Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 14, číslo 3-4/2012 **1. duben**

3-4/2012

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1310 registrovaných odběratelů)

Obsah :

A. Československé šifry z obdobia 2. svetovej vojny Diel 11., Šifra „Palacký“

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.

11 Šifra „Palacký“

Šifra „Palacký“ je typu SPN. Jednalo sa o nahrádzanie znakov číslami, pričítanie periodického hesla a násobenie konštantou. Používali ju napríklad rádiostanice Margita, Maruša, Nina a Olena pri spojení medzi Moskvou a Slovenskom. Popis tejto šifry je uvedený v knihe [2] (str. 132–133).

11.1 Všeobecný popis a príklad šifrovania depeší

Popis šifry v [2] je v časti o pridelovaní a používaní hesiel veľmi nezrozumiteľný a mätúci. Podľa toho, čo je v danej knihe uvedené, sa dá získať len základná predstava o tom, ako asi bola táto šifra konštruovaná.

Pri šifrovaní touto šifrou sa text najskôr previedol do číselnej podoby. Substitúcia sa vykonávala pomocou tabuľky **A**, ktorá sa konštruovala z dvoch hesiel. Tieto heslá mali rovnaký počet znakov, jedno bolo textové a druhé číselné a označovali sa ako heslá **A**. Podľa informácie z [2] boli tieto heslá stále[1]. Ak by bola táto informácia aspoň čiastočne správna, tak by sa dalo predpokladať, že stála bola len textová časť hesla **A** a číselná časť sa volila vhodným spôsobom (musí mať rôzne cifry). Vyplýva to z popisu šifry a príkladu v [2]. Po vykonaní substitúcie sa pričitávalo periodické heslo, ktoré sa označovalo ako heslo **B**. Toto periodické heslo sa najskôr previedlo do číselnej podoby podľa tabuľky **A**, ktorá bola použitá pri substitúcii textu. Nakoniec sa ešte cifry depeše násobili dohodnutou konštantou modulo 10. Postup šifrovania predvedieme na texte:

[1] Táto informácia ale nie je príliš spoľahlivá, pretože práve v tejto časti je popis pána Hanáka veľmi mätúci.

Síla poctivosti je tak velká, že si jí vážíme i u těch, které jsme nikdy neviděli, a také, což je ještě důležitější, u nepřítele. [2]

Na šifrovanie a dešifrovanie potrebujeme heslá **A** (textové a číselné), heslo **B** a dohodnutú multiplikatívnu konštantu. Okrem toho mal každý šifrant pridelené identifikačné číslo, ktoré sa schovávalo do služobných údajov a identifikovalo odosielateľa, čo uvedieme neskôr.

V našom príklade použijeme tie isté heslá a multiplikátívnu konštantu, ako sú uvedené v [2] na strane 132. Takže:

Heslá **A**: `NITRA` a `26491`
Heslo **B**: `NAD TATROU SA BLYSKA`
Konštanta: `3`

Číselná časť hesla **A** by mohla byť aj vhodne zvolená šifrantom, pretože je obsiahnutá v služobných údajoch depeše a adresát si ju odtiaľ vie zistiť. Pri substitúcii sa používala 30-znaková abeceda, pozostávajúca z 26 znakov medzinárodnej abecedy, bez písmen `Q, W` a pridali sa písmena `Č, CH, Ř, Š, Ž` a znak `/`. Substitučná tabuľka mala rozmer 3x10 a konštruovala sa na základe hesiel **A** jedným z nasledovných dvoch spôsobov (tabuľka 1 resp. 2):

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

Tabuľka 1: Variant 1

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

Tabuľka 2: Variant 2

My budeme substitúciu robiť prvým spôsobom. Text, ktorý ideme šifrovať, prepíšeme pomocou znakov obsiahnutých v substitučnej tabuľke. Vynecháme teda špeciálne znaky a medzery. Následne pomocou substitučnej

[2] Pôvodná verzia v latinčine: *Tanta vis probitatis est, ut eam vel in eis, quos numquam vidimus, vel quod maius est, in hoste etiam diligamus. Marcus Tullius Cicero (Laelius de amicitia)*

tabuľky prevedieme text do číselnej podoby. Dostávame upravený text depeše:

SILAPOCTIVOSTIJETAKVELKAŽESIJIVAŽIMEIUTECHKTEREJSME
NIKDYNEVIDELIATAKECOŽJEJEŠTEDULEŽITEJŠIUNEPŘITELE

a jeho číselnú podobu:

46 26 65 21 60 68 25 24 26 41 68 46 24 26 61 20 24 21 63 41 20
65 63 21 48 20 46 26 61 26 41 21 48 26 67 20 26 49 24 20 69 63
24 20 29 20 61 46 67 20 22 26 63 28 45 22 20 41 26 28 20 65 26
21 24 21 63 20 25 68 48 61 20 61 20 44 24 20 28 49 65 20 48 26
24 20 61 44 26 49 22 20 60 42 26 24 20 65 20

Teraz podľa substitučnej tabuľky vyčíslime heslo **B**:

N	A	D	T	A	T	R	O	U	S	A	B	L	Y	S	K	A
22	21	28	24	21	24	29	68	49	46	21	23	65	45	46	63	21

Takto vyčíslené heslo periodicky podpíšeme pod cifry textu depeše. Potom sčítame cifry depeše s ciframi hesla modulo 10 a následne výsledok vynásobíme dohodnutou konštantou, tiež modulo 10. Takto dostaneme zašifrovaný text depeše. V našom príklade postup šifrovania bude vyzerať nasledovne:

Text 1	4	6	2	6	6	5	2	1	6	0	6	8	2	5	2	4
Heslo **B**	2	2	2	1	2	8	2	4	2	1	2	4	2	9	6	8
Súčet	6	8	4	7	8	3	4	5	8	1	8	2	4	4	8	2
Násobenie 3x	**8**	**4**	**2**	**1**	**4**	**9**	**2**	**5**	**4**	**3**	**4**	**6**	**2**	**2**	**4**	**6**
Text 2	2	6	4	1	6	8	4	6	2	4	2	6	6	1	2	0
Heslo **B**	4	9	4	6	2	1	2	3	6	5	4	5	4	6	6	3
Súčet	6	5	8	7	8	9	6	9	8	9	6	1	0	7	8	3
Násobenie 3x	**8**	**5**	**4**	**1**	**4**	**7**	**8**	**7**	**4**	**7**	**8**	**3**	**0**	**1**	**4**	**9**
Text 3	2	4	2	1	6	3	4	1	2	0	6	5	6	3	2	1
Heslo **B**	2	1	2	2	2	1	2	8	2	4	2	1	2	4	2	9
Súčet	4	5	4	3	8	4	6	9	4	4	8	6	8	7	4	0
Násobenie 3x	**2**	**5**	**2**	**9**	**4**	**2**	**8**	**7**	**2**	**2**	**4**	**8**	**4**	**1**	**2**	**0**
Text 4	4	8	2	0	4	6	2	6	6	1	2	6	4	1	2	1
Heslo **B**	6	8	4	9	4	6	2	1	2	3	6	5	4	5	4	6
Súčet	0	6	6	9	8	2	4	7	8	4	8	1	8	6	6	7
Násobenie 3x	**0**	**8**	**8**	**7**	**4**	**6**	**2**	**1**	**4**	**2**	**4**	**3**	**4**	**8**	**8**	**1**

