Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 13, číslo 9/2011 **15. září**

9/2011

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1345 registrovaných odběratelů)

Obsah :

A. Československé šifry z obdobia 2. svetovej vojny Diel 8., Šifra „Marta“

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.

8 Šifra „Marta“

Šifra „Marta“ je typu SP. Jedná sa o substitúciu znakov dvojcifernými číslami a následné prešifrovanie pomocou autoklúča vigenérovho typu. Popis tejto šifry je uvedený v knihe [2] (str. 127). Označenie „Marta“ s najväčšou pravdepodobnosťou nie je pôvodný názov tejto šifry. Jedná sa o meno rádiostanice v operácii Barium, ktorá túto šifru používala. Šifra mala zrejme označenie niektorým rímskym číslom, podobne ako iné ČS šifry. Toto sa ale v [2] nespomína.

8.1 Všeobecný popis a príklad šifrovania depeší

Pri tejto šifre sa text, ktorý sa mal zašifrovať, najskôr prepísal do číselnej podoby pomocou 49 znakovej substitučnej tabuľky. V [2] táto substitučná tabuľka nie je bližšie špecifikovaná, ale podľa uvádzaného príkladu by to mohla byť napríklad tabuľka 1 uvedená na strane 3. Je to tabuľka takmer identická s tabuľkou použitou v „rímskej desať“. Rozdieľ je len v kódovaní cifier, ktoré sú usporiadané v poradí 0 až 9, aby zodpovedali uvedenému príkladu. Ukážeme si teraz postup šifrovania na konkrétnom príklad. V niektorých detailoch, na ktoré upozorníme, sa ale bude náš postup mierne líšiť od príkladu uvádzaného v [2]. Na šifrovanie si vyberieme napríklad text:

Ostatně se domívám, že je potřeba zničit Kartágo.
(Cato starší)[1]

[1] Pôvodná verzia v latinčine: *Ceterum autem censeo Cartaginem esse delendam. Marcus Porcius Cato*

	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 šifru „Marta“

Tento text prepíšeme pomocou znakov obsiahnutých v substitučnej tabuľke 1. Špeciálne znaky, ktoré sa v tejto tabuľke nenachádzajú, vynecháme. Slová sa oddeľujú buď medzerou, alebo špeciálnym znakom. Takže za špeciálnymi znakmi medzery vynechávame. Po tejto úprave dostaneme text:

```
OSTATNĚ SE DOMNIVAM,ŽE JE POTREBA ZNIČIT KARTAGO.
```

V tomto texte potom podľa substitučnej tabuľky nahradíme znaky ich číselnou reprezentáciou. Medzery medzi slovami sa nahrádzali ciframi `7, 8` alebo `9`. Takto dostaneme číselnú podobu textu:

```
18232 50125 17077 23068 05181 61712 27011 63532 06913 06719
18252 10602 01831 17120 41225 91401 21250 10918 33
```

Depeše, ktorých počet cifier nebol násobkom 5, sa zrejme doplňovali potrebným počtom náhodných cifier. Najbezpečnejšie by bolo doplniť ich ciframi označujúcich medzeru, t.j. `7, 8` alebo `9`, na konci číselnej podoby depeše.

Pokiaľ ide o služobné údaje, v [2] sa spomína, že boli obsiahnuté v prvej skupine (pred textom) a v poslednej skupine (za textom). Nevieme o nich nič bližsie, ani čo všetko obsahovali, ani ako sa kódovali. Ale pravdepodobne obsahovali informáciu o termíne nasledujúcej relácie. V našom príklade služobné údaje nebudeme pridávať.

