadol, čiže bežným spôsobom:

9	11	1	5	2	13	14	15	8	4	6	7	10	12	3
P	O	Z	N	A	Š	-	Ž	E	-	N	E	E	X	I
S	T	U	J	E	-	N	I	C	-	O	Č	-	B	Y
-	S	E	-	N	E	P	O	K	U	S	I	L	A	-
L	I	D	S	K	A	/	A							

POZNAŠ-ŽE-NEEXISTUJE-NIC-OČ-BY-SE-NEPOKUSILA-LIDSKA/A

9	11	1	5	2	13	14	15	8	4	6	7	10	12	3
A	/	O	D	V	A	H	A	-	A	-	I	-	T	Y
-	S	A	M	-	S	E	-	S	T	A	N	E	Š	-
D	I	V	A	K	E	M	-	I	-	J	E	D	N	I
M	-	Z	-	T	Ě	C	H	/	B					

A/ODVAHA-A-I-TY-SAM-SE-STANEŠ-DIVAKEM-I-JEDNIM-Z-TĚCH/B

9	11	1	5	2	13	14	15	8	4	6	7	10	12	3
B	/	K	T	O	-	S	E	-	P	O	K	O	U	Š
E	J	I	-	O	-	V	E	L	K	E	-	V	Ě	C
I	.	S	E	N	E	C	A							

B/KTO-SE-POKOUŠEJI-O-VELKE-VĚCI.SENECA

Následne text z prvých transpozičných tabuliek prepisujeme do druhých transpozičných tabuliek. Z prvých tabuliek text vypisujeme po stĺpcoch zhora nadol, pričom poradie stĺpcov je určené vyčísleným heslom a do druhých tabuliek text zapisujeme bežným spôsobom po riadkoch zľava doprava a zhora nadol:

17	9	13	10	7	3	15	4	1	6	18	2	19	11	14	12	8	5	16
Z	U	E	D	A	E	N	K	I	Y	-	-	-	U	N	J	-	S	N
O	S	E	Č	I	E	C	K	P	S	-	L	E	-	L	O	T	S	I
X	B	A	Š	-	E	A	-	N	P	/	Ž	I	O	A				

POZNAŠ-ŽE-NEEXISTUJE-NIC-OČ-BY-SE-NEPOKUSILA-LIDSKA/A

17	9	13	10	7	3	15	4	1	6	18	2	19	11	14	12	8	5	16
O	A	V	Z	V	-	K	T	Y	-	I	A	T	-	B	D	M	A	-
-	A	J	I	N	E	-	S	I	/	A	-	D	M	-	E	D	/	S
I	-	T	Š	N	A	S	E	Ě	H	E	M	C	A	-	-	H		

A/ODVAHA-A-I-TY-SAM-SE-STANEŠ-DIVAKEM-I-JEDNIM-Z-TĚCH/B

17	9	13	10	7	3	15	4	1	6	18	2	19	11	14	12	8	5	16
K	I	S	O	O	N	Š	C	P	K	T	-	E	O	E	K	-	-	L
B	E	I	O	V	/	J	.	U	Ě	-	-	E	S	V	C	E	E	A

B/KTO-SE-POKOUŠEJI-O-VELKE-VĚCI.SENECA

Text z druhých transpozičných tabuliek opäť vypíšeme po stĺpcoch zhora nadol, pričom poradie stĺpcov bude určené vyčísleným heslom. Dostaneme texty:

IPN-LŽEEEKK-SSYSPAI--TUSBDČŠU-OJOEEANLANCANIZOX--/-EI

YIĚA-M-EATSEA/-/HVNNMDHAA-ZIŠ-MADE-VJTB--K-S-SO-IIAETDC

PU--N/C.-EKĚOV-EIEOOOSKCSIEVŠJLAKBT-EE

Teraz v uvedených troch textoch spravíme substitúciu znakov za čísla, podľa tabuľky 4 na str. 6. Následne takto získané číselné depeše zapíšeme v skupinách po 5 cifier. Pokiaľ nám budú chýbať na konci nejaké cifry do násobku 5, tak ich doplníme náhodne, pričom na mieste desiatok píšeme cifry, ktoré sa tam podľa substitučnej tabuľky nemôžu vyskytnúť (t.j. 5, 6, 7, 8, 9). Napokon už len na začiatok pridáme návestie depeše v tvare `xxx-yyy-zz`, kde `xxx` je poradové číslo depeše, `yyy` je počet cifier depeše a `zz` je deň šifrovania depeše. V našom príklade dostaneme tri depeše v tvare:

```
045-110-13
23302 80126 43181 81825 25013 43441 34301 32301 01363 73414
17163 53701 29242 91818 13282 61328 15132 82342 29400 10102
01182 38473
```

```
046-110-13
41231 91301 27011 81336 34181 30201 02223 82828 27172 21313
01422 33501 27131 71801 38243 61401 01250 13401 34290 12323
13183 61715

047-080-13
30370 10128 02154 40118 25192 93801 18231 82929 29342 51534
23183 83524 26132 51436 01181 88591
```

V uvedených depešiach je, pri znalosti použitého postupu šifrovania, hneď vidno, že do prvej depeše boli doplnené 4 cifry, do druhej depeše nebolo treba dopĺňať žiadnu cifru a do tretej depeše boli doplnené opäť 4 cifry. Uvedené depeše sú týmto pripravené na odoslanie.

1.2 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 ktorého vieme zostaviť substitučnú tabuľku.

c. Sú dané heslá potrebnej dĺžky pre prvú aj druhú transpozičnú tabuľku. Nebudeme sa zaoberať tým ako sme tieto heslá dostali, proste sú dané.

Potom šifrovanie depeše bude prebiehať podľa nasledovných krokov:

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

2. Medzery medzi slovami nahradíme pomlčkou. Pokiaľ sa medzi niektorými slovami textu nachádza niektorý zo špeciálnych znakov obsiahnutých v substitučnej tabuľke, tak sa za týmto znakom medzera vynecháva.

3. Text rozdelíme na časti približne 50 znakov dlhé tak, aby každá časť vždy končila kompletným slovom. Dávame pritom pozor, aby rôzne časti textu nemali rovnakú dĺžku, pričom zohľadníme aj znaky pridané k textu kvôli nadväznosti dielov (podľa ďalšieho bodu).

4. 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 znak `/` a na konci textu znak `/` 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.

5. Každú časť textu šifrujeme zvlášť a každá časť textu tvorí samostatnú depešu s vlastným návestím.

6. Pri šifrovaní text najskôr zapisujeme do prvej transpozičnej tabuľky po riadkoch zľava doprava a zhora nadol.

7. Z prvej transpozičnej tabuľky text čítame po stĺpcoch zhora nadol, pričom poradie stĺpcov určuje vyčíslenie transpozičného hesla pre prvú tabuľku. Tento text zapisujeme do druhej transpozičnej tabuľky po riadkoch zľava doprava a zhora nadol.

8. Z druhej transpozičnej tabuľky text čítame po stĺpcoch zhora nadol, pričom poradie stĺpcov určuje vyčíslenie transpozičného hesla pre druhú tabuľku.

9. Zostavíme si substitučnú tabuľku pre príslušný deň šifrovania. Písmeno `A` je v substitučnej tabuľke umiestnené tak, aby jeho hodnota zodpovedala dňu šifrovania a ďalšie znaky potom nasledujú v obvyklom poradí, pričom tabuľka sa vypĺňa cyklicky. Znaky majú preto len hodnoty 01 až 45.

10. V texte vypísanom z druhej transpozičnej tabuľky spravíme substitúciu znakov za čísla, podľa substitučnej tabuľky.

11. Postupnosť čísel, ktorú sme dostali rozdelíme na skupiny po 5 cifier. Pokiaľ počet cifier, nie je násobkom 5, tak náhodne doplníme chýbajúce cifry, pričom na miesta desiatok píšeme len cifry 5, 6, 7, 8, alebo 9.

12. Na začiatok depeše pridáme ešte návestie v tvare `xxx-yyy-zz`, kde `xxx` je poradové číslo depeše, `yyy` je počet cifier depeše (aj s náhodne pridanými ciframi, t.j. toto číslo musí byť násobkom 5) a `zz` je deň šifrovania depeše. Týmto je šifrovanie depeše ukončené a depeša je pripravená na odoslanie.

1.3 Postup pri dešifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii kompletný text zašifrovanej depeše aj s návestím.

b. Sú dané heslá potrebnej dĺžky pre prvú aj druhú transpozičnú tabuľku.