Text 5	4	8	2	6	6	7	2	0	2	6	4	9	2	4	2	0
Heslo **B**	6	3	2	1	2	2	2	1	2	8	2	4	2	1	2	4
Súčet	0	1	4	7	8	9	4	1	4	4	6	3	4	5	4	4
Násobenie 3x	**0**	**3**	**2**	**1**	**4**	**7**	**2**	**3**	**2**	**2**	**8**	**9**	**2**	**5**	**2**	**2**
Text 6	6	9	6	3	2	4	2	0	2	9	2	0	6	1	4	6
Heslo **B**	2	9	6	8	4	9	4	6	2	1	2	3	6	5	4	5
Súčet	8	8	2	1	6	3	6	6	4	0	4	3	2	6	8	1
Násobenie 3x	**4**	**4**	**6**	**3**	**8**	**9**	**8**	**8**	**2**	**0**	**2**	**9**	**6**	**8**	**4**	**3**
Text 7	6	7	2	0	2	2	2	6	6	3	2	8	4	5	2	2
Heslo **B**	4	6	6	3	2	1	2	2	2	1	2	8	2	4	2	1
Súčet	0	3	8	3	4	3	4	8	8	4	4	6	6	9	4	3
Násobenie 3x	**0**	**9**	**4**	**9**	**2**	**9**	**2**	**4**	**4**	**2**	**2**	**8**	**8**	**7**	**2**	**9**
Text 8	2	0	4	1	2	6	2	8	2	0	6	5	2	6	2	1
Heslo **B**	2	4	2	9	6	8	4	9	4	6	2	1	2	3	6	5
Súčet	4	4	6	0	8	4	6	7	6	6	8	6	4	9	8	6
Násobenie 3x	**2**	**2**	**8**	**0**	**4**	**2**	**8**	**1**	**8**	**8**	**4**	**8**	**2**	**7**	**4**	**8**
Text 9	2	4	2	1	6	3	2	0	2	5	6	8	4	8	6	1
Heslo **B**	4	5	4	6	6	3	2	1	2	2	2	1	2	8	2	4
Súčet	6	9	6	7	2	6	4	1	4	7	8	9	6	6	8	5
Násobenie 3x	**8**	**7**	**8**	**1**	**6**	**8**	**2**	**3**	**2**	**1**	**4**	**7**	**8**	**8**	**4**	**5**
Text 10	2	0	6	1	2	0	4	4	2	4	2	0	2	8	4	9
Heslo **B**	2	1	2	4	2	9	6	8	4	9	4	6	2	1	2	3
Súčet	4	1	8	5	4	9	0	2	6	3	6	6	4	9	6	2
Násobenie 3x	**2**	**3**	**4**	**5**	**2**	**7**	**0**	**6**	**8**	**9**	**8**	**8**	**2**	**7**	**8**	**6**
Text 11	6	5	2	0	4	8	2	6	2	4	2	0	6	1	4	4
Heslo **B**	6	5	4	5	4	6	6	3	2	1	2	2	2	1	2	8
Súčet	2	0	6	5	8	4	8	9	4	5	4	2	8	2	6	2
Násobenie 3x	**6**	**0**	**8**	**5**	**4**	**2**	**4**	**7**	**2**	**5**	**2**	**6**	**4**	**6**	**8**	**6**
Text 12	2	6	4	9	2	2	2	0	6	0	4	2	2	6	2	4
Heslo **B**	2	4	2	1	2	4	2	9	6	8	4	9	4	6	2	1
Súčet	4	0	6	0	4	6	4	9	2	8	8	1	6	2	4	5
Násobenie 3x	**2**	**0**	**8**	**0**	**2**	**8**	**2**	**7**	**6**	**4**	**4**	**3**	**8**	**6**	**2**	**5**
Text 13	2	0	6	5	2	0										
Heslo **B**	2	3	6	5	4	5										
Súčet	4	3	2	0	6	5										
Násobenie 3x	**2**	**9**	**6**	**0**	**8**	**5**										

Zašifrovaný text depeše bude:

```
84214 92543 46224 68541 47874 78301 49252 94287 22484 12008
87462 14243 48810 32147 23228 92522 44638 98820 29684 30949
29244 22887 29228 04281 88482 74887 81682 32147 88452 34527
06898 82786 60854 24725 26468 62080 28276 44386 25296 085
```

K tomuto zašifrovanému textu ešte treba pridať služobné údaje. O tých sa v [2] toho moc nepíše. Spomína sa tam len spôsob maskovania identifikačného čísla šifranta a číselnej časti hesla **A** do päťmiestnych skupín. Skupina s číslom šifranta sa umiestňovala ako tretia a skupina s maskovaným heslom **A** sa umiestňovala ako predposledná skupina depeše. Prvé dve skupiny depeše zrejme obsahovali zamaskované číslo depeše, dátum odosielania a možno aj nejaké ďalšie informácie. Posledná skupina bola, podľa príkladu z [2], tvorená zašifrovaným textom. Ak táto posledná skupina nebola úplná, náhodne sa doplnila do piatich cifier. V príklade na strane 133 v [2] je táto skupina doplnená ciframi 0, čo nie je najšťastnejšie riešenie, pretože potom je veľmi pravdepodobné, že sa jedná o „nuly“ v kryptografickom zmysle. Pokiaľ túto skupinu doplníme na násobok 5 náhodne, spôsobíme tým len to, že po dešifrovaní na konci textu pribudnú 0 až 2 náhodné znaky, čo zrozumiteľnosť textu nijako neovplyvní.