Takisto sa v [2] neuvádza nič o rozdeľovaní dlhších depeší. Z uvádzaného príkladu ale vyplýva, že depeše sa rozdeľovali na kratšie časti a znaky označujúce nadväznosť obsahovali namiesto písmen abecedy čísla. Je to síce možné, ale pravdepodobnejšie je, že sa jedná o chybu pána Hanáka. Čísla namiesto písmen v znakoch nadväznosti síce nie sú žiaden problém, ale pri tejto šifre sa zrejme text vôbec nezvykol rozdeľovať. Prvý dôvod je ten, že celá táto šifra je navrhnutá dosť amatérskym spôsobom a jej autor pravdepodobne autokľúč považoval za dosť bezpečný na to, aby text nebolo treba rozdeľovať. To je „psychologický“ dôvod. Druhý dôvod je ten, že ak sa v prípade tejto šifry text

rozdeľuje na časti a máme viacero častí zašifrovaných tým istým heslom (čo by sme mali), potom to výrazne zníži už aj tak dosť nízku bezpečnosť tejto šifry a uľahčí prácu lúštiteľom. Toto je odborný argument proti rozdeľovaniu textu depeší a ešte sa neskôr k nemu vrátime. To ale predpokladá odborné znalosti zo strany autora šifry, čo je v rozpore s prvým dôvodom.

Náš príklad je aj tak príliš krátky na to, aby sa delil na ešte kratšie časti. Takže ho uvedieme bez rozdeľovania a v popise šifrovania spomenieme potom aj rozdeľovanie textov tak, ako to vyplýva z príkladu v [2].

Na prešifrovanie autokľúčom sa používalo heslo, ktoré malo mať aspoň 17 znakov. Podľa informácii z [2] boli pre túto šifru určené 2 základné heslá[2]:

1. *Aj, zde leží zem ta před okem mým slzy ronícím.*
   pre 1. až 15. deň mesiaca

2. *Dříve kolébka, nyní národu mého rakev.*
   pre 16. až 31. deň mesiaca

Denné heslo sa z týchto základných hesiel tvorilo tak, že začínalo písmenom zodpovedajúcim dňu šifrovania. Denné heslo muselo mať aspoň 17 písmen a pokiaľ sedemnáste písmeno padlo doprostred slova, vzalo sa celé toto slovo. Denné heslo sa vyčíslilo obvyklým spôsobom, pričom medzery a interpunkčné znamienka sa nevyčíslovali. V príklade v [2] je pravdepodobne opäť chyba, pretože heslo sa tam vyčísluje podľa medzinárodnej abecedy. Podľa popisu iných šifier používaných československou vládou v Londýne je pravdepodobnejšie, že sa heslo vyčíslovalo podľa tej istej abecedy, podľa ktorej sa robila aj substitúcia. Takže vyčíslenie sa zrejme robilo podľa abecedy z tabuľky 1. Predpokladajme, že depešu v príklade budeme šifrovať 10. deň v mesiaci. Potom denné heslo a jeho vyčíslenie budú:

Z	E	M	T	A	P	Ř	E	D	O	K	E	M	M	Y	M	S	L	Z	Y
19	3	8	16	1	13	14	4	2	12	6	5	9	10	17	11	15	7	20	18

Teraz už len zostáva prešifrovanie zprávy v číselnej podobe autoklúčom. Šifrovanie autokľúčom (autokláv) vigenérovho typu môže mať v zásade dve formy. V oboch najskôr začneme dohodnutým heslom a keď ho vyčerpáme, k šifrovanému textu buď pričitávame samotný text v otvorenej podobe, alebo už zašifrovaný text. Ak dáme možnosť voľby laikovi, vo väčšine prípadov sa asi rozhodne pre pričitávanie už zašifrovaného textu, pretože ten napohľad vyzerá ako náhodná postupnosť znakov. Toto je opäť „psychologický“ argument, ale väčšinou to tak funguje a fungovalo to tak aj v prípade autora tejto šifry. Žiaľ je to tá výrazne horšia možnosť z uvedených dvoch alternatív. Takto totiž dáme prípadenému lúštiteľovi do rúk priamo šifrovací kľúč. Pokiaľ už

[2]Ján Kollár: *Slávy dcéra*

pozná typ šifry, okrem úvodnej časti depeše, šifrovanej denným heslom, si celý zvyšok depeše môže bez problémov prečítať a nemusí nič lúštiť.