Potom dešifrovanie depeše bude prebiehať podľa nasledovných krokov:

1. Na základe návestia si overíme kompletnosť depeše (počet cifier).
2. Podľa návestia depeše zistíme dátum šifrovania a zostavíme si príslušnú substitučnú tabuľku.
3. Vynecháme návestie depeše, ktoré už nebudeme potrebovať.
4. Z konca depeše vynecháme náhodne pridané cifry. Tieto spoznáme podľa toho, že na miestach desiatok majú cifry 5, 6, 7, 8, alebo 9.
5. Cifry depeše rozdelíme na dvojice a podľa substitučnej tabuľky ich nahradíme príslušnými znakmi.
6. Posledný riadok oboch transpozičných tabuliek nemusí byť úplný. Poznáme ale počet znakov samotnej depeše, poznáme šírku prvej aj druhej transpozičnej tabuľky, a teda vieme, koľko posledných stĺpcov v oboch tabuľkách bude kratších. Označíme si v oboch tabuľkách tieto kratšie stĺpce.
7. Znaky depeše zapíšeme do druhej transpozičnej tabuľky po stĺpcoch zhora nadol, pričom poradie stĺpcov bude dané vyčíslením druhého transpozičného hesla a niekoľko posledných stĺpcov tabuľky môže byť kratších.
8. Znaky depeše čítame z druhej transpozičnej tabuľky po riadkoch zhora nadol a zľava doprava a zapisujeme do prvej transpozičnej tabuľky po stĺpcoch zhora nadol, pričom poradie stĺpcov bude dané vyčíslením prvého transpozičného hesla a niekoľko posledných stĺpcov tabuľky môže byť kratších.
9. Znaky depeše čítame z prvej transpozičnej tabuľky po riadkoch zhora nadol a zľava doprava a zapíšeme. Pomlčky nahradíme medzerami a rovnako doplníme medzery za špeciálne znaky v texte. Týmto sme dostali pôvodný text depeše.
10. Pokiaľ sa jedná o seriál, tak text zostavíme v správnom poradí podľa označenia na začiatku a na konci jednotlivých častí seriálu.

1.4 Lúštenie

Z hľadiska lúštenia patrila šifra TTS k tým najjednoduchším, ktoré exilová vláda v Londýne používala. Ak totiž spravíme na texte dvojitú transpozíciu, tak opäť dostaneme len transpozíciu. Pri vhodne zvolenej veľkosti transpozičných tabuliek, bude táto nová transpozícia o čosi komplikovanejšia (bude mať „širšiu“ tabuľku), ale stále to bude len transpozícia a bude sa na ňu dať útočiť anagramovou metódou. Substitúcia znakov za čísla sa robila až po transpozícii a preto číselné dvojice predstavujúce znaky zostávajú pohromade. Jednotlivé znaky sa dajú dobre rozpoznať, pretože na mieste desiatok môžu mať len cifry 0, 1, 2, 3, alebo 4 a môžme použiť frekvenčnú analýzu. Toto všetko nemecký lúštitelia vedeli a robili. Naviac ich z Londýna zásobovali veľkým množtvom, často zbytočného[3], textu a množtvom depeší rovnakej dĺžky, zašifrovaných rovnakými heslami.

Postup lúštenia popísal dostatočne dobre pán Janeček v knihe [3] (str. 49–60) a ešte podrobnejšie v knihe [5] (str. 253–268). V knihe [5] sa podrobne uvádza postup lúštenia na príklade autentických depeší z 2. svetovej vojny. K tomuto už niet viac čo dodať a záujemcov možno len odporučiť na uvedené zdroje. Lúštenie sa zakladalo na anagramovej metóde a využívalo aj časté chyby šifrantov. Nemecký lúštitelia depeše šifrované pomocou TTS lúštili počas celej doby ich používania.

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

[3] Napr. dlhé Benešové prejavy, opisy novinových článkov, ktoré sa dali zohnať aj v protektoráte a pod.