Teraz ukážeme ako sa, podľa [2], tvorili kontrolné skupiny s identifikačným číslom šifranta a heslom **A**. Identifikačné čísla šifrantov boli, podľa príkladu v [2], trojmiestne. Pre náš príklad predpokladajme, že šifrant má identifikačné číslo 127. Potom sa toto číslo maskovalo takto:

Osobné číslo:	1		2		7
Vzájomné súčty:		3		9	
Medzivýsledok:	1	3	2	9	7
Násobenie 3x:	3	9	6	7	1
Zvolená konštanta:	3	3	3	3	3
Kontrolná skupina:	**6**	**2**	**9**	**0**	**4**

Tabuľka 3: Kontrolná skupina s osobným číslom šifranta

Podobne sa tvorila aj kontrolná skupina s heslom **A**. Príklad jej tvorenia je uvedený v tabuľke 4 na strane 7.

O tom, čo presne obsahovali prvé dve skupiny depeše, nič nevieme. Pre potreby nášho príkladu budeme predpokladať, že tieto skupiny obsahujú trojciferné číslo depeše, identifikátor použitej substitučnej tabuľky (variant 1

Heslo **A**:	2	6	4	9	1
Násobenie 3x:	6	8	2	7	3
Zvolená konštanta:	3	3	3	3	3
Kontrolná skupina:	**9**	**1**	**5**	**0**	**6**

Tabuľka 4: Kontrolná skupina s heslom **A**

alebo 2) a šesťciferný dátum vo formáte `cccvd dmmrr`, kde `ccc` je číslo depeše, `v` je identifikátor použitého variantu substitučnej tabuľky, `dd` je deň, `mm` je mesiac a `rr` je rok odoslania depeše. Identifikátor použitej substitučnej tabuľky zvolíme tak, že nepárna cifra bude označovať prvý variant a párna druhý variant substitučnej tabuľky. Tieto prvé dve skupiny zamaskujeme rovnako, ako sa maskovalo heslo **A**. Predpokladajme, že depeša má číslo 67, pri šifrovaní sme použili prvý variant substitučnej tabuľky a depeša bola odoslaná 13. mája 1944. Potom prvé dve skupiny v otvorenom tvare môžu byť napríklad: `06731 30544`. Zamaskujú sa nasledovne:

Prvé dve skupiny:	0	6	7	3	1	3	0	5	4	4
Násobenie 3x:	0	8	1	9	3	9	0	5	2	2
Zvolená konštanta:	3	3	3	3	3	3	3	3	3	3
Kontrolná skupina:	**3**	**1**	**4**	**2**	**6**	**2**	**3**	**8**	**5**	**5**

Tabuľka 5: Prvé dve kontrolné skupiny depeše

Na začiatok depeše pridáme ešte návestie v tvare `GR xx`, kde `xx` je počet päťmiestnych skupín depeše. Konečná podoba našej depeše aj so služobnými údajmi (kontrolnými skupinami) potom bude:

```
GR 44
31426 23855 62904 84214 92543 46224 68541 47874 78301 49252
94287 22484 12008 87462 14243 48810 32147 23228 92522 44638
98820 29684 30949 29244 22887 29228 04281 88482 74887 81682
32147 88452 34527 06898 82786 60854 24725 26468 62080 28276
44386 25296 91506 08527
```

Prvé dve skupiny obsahujú číslo a dátum odoslania depeše, tretia skupina obsahuje identifikačné číslo šifranta, predposledná skupina obsahuje číselnú časť hesla **A** a posledná skupina depeše je poslednou skupinou zašifrovaného textu, pričom je náhodne doplnená na 5 cifier (v našom príklade sú doplnené posledné dve cifry). Týmto je depeša pripravená na odoslanie.

11.2 Postup pri šifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii text na šifrovanie.

b. Je dané päťznakové heslo **A**. Číselné heslo **A** zvolíme sami tak, aby pozostávalo z piatich rôznych cifier.

c. Vyberieme variant substitučnej tabuľky (1 alebo 2).

d. Je dané textové heslo **B**. Toto heslo by malo mať aspoň 15 znakov.

e. Je daná multiplikatívna konštanta. Z jednociferných čísel prichádzajú do úvahy len 1, 3, 7 a 9, pričom 1 nemá žiadny zmysel pre bezpečnosť šifrovania textu.

f. Je dané trojciferné identifikačné číslo šifranta.

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

h. Je daný dátum šifrovania.

Potom šifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Text, ktorý ideme šifrovať, prepíšeme pomocou znakov obsiahnutých v substitučnej tabuľke. To sú znaky medzinárodnej abecedy bez `Q` a `W` a znaky `Č`, `CH`, `Ř`, `Š`, `Ž`, `/`. Nahradíme písmená a vynecháme špeciálne znaky, ktoré sa v substitučnej tabuľke nevyskytujú.

2. Text rozdeľujeme na časti dlhé 100–200 znakov. Jednotlivé časti by nemali byť dlhšie než 10 až 20 násobok dĺžky hesla **B**, pretože sa jedná o šifru s periodickým heslom.

3. 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.

4. Podľa tabuľky 1 nahradíme znaky depeše číslami.

5. Ak počet cifier depeše nie je násobkom 5, na jej koniec náhodným spôsobom doplníme potrebný počet cifier.

6. Vytvoríme a zamaskujeme prvé dve skupiny depeše tak, ako je to popísané v texte a znázornené v tabuľke 5 na strane 7. Tieto dve skupiny obsahujú poradové číslo depeše, variant použitej substitučnej tabuľky a dátum odoslania depeše.

7. Vytvoríme a zamaskujeme tretiu skupinu depeše, obsahujúcu identifikačné číslo šifranta. Spôsob jej tvorenia a maskovania je znázornený v tabuľke 3 na strane 6.

8. Vytvoríme a zamaskujeme kontrolnú skupinu s číselným heslom **A**. Postup je znázornený v tabuľke 4 na strane 7. Túto skupinu umiestnime ako predposlednú skupinu depeše.

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

11.3 Postup pri dešifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii kompletný text zašifrovanej depeše.

b. Je dané päťznakové heslo **A**.

c. Je dané textové heslo **B**.

d. Je daná multiplikatívna konštanta.

Potom dešifrovanie depeše bude prebiehať v nasledovných krokoch:

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

2. Z prvých dvoch skupín depeše zistíme číslo depeše, variant použitej substitučnej tabuľky a dátum odoslania depeše. Tieto skupiny sú v tvare `cccvd dmmrr`. Maskovanie týchto skupín je predvedené v tabuľke 5 na strane 7. Ak je `v` nepárne, bol použitý prvý a ak párne, tak druhý variant substitučnej tabuľky.