Prešifrovanie autokľúčom sa robilo tak, že pod text v číselnej podobe, už doplnený tak, aby počet cifier bol násobok 5, sa najskôr napísali cifry vyčísleného denného hesla. Potom sa spravil súčet cifier textu s ciframi hesla modulo 10. Tým dostaneme začiatok zašifrovanej depeše. Tam, kde končí vyčíslené heslo, budeme pokračovať ciframi zašifrovanej depeše od jej začiatku potiaľ, pokiaľ bude potrebné. Takže v príklade bude mať prešifrovanie nasledovnú podobu:

Text:	18	232	50125	17	077	23068	05	181	61	712	27011	63532	06913	06719
Kľúč:	**19**	**381**	**61131**	**44212**	**65910**	**17111**	**57201**	**8**2751	31125	65128	98897
Depeša:	27	513	11256	51	289	88978	12	292	18	913	09762	94657	61031	94506

Text:	18252	10602	01831	17120	41225	91401	21250	10918	33978
Kľúč:	81229	21891	30976	29465	76103	19450	69947	13149	33170
Depeša:	99471	31493	31707	36585	17328	00851	80197	23057	66048

V prvej časti tabuľky sú tučným písmom vyznačené cifry vyčísleného denného hesla. Ďalšie cifry kľúča sú potom už cifry zašifrovanej depeše od jej začiatku.

Týmto je šifrovanie depeše ukončené. V [2] sa spomína, že následne sa mohla ešte robiť spätná substitúcia cifier na znaky medzinárodnej abecedy a že substitučné tabuľky pre spätnú substitúciu boli rôzne a že sa tvorili nejakým spôsobom z pridelených hesiel. Zrejme to bolo niečo podobné ako pri šifre „rímska deväť“, ale žiadne podrobnosti nepoznáme, takže spätnú substitúciu robiť nebudeme.

Na záver ešte k zašifrovanej depeši pridáme návestie v tvare `xxx-yyy-zz`, kde `xxx` je poradové číslo depeše, `yyy` je počet cifier depeše a `zz` je deň šifrovania depeše. Ak bolo číslo depeše napríklad 54, tak depeša bude mať podobu:

```
054-095-10
27513 11256 51289 88978 12292 18913 09762 94657 61031 94506
99471 31493 31707 36585 17328 00851 80197 23057 66048
```

a týmto je pripravená na odoslanie.

8.2 Postup pri šifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii text na šifrovanie.

b. Máme dané dostatočne dlhé základné heslo.

c. Je daný dátum šifrovania. Podľa dňa v mesiaci sa určuje denné heslo.

d. 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. 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.

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

3. Text rozdelíme na približne 100 znakov dlhé časti tak, aby každá časť končila kompletným slovom.[3]

4. Na koniec prvej časti pridáme, kvôli nadväznosti dielov `/1`. Na začiatok druhej časti pridáme `1/`, na koniec druhej časti pridáme `/2` atď. Každá časť textu (okrem prvej a poslednej) bude mať na začiatku číslo identické s koncovým číslom predošlej časti, znak `/` a na konci textu znak `/` a číslo identické s číslom označujúcim nasledovnú časť textu. Čísla na označovanie častí berieme od 1 vzostupne. Prvá časť má označenie len na konci a posledná časť len na začiatku.

5. Podľa tabuľky 1 nahradíme znaky depeše za čísla. Medzery medzi slovami sa nahrádzajú jednocifernými číslami `7, 8` alebo `9`.

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

7. Denné heslo zostrojíme zo základného hesla. Bude začínať písmenom základného hesla, ktorého poradie zodpovedá dňu šifrovania. Denné heslo musí mať aspoň 17 písmen a pokiaľ sedemnáste písmeno padne doprostred slova, tak vezmeme celé toto slovo.

8. Obvyklým spôsobom vyčíslime denné heslo. Medzery a interpunkčné znamienka sa nevyčíslujú a znaky vyčíslujeme v poradí podľa substitučnej tabuľky 1 (str. 3).

[3]Rozdeľovanie dlhších textov vyplýva z príkladu v [2], ale nie je to ani potrebné, ani žiaduce. Tu je to uvedené len pre úplnosť.