C. Nové užitečné statistické testy

Vlastimil Klíma, kryptolog, KNZ, s.r.o., Praha
(http://cryptography.hyperlink.cz, vlastimil.klima@knzsro.cz)

Je to s podivem, že byly objeveny nové statistické testy, které jsou jiné a užitečnější, než stávající. Jsou univerzálně použitelné na testování náhodnosti binárních (a po modifikaci i nebinárních) dat. Statistika je věda natolik propracovaná, že přijít s něčím novým je opravdu neobvyklé. Proto ta novota vznikla na pomezí statistiky a kryptologie, kdy se tyto statistické testy ukázaly jako velmi citlivé k měření kvality některých vlastností kryptografických nástrojů. Pomocí nich byly po třinácti letech zkoumání nalezeny první "slabiny" (to je přehnané slovo) blokové šifry AES, přesněji řečeno první odchylky blokové šifry AES od očekávaného náhodného chování kvalitní šifry. Další výsledky přinesly tyto testy při zkoumání hašovacích funkcí v rámci probíhající světové soutěže na nový standard SHA-3. Mohou dokonce zasáhnout do jejího průběhu a naznačují, kde mohou mít kandidátské funkce slabiny a silné stránky. Testy jsou natolik složité a výkonnostně náročné, že se musí ještě potvrdit nezávislými realizacemi, stejně jakoby se jednalo o nějaké fyzikální experimenty nebo astronomická zkoumání. To, že se testy musí ověřovat nezávislými týmy, aby se potvrdila jejich platnost, je také zajímavá paralela s naším okolním vědeckým světem, avšak pokud vím, první svého druhu v kryptologii (v matematice se toto už stalo mnohokrát). Možná se vám testy zalíbí a uvidíte možnost jejich využití ve své praxi. Ve své podstatě jsou jednoduché, což je činí ještě atraktivnějšími. Složité na jejich realizaci pro AES nebo hašovací funkce je v tom, že k rozpoznání odchylek pro odlišení těchto funkcí od náhodných funkcí je potřeba enormní objem dat. Předpokládáme, že se brzy dostanou do učebnic a do standardních balíků statistických testů a že ukáží některé vlastnosti finálních pěti kandidátů na SHA-3.

Test: Šifra:	SAC	LST	CoiT	CovT	Výsledky NIST
MARS	6	2	3	3	4
RC6	5	2	5	5	4
Rijndael	4	2	3	3	3
Serpent	4	2	4	4	4
Twofish	4	2	4	4	2

Tab.1: Staré výsledky (NIST) a přesnější výsledky nových testů 5 kandidátů AES

Sada testů náhodnosti

Předesíláme, že nyní se budeme věnovat sadě 4 testů, které navrhli turečtí matematici [1]. Netvrdíme, že právě tyto testy testují všechno a jsou jediné pravé pro testování náhodnosti, avšak umí dostat lepší výsledky při použití k testování blokových šifer, než byly obdrženy dosud a lepší, než balík statistických testů NIST, který byl mj. jiné použit v soutěži AES. Jistě je proto můžete použít i tam, kde jste testování náhodnosti binárních posloupností už prováděli nebo se ho chystáte provádět. Zajímavé by bylo porovnání i s jinými existujícími statistickými balíky nebo jejich obohacení o nové testy. Konkrétně si ukážeme výsledky sady 4 testů při použití na pět blokových šifer, z nichž se vybíral vítězný AES (tj. i včetně Rijndaelu, budoucího AES), viz tabulka 1. V pravém sloupci tabulky vidíme starý výsledek. Každý z algoritmů postupně nabírá složitost v tzv. rundách, které se opakují až do poslední rundy, která dává výsledek. Při první rundě není výsledek "šifrování" valný, takže ho všechny

testy zachytí jako nenáhodný, při druhé rundě už neprotestuje test Linear Span, při třetí rundě mlčí další dva testy u MARSu a Rijndaelu atd. Například pro splnění testu SAC potřeboval MARS 6 rund, zatímco staré testy NIST prohlašovaly už MARS se 4 rundami za náhodný. V tabulce vidíme, že nová sada testů zpřesnila výsledky NIST u všech pěti testovaných blokových šifer.

Test lavinovitosti (SAC)

Kdykoliv se změní jeden bit vstupu blokové šifry, měl by se s pravděpodobností 0,5 změnit každý bit výstupu. Toto nazýváme kritériem lavinovitosti (Strict Avalanche Criterion, SAC).

Test nelinearity (LST)

Správná náhodná Booleovská funkce by měla být nelineární, čili její vzdálenost od množiny všech afinních Booleovských funkcí daného počtu vstupních proměnných (bitů) by měla být velká. Nelinearita je také odrazem základního kritéria, který pro šifru stanovil Shannon jakožto kritérium zvané konfúze (confusion). Odpovídající test se nazývá test rozsahu lineární závislosti (Linear Span Test, LST) a měří, jak mnoho je lineárně závislá množina výstupů dané funkce (šifry), když její vstup tvoří množina vysoce lineárně závislých vstupů.