3. Z tretej skupiny depeše zistíme identifikačné číslo šifranta. Maskovanie tejto skupiny je predvedené v tabuľke 3 na strane 6.

4. Z predposlednej skupiny depeše zistíme číselnú časť hesla **A**. Maskovanie tejto skupiny je predvedené v tabuľke 4 na strane 7.

5. Vynecháme návestie, prvé tri a preposlednú skupinu depeše a môžme zostaviť príslušnú substitučnú tabuľku **A** s rozmermi 3x10.

6. Podľa substitučnej tabuľky vytvoríme číselnú podobu hesla **B**. Toto číselné heslo potom periodicky zapíšeme pod cifry depeše.

7. Dešifrujeme číselnú podobu depeše. Najskôr invertujeme násobenie dohodnutou konštantou a potom odčítame cifry periodického hesla od cifier depeše. Všetky operácie sa robia modulo 10.

8. Podľa substitučnej tabuľky prevedieme číselnú depešu na textovú. Pri tomto na konci depeše môžu vzniknúť až 2 náhodné znaky v dôsledku dopĺňania počtu cifier na násobok 5. Ani séria nepredstavuje žiaden problém, pretože tieto náhodné znaky budú až za znakmi označujúcimi nádväznosť, takže ich ľahko identifikujeme.

9. Ak sa jedná o sériu, okrem prvej a poslednej majú všetky časti na začiatku a na konci znaky určujúce nadväznosť častí. Prvá časť má tieto znaky len na konci a posledná len na začiatku. Text depeše teda zostavíme v správnom poradí podľa označenia na začiatku a konci jednotlivých častí série.

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

11.4 Lúštenie

Na základe rôznych indícii sa zdá, že šifru „Palacký“ nevymysleli Moravcovi spravodajci v Londýne, ale že pochádza odinakiaľ. Použitá substitučná tabuľka sa ako svojou abecedou, tak konštrukciou a tvarom (rozmer 3x10) líši od substitučných tabuliek, ktoré sa používali pri iných československých šifrách. Podobne aj násobenie konštantou sa nevyskytuje pri žiadnej inej nám známej československej šifre z inkriminovaného obdobia. A napokon táto šifra sa nepoužívala pri spojení medzi Londýnom a nejakou ich expozitúrou, prípadne výsadkom, ale pri spojení medzi Moskvou a Slovenskom. Každopádne sa ale jedná o československú šifru z obdobia 2. svetovej vojny, a preto sa ňou zaoberáme.

Šifra „Palacký“ je typu SPN. Šifry typu SP neboli nič nového a používala ich aj exilová vláda v Londýne. Nové je len použitie multiplikatívnej konštanty po aplikovaní periodického hesla. To však bezpečnosť šifry nijako

nezvýšilo. Podľa informácii z [2] sa zdá, že multiplikatívna konštanta sa volila jednociferná, aj keď to nemáme overené a potvrdené z iných zdrojov. V takom prípade by voľba multiplikatívnej konštany bola dosť obmedzená. Musí byť totiž zabezpečená jednoznačná dešifrovateľnosť. Takže z jednociferných čísel ako multiplikatívna konštanta prichádzajú do úvahy len čísla 1, 3, 7 alebo 9, pričom voľba 1 je zjavne úplne zbytočná. Takže lúštiteľovi, aby sa zbavil multiplikatívnej konštanty, stačí overiť len tri čísla! Potom mu už zostane len text zašifrovaný šifrou typu SP.

V [5] na stranách 304–313 pán Janeček na príklade autentických depeší ukazuje postup lúštenia šifier typu STP, ktoré používala exilová vláda v Londýne pri spojení so svojím agentom v Marseille. Ten istý postup sa dá aplikovať aj na šifry typu SP. Tam je to ešte jednoduchšie, pretože odpadá lúštenie transpozičnej časti. V šifre „Palacký“ je síce použitá iná substitučná tabuľka, ale to nie je podstatné. Postup odhalenia periodického hesla je presne ten istý ako ho popisuje pán Janeček v [5] na stranách 306–307. Po odhalení a odstránení periodického hesla zostáva už len jednoduchá substitúcia a tú vedeli lúštiť už Arabi v stredoveku.

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. Má zmysel používať autokľúč?

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

Abstrakt

Text stručne popisuje šifrovanie s použitím autokľúča a ukazuje ako sa dá takto zašifrovaný text lúštiť rovnako jednoduchým spôsobom ako šifry s periodickým heslom.

1 Označenia

V texte budeme pomocou OT, resp. malými písmenami $(a_1, a_2, ...)$, označovať otvorený (nezašifrovaný) text. Pomocou ZT, resp. veľkými písmenami $(Z_1, Z_2, ...)$, budeme označovať zašifrovaný text. Pojmy heslo, kľúč, inicializačný kľúč, inicializačné heslo budú mať v texte identický význam. Označujeme nimi tajnú postupnosť znakov, ktorá vstupuje ako premenná zložka do procesu šifrovania a dešifrovania. Heslo (kľúč) budeme v texte označovať písmenami $(k_1, k_2, ...)$. Na záver ešte poznámka: šifry s autokľúčom sa zvyknú označovať aj pojmom *autokláv*.

2 Úvod

Trvalo veľmi dlho kým sa ľudia v kryptografii prepracovali k používaniu polyalfabetických šifier a šifier s periodickým heslom. Tieto zlepšili bezpečnosť v porovnaní s monoalfabetickými šiframi a veľmi dlho boli považované za nerozlúštiteľné. Prvým pokusom v Európe bol v tomto smere Albertiho disk v 15. storočí ([2], 127-128). Táto, na svoju dobu, veľmi dobrá a progresívna šifra sa žiaľ neujala a na veľmi dlho upadla do zabudnutia. Ďalším pokusom bola Trithemiova *tabula recta* v 16. storočí ([2], 136). Trithemiova šifra bola podstatne slabšia než Albertiho disk, pretože heslo pozostávalo z usporiadanej abecedy. Tento nedostatok ešte v roku 1553 napravil Belaso, keď zaviedol používanie periodického hesla ([2], 137). Ako ďalší v poradí sa o rozvoj polyalfabetických šifier zaslúžil takisto v 16. storočí Porta, ktorý vylepšil Albertiho disk a skombinoval ho s ľahko zapamätateľným periodickým heslom Belasa ([2], 141-142). Porta zároveň použil neusporiadané abecedy, čo komplikovalo lúštenie. Už v čase vzniku polyalfabetických šifier sa vyskytli pokusy o ich kryptoanalýzu. Sám Porta v jednej svojej práci takmer objavil univerzálnu

metódu lúštenia šifier s periodickým heslom. Žiaľ, len takmer. Napokon túto metódu ako prvý publikoval až v 19. storočí major pruskej armády Kasiski ([2], 207-208). Už v 16. storočí ale bolo intuitívne známe, že čím dlhšie bude heslo, tým silnejšia bude šifra. A samozrejme by sa nemalo rovnaké heslo používať pre viacero depeší. Preto by bolo vhodné ak by sa dalo heslo nejako odvodiť priamo z textu depeše. Tým sa dostávame k pojmu *autokľúč*.