9. Text v číselnej podobe prešifrujeme autokľúčom tak, že pod neho najskôr napíšeme cifry vyčísleného denného hesla. Potom spravíme súčet cifier textu s ciframi hesla modulo 10. Tým dostaneme začiatok zašifrovanej depeše. Tam kde končí vyčíslené denné heslo budeme v kľúči pokračovať ciframi zašifrovanej depeše od jej začiatku potiaľ, pokiaľ to bude potrebné.

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

8.3 Postup pri dešifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii kompletný text zašifrovanej depeše.

b. Máme dané základné heslo.

Potom dešifrovanie depeše bude prebiehať v nasledovných krokoch:

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

2. Podľa dátumu šifrovania z návestia depeše a podľa základného hesla zostrojíme denné heslo. Toto bude začínať písmenom základného hesla, ktorého poradie zodpovedá dňu šifrovania. Denné heslo musí mať aspoň 17 písmen a pokiaľ sedemnáste písmeno padne doprostred slova, tak vezmeme celé toto slovo.

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

4. Vynecháme návestie depeše, ktoré už nebudeme potrebovať.

5. Pod cifry depeše ako kľúč najskôr zapíšeme vyčíslené denné heslo a za ním potom cifry samotnej depeše.

6. Od cifier depeše odčítame cifry kľúča modulo 10. Tým dostaneme text depeše v číselnej podobe.

7. Podľa tabuľky 1 nahradíme čísla znakmi. Tie sú kódované dvojcifernými číslami. Pokiaľ by na mieste desiatok bola cifra `7`, `8` alebo `9`, jedná sa o medzeru, ktorá je kódovaná jednociferne.

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

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

8.4 Lúštenie

Táto šifra, tak ako je popísaná v [2], je asi najslabšia zo všetkých popisovaných šifier. Pokiaľ lúštiteľ poznal princíp tejto šifry, mohol si priamo prečítať v každej depeši úsek šifrovaný od denného hesla ďalej. Začiatok depeše si mohol buď domyslieť, alebo spätne „skonštruoval“ použité heslo. Vzhľadom na malú dĺžku hesla, ktorá sa pohybovala okolo 17 znakov, to nemohol byť veľký problém. Ani v prípade rozdeľovania šifrovaného textu na kratšie časti by sa úroveň bezpečnosti príliš nezvýšila. Vzhľadom na popísaný spôsob šifrovania by sa všetky časti šifrovali tým istým denným heslom. Lúštiteľ by mal teda k dispozícii hneď niekoľko začiatkov depeší šifrovaných rovnakým heslom. Jednak by si z pokračovania textu jednotlivých častí mohol ľahšie spätne odvodiť použité heslo, jednak by mal na začiatku a konci jednotlivých častí mal znaky označujúce nadväznosť, ktoré by mu prácu ďalej uľahčili. Takže ak sa táto šifra skutočne používala tak, ako to popisuje pán Hanák vo svojej knihe, delenie textu depeší by bolo kontraproduktívne.

Literatúra

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

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

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

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

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

B. Rotorový šifrátor Fialka M-125
Diel 4., Implementácia a možnosti využitia

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

1 Výkonnostné parametre šifrátora

Dôležitým parametrom každého šifrátora je maximálna dosiahnuteľná rýchlosť šifrovania, aj keď reálna použiteľnosť šifrátora závisí v praxi hlavne od zložitosti implementácie.

V rámci [1] sme vytvorili jednoduchú konzolovú aplikáciu v programovacom jazyku C na simulovanie šifrátora a odmeranie rýchlosti danej implementácie. Funkčnosť a implementácia jednotlivých častí boli navrhnuté podľa popisu algoritmu z [1] a [2].

Na meranie sme použili náhodne generovanú testovaciu vzorku veľkosti 1MB a postupne sme ju po 1MB zvyšovali až na veľkosť 50MB. V algoritme používame čísla Z_{30}. Každé číslo (znak otvoreného textu) je reprezentované jedným bajtom.

Na generovanie náhodných čísiel sme použili funkciu rand() a funkciu srand() na inicializáciu pseudo-náhodného generátora. Vstupom do inicializačnej funkcie generátora sú aktuálny čas a identifikačné číslo programu v operačnom systéme.