Test kolize (ColT)

Nalezení dvou hodnot vstupu, které dávají stejnou hodnotu výstupu by mělo být u náhodného zobrazení složité. Víme, že u náhodného zobrazení binárního zobrazení n bitů na n bitů je množina výstupů pouze cca 70 procent z celkového možného počtu a existují hodnoty, které není možno nabýt a naopak některé mají několik vzorů (nastane kolize). Bloková šifra je zvláštní v tom, že při pevném klíči je to náhodná permutace (kolize nikdy nenastane), ale při pevném vstupu a proměnném klíči je to (mělo by být) náhodné zobrazení, u kterého se může měřit míra koliznosti. V praxi se také z blokové šifry (náhodné permutace) vyrobí náhodné zobrazení tak, že se výstup ořízne na menší počet bitů (třeba 10 nebo 20) a kolize se hledají v této množině hodnot. Podobně to lze provést i při pevném klíči.

Test pokryvnosti (CovT)

Tento test měří náhodné zobrazení z opačné strany, tj. dívá se na to, jak mohutný je obraz celé vstupní množiny a jestli náhodou velikost této množiny obrazů není malá nebo velká. Také zde se může uvažovat jen příslušný počet bitů výstupu.

LITERATURA

[1] A. Doganaksoy, B. Ege, O. Kocak, F. Sulak: Cryptographic Randomness Testing of Block Ciphers and Hash Functions, http://eprint.iacr.org/2010/564.pdf

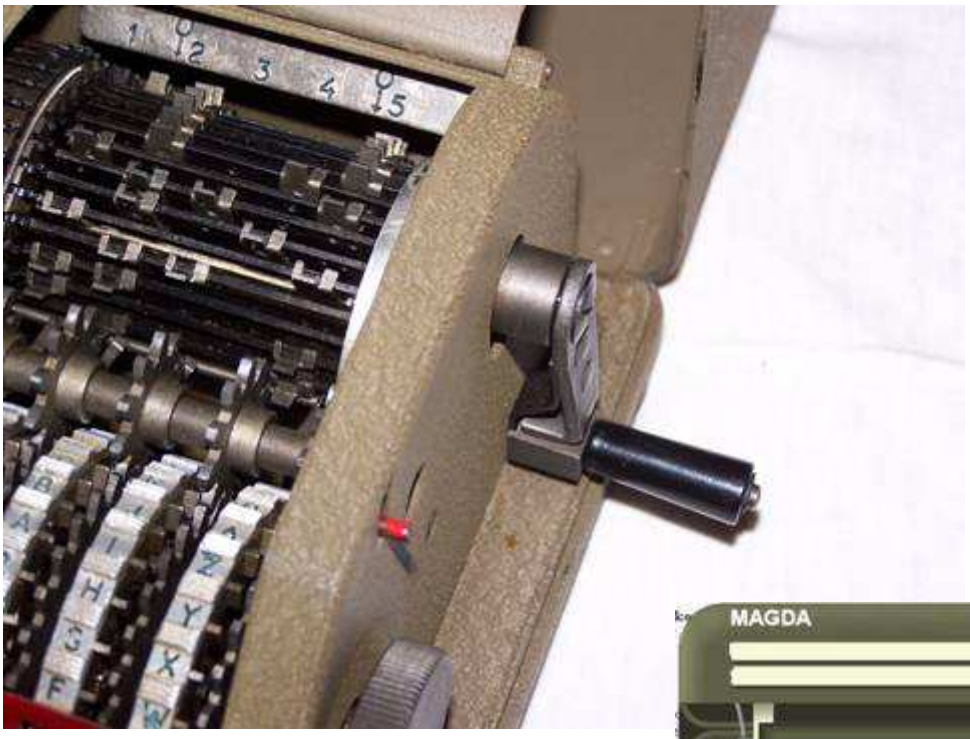
Tento článek v mírně odlišné podobě vyšel jako 89. pokračování seriálu ***Kryptologie pro praxi*** ve **Sdělovací technice**. Tyto články jsou většinou k dispozici na stránkách ST www.stech.cz po vydání časopisu nebo je k dispozici jejich archiv na stránkách autora http://cryptography.hyperlink.cz a část archivu (ale zase přehledněji) na stránkách kolegy Dr. Rosy http://crypto.hyperlink.cz.