Prvý známy pokus o šifru s autokľúčom publikoval v roku 1550 Cardano ([2], 143-144). Jeho návrh mal ale viacero závažných nedostatkov. Okrem iného Cardano nepoužíval inicializačné heslo, resp. ako inicializačné heslo použil prvé písmená otvoreného textu. Ďalší, už použiteľný, pokus o autokľúč pochádza od Vigenèra a je z druhej polovice 16. storočia ([2], 147). Je iróniou osudu, že dnes sa väčšinou šifry s periodickým heslom označujú ako šifry Vigenèrovho typu. Pritom Vigenère nebol ich autorom a ani sa ku ich autorstvu nikdy nehlásil. On len študoval diela už uvedených autorov a písal o nich, pričom svoje zdroje riadne citoval. V jednej zo svojich prác popísal aj šifru s autokľúčom, ktorá používa inicializačné heslo. Popísal pritom obe varianty tejto šifry, t.j. autokľúč z OT aj autokľúč zo ZT. Nedostatkom jeho popisu bolo len to, že použil iba jednoznakové inicializačné heslo.

3 Autokľúč zo ZT

Teraz si v stručnosti ukážeme šifru s autokľúčom používajúcim ZT. V stručnosti preto, lebo táto šifra je veľmi slabá. Je podstatne slabšia než obyčajná šifra s periodickým heslom, a preto ju nemá zmysel používať. Napriek tomu ale v minulosti bola používaná, pretože laici k nej z psychologických dôvodov inklinujú.

Postup pri šifrovaní je nasledovný. Najskôr určíme inicializačné heslo. Nech toto inicializačné heslo pozostáva z n znakov $k_1, k_2, ..., k_n$. Pod prvých n znakov OT napíšeme inicializačné heslo a do ďalšieho riadku súčet znakov OT so zodpovedajúcimi znakmi hesla tak, ako sa to robí aj pri šifrách s periodickým heslom. Rozdiel nastane až pri $(n+1)$-vom znaku. Tam totiž nebudeme opakovať samotné heslo ako pri šifrách s periodickým heslom, ale začneme opisovať znaky ZT. Postup je zrejmý z nasledujúceho obrázku:

a_1	a_2	...	a_n	b_1	b_2	...	b_n	c_1	c_2	...	c_n	.....
k_1	k_2	...	k_n	Z_1	Z_2	...	Z_n	Z_{n+1}	Z_{n+2}	...	Z_{2n}	.....
Z_1	Z_2	...	Z_n	Z_{n+1}	Z_{n+2}	...	Z_{2n}	Z_{2n+1}	Z_{2n+2}	...	Z_{3n}	.....

Na obrázku sú znaky OT a ZT rozdelené na n-tice len kvôli prehľadnosti. Vidíme, že prvá n-tica znakov OT je šifrovaná znakmi hesla, druhá n-tica znakov OT je šifrovaná prvou n-ticou znakov ZT, atď. Šifrovanie sa pritom realizuje bežným cyklickým sčítaním znakov. V 26-znakovej telegrafnej abecede (TSA) by teda platilo:

$$Z_1 = (a_1 + k_1) \bmod 26 \ , Z_2 = (a_2 + k_2) \bmod 26 \ , ...$$

Slabina tejto šifry je hneď zrejmá. Pokiaľ „uhádneme“ dĺžku hesla, tak máme k dispozícii priamo šifrovací kľúč a celý ZT, okrem prvých n znakov, môžme dešifrovať a nemusíme nič lúštiť. Pri krátkych inicializačných heslách (napr. 1-znakových ako použil vo svojom popise Vigenère) je veľmi pravdepodobné, že inicializačné heslo uhádneme z kontextu.

Túto časť teda môžme uzavrieť konštatovaním, že autokľúč zo ZT je veľmi slabá šifra a zmysel by mohol mať jedine v prípade, ak by dĺžka inicializačného hesla bola blízka dĺžke OT. To by potom bolo po prvé veľmi nepraktické a po druhé by to už takmer bola iná šifra[1].

4 Autokľúč z OT

Autokľúč používajúci OT má už aj svoj praktický význam a bol veľmi často používaný v praxi. Šifrovanie prebieha podobne ako pri autokľúči zo ZT. Začíname šifrovať n-znakovým inicializačným heslom rovnako ako v predošlom prípade. Keď vyčerpáme všetky znaky hesla, pokračujeme v šifrovaní znakmi OT, čo je jediný rozdiel oproti autokľúču zo ZT. Tento rozdiel je ale veľmi dôležitý a má podstatné dôsledky pre bezpečnosť šifry. Postup šifrovania je ilustrovaný na obrázku:

a_1	a_2	...	a_n	b_1	b_2	...	b_n	c_1	c_2	...	c_n	.....
k_1	k_2	...	k_n	a_1	a_2	...	a_n	b_1	b_2	...	b_n	.....
Z_1	Z_2	...	Z_n	Z_{n+1}	Z_{n+2}	...	Z_{2n}	Z_{2n+1}	Z_{2n+2}	...	Z_{3n}	.....

Na obrázku sú opäť OT a ZT rozdelené na úseky dĺžky n pre lepšiu prehľadnosť. Vidíme, že prvá n-tica znakov OT je šifrovaná inicializačným heslom, druhá prvou n-ticou znakov OT, tretia druhou n-ticou znakov OT, atď.

[1] Táto „iná šifra“ sa označuje ako OTP, čiže One Time Pad. V prípade OTP je dĺžka hesla presne rovnaká ako dĺžka OT a v prípade, že heslo pozostáva z dokonale náhodnej postupnosti znakov a nepoužíva sa opakovane, je táto šifra absolútne bezpečná.