V prvom experimente sme na odmeranie rýchlosti použili funkciu clock(), ktorá vracia približný počet hodinových cyklov procesoru od začiatku spustenia programu. [4] Takto získané hodnoty sú síce použiteľné, ale nie sú celkom presné. Preto sme na dosiahnutie presnejších výsledkov sme použili dve ďalšie metódy merania rýchlosti:

1. QueryPerformanceCounter
2. volanie RDTSC.

QueryPerformanceCounter API vyvinuté firmou Microsoft predstavuje nástroj na komplexnejšie a presnejšie meranie času. [6] Výhodou tejto funkcie je, že na viacprocesorových počítačoch presne odmeria počet hodinových cyklov nezávisle od procesoru, na ktorom bola volaná. Na presné určenie času potom slúži ďalšia (konverzná) funkcia.

Time Stamp Counter je 64 bitový register na procesoroch Pentium, ktorý vracia počet cyklov od spustenia procesoru pri štarte počítača. Funkcia RDTSC slúži na načítanie hodnoty tohto registra. Predstavuje jednu z najpresnejších metód merania času procesora. [7]

Na zvýšenie rýchlosti a efektivity aplikácie sme sa rozhodli zdrojový kód optimalizovať (aspoň čiastočne). Existuje veľa spôsobov a metód ako optimalizovať kód, my sme sa snažili použiť také metódy, aby sme čo najmenej museli zmeniť štruktúru existujúceho kódu.
Takéto zmeny boli napr.:

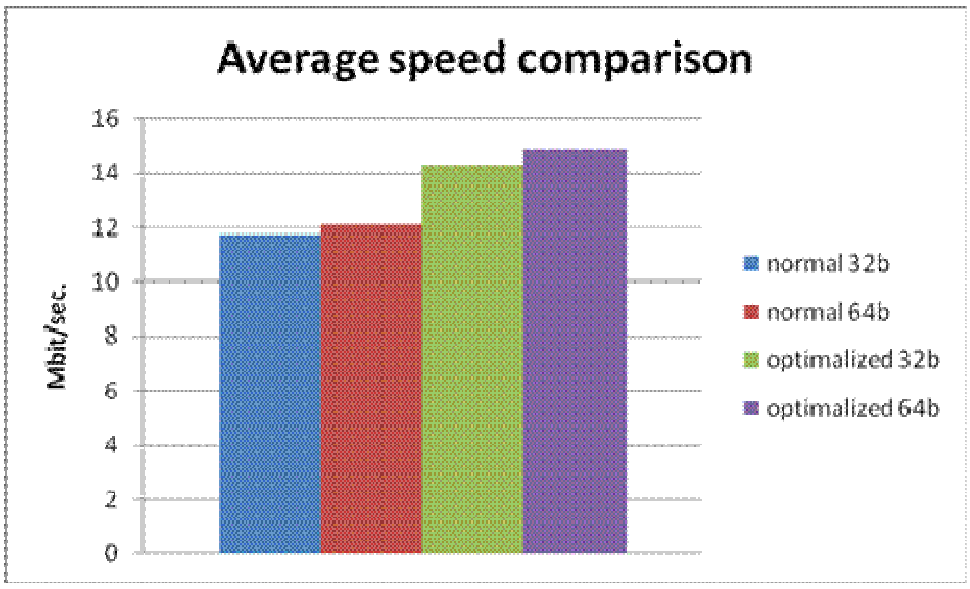
- použitie vložených funkcií,
- rozklad krátkych cyklov na jednotlivé iterácie,
- požitie takých údajových typov na reprezentáciu použitej abecedy, ktoré zodpovedajú natívnym veľkostiam typov použitej architektúry počítača.

Tieto optimalizácie nemôžeme považovať za také, ktoré už nie je možné zlepšiť. V našom experimente sa jednalo hlavne o poukázanie na možné spôsoby zrýchlenia implementovaného algoritmu.