D. Československý šifrátor MAGDA – dodatek k popisu v e-zinu Crypto-World č. 5/2007

Mgr. Karel Šklíba (karel.skliba@crypto-world.info)

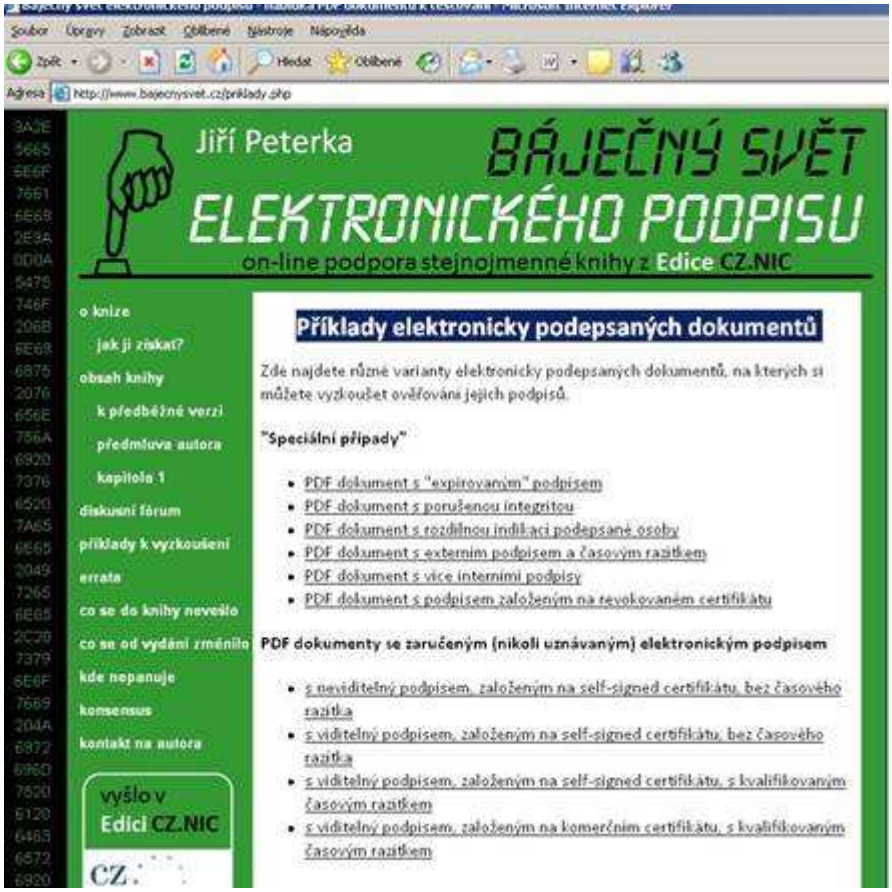
Díky laskavosti RNDr. Miloše Soukupa se podařilo zajistit detailnější popis a fotodokumentaci československého šifrátoru Magda, který byl vyvinut v první polovině padesátých let minulého století na generálním štábu tehdejší československé armády a který byl na základě dostupných informací popsán v příspěvku v e-zinu Crypto-Worldu 5/2007.

Šifrovací stroj Magda měl přesné rozměry šířka 152 mm, hloubka 160 mm a výška 105 mm bez gumových nožiček. S nožičkami měl výšku 115mm. Šifrátor měl hmotnost 4,23 kg. Na přiložených fotografiích lze odhalit různé podivuhodné konstrukční detaily i pěkný design. Stále však mějme na paměti, že se jedná o malého českého levobočka rozsáhlé euroamerické rodiny tohoto konstrukčního typu strojů, jejichž otcem je nezapomenutelný **Boris Hagelin**.



SW simulátor Hagelinu M-209, verze MAGDA od D. Rijmenantse.

E. Báječný svět elektronického podpisu J.Peterky



Následující informace vychází z tiskové zprávy internetového sdružení CZ NIC a z osobní komunikace s autorem připravované knihy.