Výhoda tohto šifrovania, v porovnaní s autokľúčom zo ZT, spočíva v tom, že prípadný útočník nedostane so ZT do rúk rovno aj šifrovací kľúč, alebo jeho časť. Je zrejmé, že sila tejto šifry bude aspoň taká ako je sila šifry s periodickým heslom.

5 Lúštenie

Budeme predpokladať, že útočníkovi sa dostal do rúk ZT a vie (alebo predpokladá), že sa jedná o text zašifrovaný autokľúčom, pričom nepozná inicializačné heslo ani jeho dĺžku. Postup lúštenia autokľúča zo ZT je veľmi jednoduchý a dá sa vybaviť pár vetami v nasledujúcom odstavci. Potom sa budeme venovať už len autokľúču z OT.

Pri autokľúči zo ZT stačí aby útočník „hádal“ dĺžku inicializačného hesla. Znaky ZT budeme písať pod znaky ZT s posunom postupne $1, 2, 3, ..., n$. Ak uhádne dĺžku n inicializačného hesla, pri dešifrovaní dostane zmysluplný OT od znaku $(n + 1)$ až po koniec textu. Ak bude mať šťastie, tak z kontextu môže spätne zrekonštruovať alebo uhádnuť aj prvých n znakov OT a z toho následne aj použitý inicializačný kľúč.

Lúštenie autokľúča z OT je trocha komplikovanejšie, pretože útočník nemá k dispozícii heslo, ani žiadnu jeho časť. Môže ale hádať dĺžku inicializačného hesla. Bude postupne skúšať dĺžky $1, 2, 3, ..., n$. To, na čo mu to bude dobré vidno z nasledovného obrázku:

a_1	a_2	...	a_n	b_1	b_2	...	b_n	.....
k_1	k_2	...	k_n	a_1	a_2	...	a_n	.....
$a_1 + k_1$	$a_2 + k_2$	...	$a_n + k_n$	$b_1 + a_1$	$b_2 + a_2$	...	$b_n + a_n$	.....

Je to tabuľka zobrazujúca šifrovanie prvý dvoch n-tíc znakov pomocou autokľúča s OT. Súčty sú samozrejme cyklické, t.j. pre abecedu s 26 znakmi sú všetky súčty mod 26. Pokiaľ útočník uhádne dĺžku inicializačného hesla n, môže odčítať prvú n-ticu ZT od druhej, potom túto už upravenú druhú n-ticu znakov od tretej atď. Dostane potom nasledovnú postupnosť znakov:

$$(a_1 + k_1)(a_2 + k_2)...(a_n + k_n)\ (b_1 - k_1)(b_2 - k_2)...(b_n - k_n)\ (c_1 + k_1)(c_2 + k_2)...(c_n + k_n)\ ...$$

Ako vidno, prvá n-tica znakov OT je zašifrovaná heslom $(k_1, k_2, ..., k_n)$, druhá n-tica OT je zašifrovaná heslom $(-k_1, -k_2, ..., -k_n)$, tretia opäť heslom $(k_1, k_2, ..., k_n)$ atď. Dostali sme vlastne šifru s periodickým heslom:

$$(k_1, k_2, ..., k_n, -k_1, -k_2, ..., -k_n)$$

Takže ZT zašifrovaný autokľúčom z OT sme previedli na ZT zašifrovaný periodickým heslom. Pritom ak dĺžka inicializačného hesla bola n, dĺžka periodického hesla bude $2n$. Prvých n znakov je totožných s inicializačným heslom a druhých n znakov je tvorených inverznými hodnotami znakov inicializačného hesla. Lúštenie ZT zašifrovaného autokľúčom z OT sa týmto redukuje na lúštenie ZT zašifrovaného periodickým heslom.

Texty zašifrované periodickým heslom vieme rozpoznať a lúštiť. Prvé sporadické lúštenia šifier s periodickým heslom sú známe už zo 16. a 17. storočia. Prvé systematické úspechy s ich lúštením mal a v druhej polovici 19. storočia ich aj publikoval pruský dôstojník Kasiski. Metódy lúštenia šifier s periodickým heslom ďalej zdokonalilo viacero ďalších kryptológov a celý tento proces bol zavŕšený v dvadsiatych rokoch 20. storočia Friedmanom. Zjednodušene sa dá povedať, že úspešnosť vylúštenia ZT zašifrovaného pomocou periodického hesla závisí na pomere dĺžky ZT a dĺžky použitého hesla. Čím je tento pomer väčší, tým je väščia aj šanca na vylúštenie zašifrovaného textu.

6 Záver

Odpoveď na otázku z názvu článku je neurčitá. Bratislavčan by to vyjadril slovami *„Es kommt darauf an...“* a môžme to rozdeliť na dve samostatné časti.

Autokľúč zo ZT určite nemá zmysel používať, pokiaľ by dĺžka hesla bola významne kratšia než je dĺžka samotného textu, pretože inak by útočník dostal so ZT do rúk aj šifrovacie heslo a väčšinu textu by si mohol dešifrovať bez akejkoľvek námahy s lúštením.

Autokľúč z OT je oproti klasickej šifre s periodickým heslom silnejší len v tom zmysle, že zdvojnásobuje efektívnu dĺžku hesla. Čiže pomer dĺžky textu a hesla klesne na polovicu, čo v istých prípadoch môže byť práve rozdiel medzi zašifrovaným textom, ktorý vieme, resp. nevieme vylúštiť[2]. Takže pri rovnakom texte a rovnakom periodickom hesle, resp. inicializačnom hesle pre autokľúč z OT je varianta s autokľúčom bezpečnejšia (pokiaľ sa máme rozhodnúť len medzi týmito dvoma možnosťami). Samozrejme v súčasnej dobe sú už obe tieto šifry dávno prekonané a zaujímavé sú už len z historického a pedagogického hľadiska. Používajú sa zväčša už len v úlohách pre študentov a v rôznych kryptosúťažiach.

[2]Samozrejme ak neuvažujeme aj iné metódy lúštenia ZT, ako je znalosť časti OT, znalosť časti použitého hesla, predpokladaný text a pod.