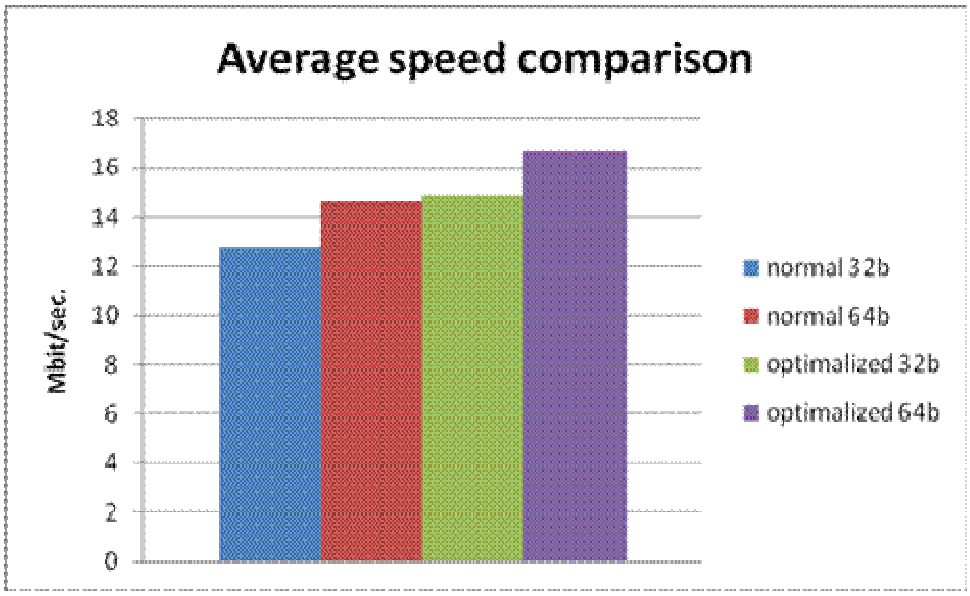
Experimentálne meranie rýchlosti sme vykonali na dvoch rôznych hardvérových konfiguráciách:

1. konfigurácia PC1: HP Pavilion dv6, Core2 Duo P8700 2x 2,53GHz, 4GB DDR3, 64bit OS,
2. konfigurácia PC2: Core i7 4x2.83GHz, 24 GB DDR3, 64bit OS.

V oboch prípadoch sme použili 32 aj 64 bitovú platformu. Výsledky možno vidieť na obrázkoch č. 1 a 2.



Obr. 1. Porovnanie priemeru rýchlosti z vykonaných experimentov (PC1)



Obr. 2. Porovnanie priemeru rýchlosti z vykonaných experimentov (PC2)

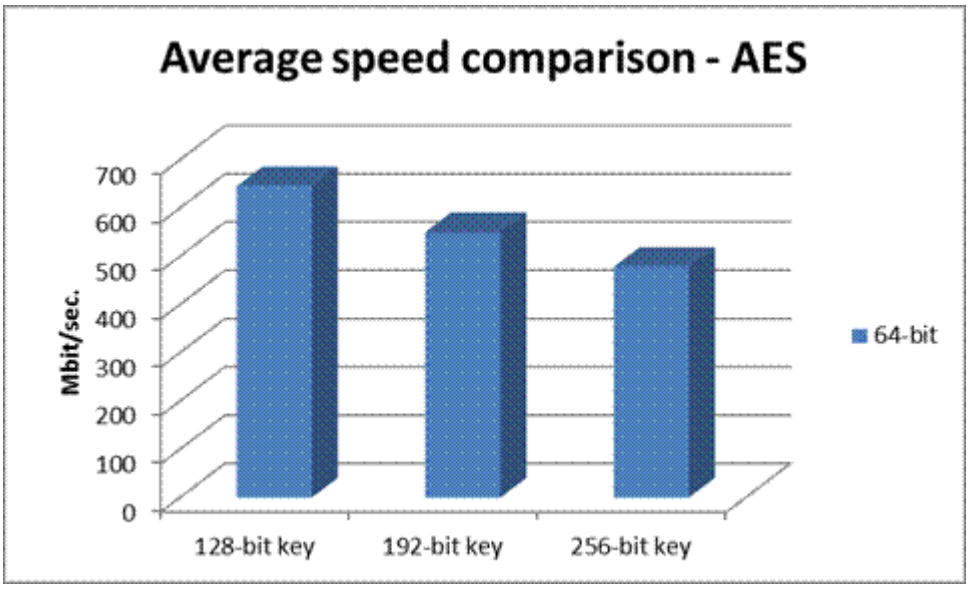
2 Porovnanie so súčasným šifrovacím štandardom