Motto

Rychlejší a komfortnější komunikace se státní správou, úřady, bankami a dalšími institucemi – to je hlavní přínos elektronického podpisu. Přes své výhody je v České republice stále využíván minimálně, na vině je zejména nízká informovanost veřejnosti o tomto nástroji. Změnit by to mohla pomoci chystaná kniha publicisty a nezávislého konzultanta v oblasti internetových technologií Jiřího Peterky *Báječný svět elektronického podpisu*, kterou vydá správce české národní domény .CZ a to jako další titul v rámci své Edice CZ.NIC.

Podpůrný web, diskuzní fórum

Pracovní verze knihy je přístupná na internetové adrese http://www.bajecnysvet.cz .
Pokud chcete, aby byl *Báječný svět elektronického podpisu* ještě báječnější, pak můžete její finální verzi ovlivnit i vy a to v rámci diskusního fóra, které bylo na tomto webu pro daný účel zřízeno. Toto fórum bude laické i odborné veřejnosti otevřeno až do 11. února 2011.
Po uzavření diskusního fóra budou všechny příspěvky vyhodnoceny a případně zapracovány. Poté CZ.NIC finální verzi uvolní zdarma ke stažení (!) na stránkách své edice http://knihy.nic.cz/ , kde je již nyní k dispozici několik dalších odborných titulů z oblasti IT. Předpokládaný termín vydání knihy je duben 2011.

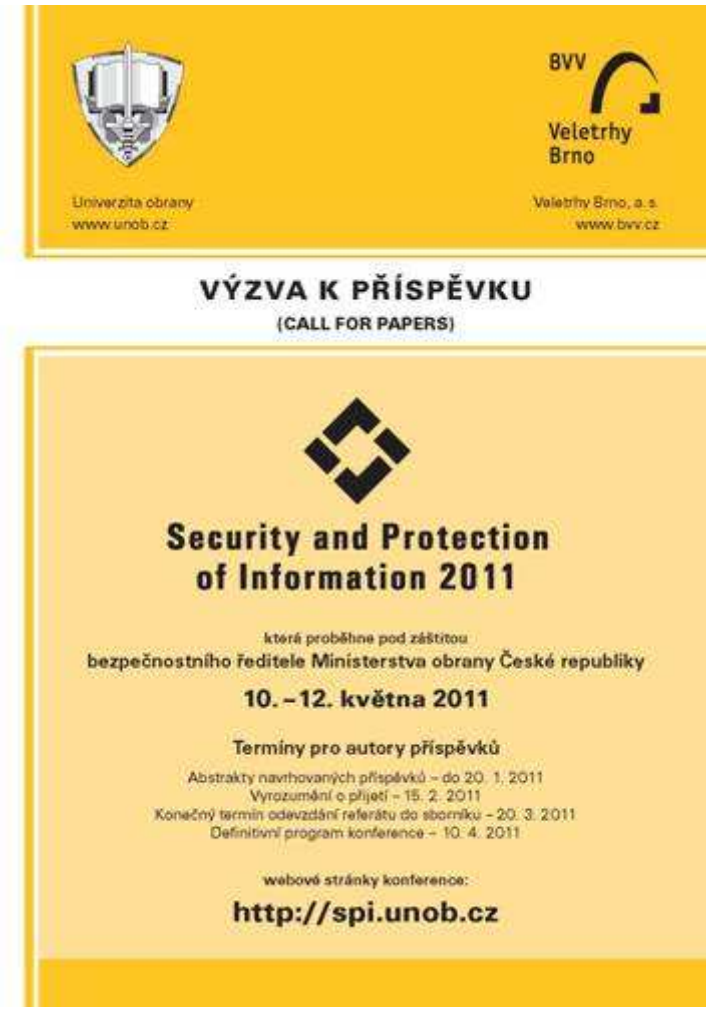
Citace z přebalu knihy

Tato kniha je psána pro lidi, kteří chtějí (či musí) používat elektronický podpis, chtějí mu rozumět, ale současně nepotřebují být odborníky na kryptografii. Celou složitou problematiku elektronického podpisu vysvětluje na třech úrovních: na úrovni úvodu a celkového přehledu, na úrovni principů elektronického podpisu a na úrovni běžné praxe (příprava počítače, podpisy na PDF dokumentech, podpisy v rámci MS Office, šifrování, přihlašování a zabezpečená komunikace).