Literatúra

[1] Grošek, O., Vojvoda, M., Zajac, P.: Klasické šifry, *STU v Bratislave, 2007*

[2] Kahn, D.: The Codebreakers, *Scribner, 1996*, pp. 125-156

Portov šifrovací disk
Zdroj: `http://hiwaay.net/~paul/cryptology/portadisc.html`

C. Slabý generátor náhodných čísel umožňuje faktorizovať RSA moduly

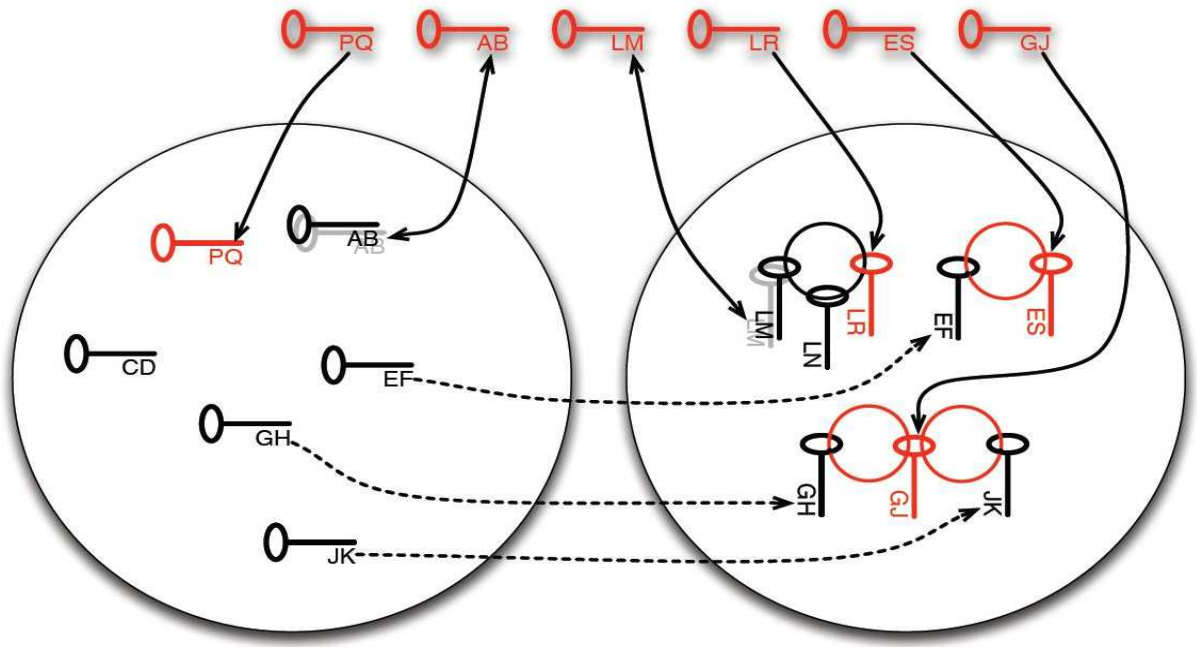
Ondrej Mikle, výzkumná a vývojová v Laboratoř CZ.NIC, ondrej.mikle@gmail.com

Místo úvodu (P.Vondruška)

Osobně považuji za jeden z nejzajímavějších výsledků současné kryptologie (a navíc s dopadem do praktické infomrační bezpečenosti) objev K.Lenstry a jeho kolegů, který byl začátkem ledna publikován v článku **Ron was wrong, Whit is right** autorů Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, a Christophe Wachter. Článek je uložen ve volně dostupném archívu IACR http://eprint.iacr.org/2012/064.pdf

Ihned po jeho publikování se na Internetu objevila řada výkladů a interpretací. Bohužel ne vždy zcela přesných a někdy dokonce lehce zavádějících, protože autoři často dovozovali o něco více než v článku skutečně je.

Hlavní myšlenka článku je poměrně jednoduchá. K jejímu vyložení použijeme obrázek z originálního Lenstrova článku. Při vyšetřování modulů RSA tým zjistil, že v sebraném velkém vzorku existuje statisticky neočekávané množství modulů, které mají společného dělitele.



Pokud známe faktorizaci jednoho z modulů z množiny modulů se společný dělitelem, pak zcela triviálně samozřejmě umíme faktorizovat postupně všechny moduly z této množiny. Příklad z obrázku: X= L*M , Y=L*N , Z=L*R. Ze znalosti faktorizace modulu X na prvočísla L, M postupně snadno faktorizujeme modul Y a nakonec modul Z.

Jednu z velice dobrých a přesných interpretací tohoto článku sepsal Ondrej Mikle. Jeho krátký článek je přitom o to cennější, že vyšel již 16. 2. 2012 a to konkrétně na blogu nic.cz http://blog.nic.cz/ . Vyšel tedy v době, kdy na Internetu nebylo k dispozici mnoho kvalitních rozborů a naopak se zde našly spíše spekulace a poněkud nepřesné interpretace výsledků. Samozřejmě tyto články byly často doplněné i o některé konspirační teorie. Ovšem není šprochu, aby v něm nebylo pravdy trochu. Takže alespoň jedna konspirativní teorie k zamyšlení. Je všeobecně známo, že v USA se algoritmus RSA nemohl dlouho prosadit a NIST naopak zařadil mezi sadu bezpečných algoritmů pouze asymetrický algoritmus DSA a nikoliv RSA. Toto se dosud vysvětlovalo tím, že do roku 2000 byl algoritmus RSA na území USA a Kanady patentován, a proto se zde spíše preferoval algoritmus DSA. Jenže, co když to je úplně jinak? Co když „slabost“ generátoru velkých prvočísel použitá v OS (zejména Windows) a aplikacích byla NISTu (a spíše jiným „třípísmenkovým organizacím již tehdy známa), a proto byl jednoznačně preferován algoritmus DSA a Lenstrou objevená vlastnost, která za jistých okolností může být využita k faktorizaci „příbuzných“ RSA modulů, již jim byla známa…

Z výše uvedených důvodu jsem chtěl do e-zinu Crypto-World získat rozbor tohoto Lenstrova objevu abych s ním mohl čtenáře blíže seznámit.

Uvítal jsem proto souhlas, který Ondrej Mikle udělil a povolil nám otisknout v plném znění jeho článek.

Těm, který tento jeho krátký článek „nestačí“ si dovolím doporučit ještě jiný článek, který mne při shánění podkladů k tomuto objevu zaujal. Je to tentokráte poměrně rozsáhlý článek **Understanding Common Factor Attacks: An RSA-Cracking Puzzle** http://www.loyalty.org/~schoen/rsa/ . V článku se také uvádí poměrně přesně problém s nekvalitně generovanými prvočísly pro algoritmus RSA, ale navíc je zde pro nadšence (typu luštitelů soutěží našeho e-zinu) uvedena výzva. Můžete si stáhnout data obsahující 100 veřejných klíčů pro RSA a 100 odpovídajících

zašifrovaných zpráv. Součin prvočísel má délku 1024 bitů. Asi tušíte, že díky sdíleným modulům je možné provést faktorizaci a dešifraci.