Podpůrný web knihy http://www.bajecnysvet.cz/
Edice CZ.NIC http://knihy.nic.cz/
Tisková zpráva http://www.nic.cz/page/839/pomozte-s-knihou-o-elektronickem-podpisu/

F. Poslední výzva k příspěvku na mezinárodní konferenci Security and Protection of Information konanou 10.– 12.května v Brně

Doc. Ing. Jaroslav Dočkal, CSc., jdockal.spi@gmail.com



Cílem mezinárodní vědecké konference **Security and Protection of Information** http://spi.unob.cz konané 10. – 12. května v Brně je pokračovat v tradici setkávání tuzemských i zahraničních zájemců o bezpečnost ICT ze státního sektoru, školství i komerční sféry a navázat tak na dosavadní konference pořádané od roku 2001 jednou za dva roky na BVV jako doprovodný program výstavy IDET.

Jako zvaní řečníci již potvrdili účast na letošní konferenci přední evropští experti v oblasti informační bezpečnosti Mike Just (Glasgow Caledonian University), Georgie Danezis (Microsoft Research, Cambridge), Dan Cvrček (Deloitte UK), Gilbert Wondracek (Technische Universität Wien) a Christian Rechberger (Katholieke Universiteit Leuven).

Zájemci o aktivní vystoupení by měli poslat své krátké teze v angličtině pořadatelům na adresu jdockal.spi@gmail.com elektronickou poštou do **20. ledna** (výjimečně do 31. ledna), konečný termín odevzdání referátu do sborníku je **20. března**.
Podrobné informace jsou na http://spi.unob.cz/vyzva.asp.

Témata konference nabídnutá autorům se týkají ochrany utajovaných informací: od bezpečnostní politiky po bezpečnost virtualizovaných datových center, bezpečnosti počítačových i unifikovaných sítí, aplikované kryptografie až po specifika bezpečnosti informací ve vojenském prostředí.

Na webu konference http://spi.unob.cz lze nalézt řadu podrobných informací a to včetně přihlašovacího formuláře a prezentací vystoupení na předchozích konferencích.

Témata konference nabídnutá autorům

Ochrana utajovaných informací:

- bezpečnostní politiky
- vývoj a aplikace bezpečnostních standardů
- slabiny IT systémů, management rizik, řešení rizik
- management bezpečnostních oprav
- bezpečnost mobilních zařízení
- forénzní analýza výpočetních systémů a sítí
- ekonomické otázky bezpečnosti
- bezpečnostní aspekty cloud computingu
- plánování kontinuity byznysu, obnova po havárii
- management identit, přístupu a autorizace
- prevence ztráty dat
- aplikace elektronického podpisu a PKI
- personální bezpečnost a ochrana programů
- virtualizace datových center a jejich bezpečnost

Bezpečnost počítačových sítí:

- bezpečnostní hrozby, hackerské aktivity, řešení incidentů
- bezpečnost protokolové sady TCP/IP, bezpečnost směrování
- bezpečnost VoIP, IT telefonie a WiFi sítí
- bezpečnost adresářů, elektronické pošty, DNS, a webu
- firewally, VPN, detekce a prevence průniku
- bezpečné programování a antivirové programy

Aplikovaná kryptografie:

- kryptografické aplikace
- bezpečnostní aplikace kryptografie a kryptoanalýza
- kryptografické algoritmy, jejich návrh a implementace
- modularita a opakované použití ověřených kritických komponent
- stanovení míry kryptografické bezpečnosti
- přijatelná rizika kryptografické bezpečnosti
- standardizace a kryptografie
- legislativa související s kryptografií
- technologie posilující soukromí
- dokazatelnost bezpečnosti
- RFID – bezpečnostní a kryptografické aspekty
- další oblasti kryptografie

Bezpečnost informací ve vojenském prostředí:

- víceúrovňové bezpečnostní systémy
- bezpečnostní politiky, procedury a regulace
- bezpečné nastavení operačních a databázových systémů
- technologické otázky počítačové bezpečnosti
- použití PKI ve vojenských aplikacích
- bezpečnost videokonferencí
- scénáře řešení bezpečnostních problémů, bezpečné vzdělávání a výcvik

G. 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
26.-27. 01. 2011	09:00–17:00	Pavel Vondruška	15	

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/

H. O čem jsme psali v lednu 2000 – 2010

Crypto-World 1/2006

Crypto-World 1/2007

Crypto-World 1/2008

Crypto-World 1/2009

Crypto-World 1/2010

I. 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