Nyní již předám slovo Ondrejovi .

Slabý generátor náhodných čísel umožňuje faktorizovať RSA moduly (O. Mikle)

Akoby nestačilo napadnutie certifikačných autorít v roku 2011 a nedávne priznanie Trustwave, že vydávala certifikáty na korporátne man-in-the-middle útoky, našla sa ďalšia trhlina spôsobená nesprávnou implementáciou generátora náhodných čísel (kauza s debianími slabými kľúčmi bola podobne spôsobená chybou v náhodnom generátore).

Tým výskumníkov vedený A. Lenstrom z EPFL našiel v databáze certifikátov z SSL Observatory a iných zdrojoch ďalšie páry kľúčov, ktoré zdieľajú v RSA module prvočíslo. To znamená, že použitím obyčajného vyše 2000 rokov starého Euklidovho algoritmu je možné niektoré RSA moduly faktorizovať. Z ich výsledkov vyplýva, že zhruba 2 z 1000 kľúčov idú týmto spôsobom faktorizovať! Testovali celkovo 11.7 milióna RSA, ElGamal, DSA a ECDSA kľúčov, z toho šlo uvedenou metódou prelomiť cca 27 000 RSA kľúčov.

DSA a ElGamal kľúče nevykazovali žiadne podobné štatistické anomálie, ECDSA kľúč bol len jeden. Z uvedeného sa dá usudzovať, že PGP a GnuPG slabým generátorom netrpia (pretože väčšina testovaných ne-RSA kľúčov bola vygenerovaná jedným z týchto softwarov). Zatiaľ sa nevie, ktoré implementácie vygenerovali zmienené slabé RSA kľúče.

V diskrétnom grafe použitom na modelovanie zdieľaných prvočísiel a modulov je prvočíslo reprezentované vrcholom, hrana spája dve prvočísla patriace k modulu (moduly s viacerými prvočíslami neboli nájdené). V ideálnom prípade by vrcholov malo byť dvakrát toľko čo hrán, tj. žiadny pár RSA modulov nezdieľa prvočíslo. V Lenstrových výsledkoch sa ale nachádza 1995 nesúvislých komponent s tromi a viac vrcholmi.

Preložené do „nematematičtiny“: existuje 1995 skupín po niekoľkých RSA kľúčoch, kde keď poznáte prvočísla aspoň jedného z vrcholov, môžete faktorizovať ostatné. Rovnako znalosť dvoch modulov z rovnakej skupiny umožňuje použiť Euklidov algoritmus na zistenie jedného z prvočísiel a teda faktorizovanie oboch modulov.

Lenstra tiež zmieňuje dlhšie známy fakt o zdieľaní RSA modulov v X.509 SSL/TLS certifikátoch. Podľa jeho údajov 4 % kľúčov sú zdieľané, často medzi nesúvisejúcimi organizáciami alebo jedincami. Časť „s nesúvisejúcimi organizáciami“ ale treba brať trocha s rezervou.

O zdieľaní kľúčov v certifikátoch som mal pár debát s rôznymi výskumníkmi, napríklad s Ralphom Holzom, ktorého práca SSL Landscape je spomínaná v Lenstrovom príspevku. Obaja sme našli rôzne kľúče zdieľané medzi zdanlivo nesúvisejúcimi stranami, ale keď sa človek do toho začal vŕtať viac, tak zistil, že nejak prepojené sú (ale to treba robiť ručne prehliadaním obchodných registrov, atp.). Napriek tomu existujú kľúče ktoré sú zdieľané medzi organizáciami bez toho, aby to bolo úmyselné (napríklad niekto nezmení na VPS hostingu SSH/SSL kľúče, ktoré sa nakopírujú z inštalačného obrazu).

Podľa iného článku sa problém týka hlavne embedded zariadení, ktoré majú pri generovaní kľúčov malý zdroj entropie, takže netreba až tak moc panikáriť. Linkovaný článok obsahuje veľa technických podrobností, hlavná pointa je, že najskôr sa to netýka internetového bankovníctva a iných vysoko citlivých aplikácií.

Záujemcov o podrobnosti odkážem na pôvodný príspevok od Lenstra, et al publikovaný na eCrypt archíve.

D. Call for Papers - Mikulášská kryptobesídka

29. – 30. listopad 2012, Praha
http://mkb.buslab.org

Základní informace

Mikulášská kryptobesídka přichází už podvanácté. 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 *29. listopadu* a (b) půldne prezentací příspěvků a diskusí v pátek *30. listopadu 2012*. Pro workshop jsou domluveny zvané příspěvky:

- David Naccache (ENS, Francie) & Zdeněk Říha (FI MU): *Statistická zrychlení pro biometriky.*
- Karsten Nohl (nezávislý výzkumník, SRN): *Téma je domlouváno*.
- Andreas Uhl (Univerzita Salzburg): *Watermarking in Biometrics*.
- Vlastimil Klíma (KNZ): *SHA-3 a lehká kryptografie*.
- Michal Šrámka (STU Bratislava): *Achieving Privacy of Shared Information: Crypto & Beyond*.
- Klaus Schmeh (spisovatel, SRN): *Lámání zpráv Enigmy z 2. světové války*.

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 tak, aby přišly nejpozději do *1. října 2012*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2012 – 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 *29. října*. Příspěvek pro sborník workshopu pak musí být dodán do *12. listopadu*.

Důležité termíny

Návrhy příspěvků:	1. října 2012
Oznámení o přijetí/odmítnutí:	29. října 2012
Příspěvky pro sborník:	12. listopadu 2012
Konání MKB 2012:	29. – 30. listopadu 2012

Programový výbor

Dan Cvrček, Smart Architects, UK
Otokar Grošek, STU, Bratislava , SK
Jan Krhovják, Cepia Technologies, CZ
Vašek Matyáš, FI MU, Brno, CZ – předseda
Zdeněk Říha, FI MU, Brno, CZ
Luděk Smolík, Siegen, DE
Martin Stanek, UK, Bratislava, SK
Pavel Vondruška, Telefónica O2 & UK, CZ

Mediální partneři

E. 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.

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

Rozvrh

Datum	Čas	Lektor	Volná místa	Přihlásit
18.-19.04.2012	09:00–17:00	Pavel Vondruška	15	

Cena

Základní cena: 4 000,00 Kč
Základní cena včetně DPH: 4 800,00 Kč

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

F. O čem jsme psali v březnu 2000 – 2011

G. 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