AES (z angl. Advanced Encryption Standard) je súčasným celosvetovým šifrovacím štandardom. Bol odvodený od víťazného kandidáta Rijndael (zmena spočíva v nastavení parametrov, nie v zmene štruktúry) verejnej súťaže na nový šifrovací štandard v roku 2001. Jedná sa vôbec o prvý otvorený štandard pre blokovú šifru, ktorý NSA akceptovala na použitie v prípade klasifikovaných údajov.

AES je založený na princípe substitučno-permutačnej siete. Po predošlom štandarde DES, založenom na Feistelovskej schéme, prišlo ku zmene. Algoritmus spočíva v opakovaní týchto štyroch operácií (súhrnne označovaných jedno kolo šifrovania):

1. nelineárna substitúcia každého prvku údajového bloku,
2. transpozícia údajov bloku,
3. difúzia bitov bloku a
4. pripočítanie tajného kľúča.

Dôležitými požiadavkami kladenými na víťaza nového šifrovacieho štandardu boli vysoká rýchlosť a malá pamäťová náročnosť. Oboje víťazný kandidát Rijndael spĺňa. Je možné ho efektívne implementovať aj softvérovo, aj hardvérovo. Pre ukážku a porovnanie s implementáciou rotorového šifrátora Fialka uvádzame jeho výkonnosť na našich testovacích zostavách (obrázky č. 3 a 4).



Obr. 3. Porovnanie priemeru rýchlosti šifrovania AES na zostave PC1.

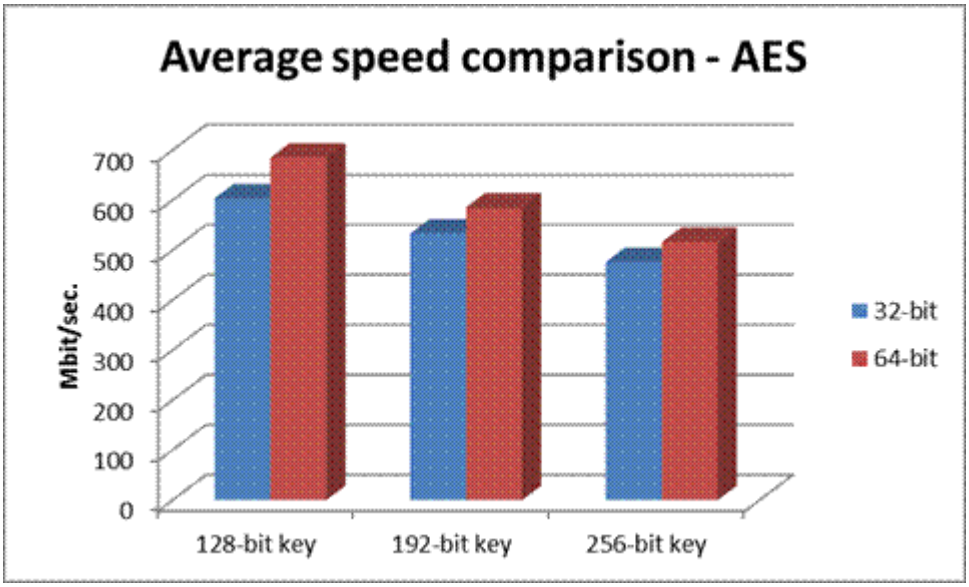
3 Simulátor

V rámci [2] sme vytvorili niekoľko webových aplikácií rôznych modifikácií šifrátora Fialka M-125, ktoré môžu byť použité ako učebné pomôcky:

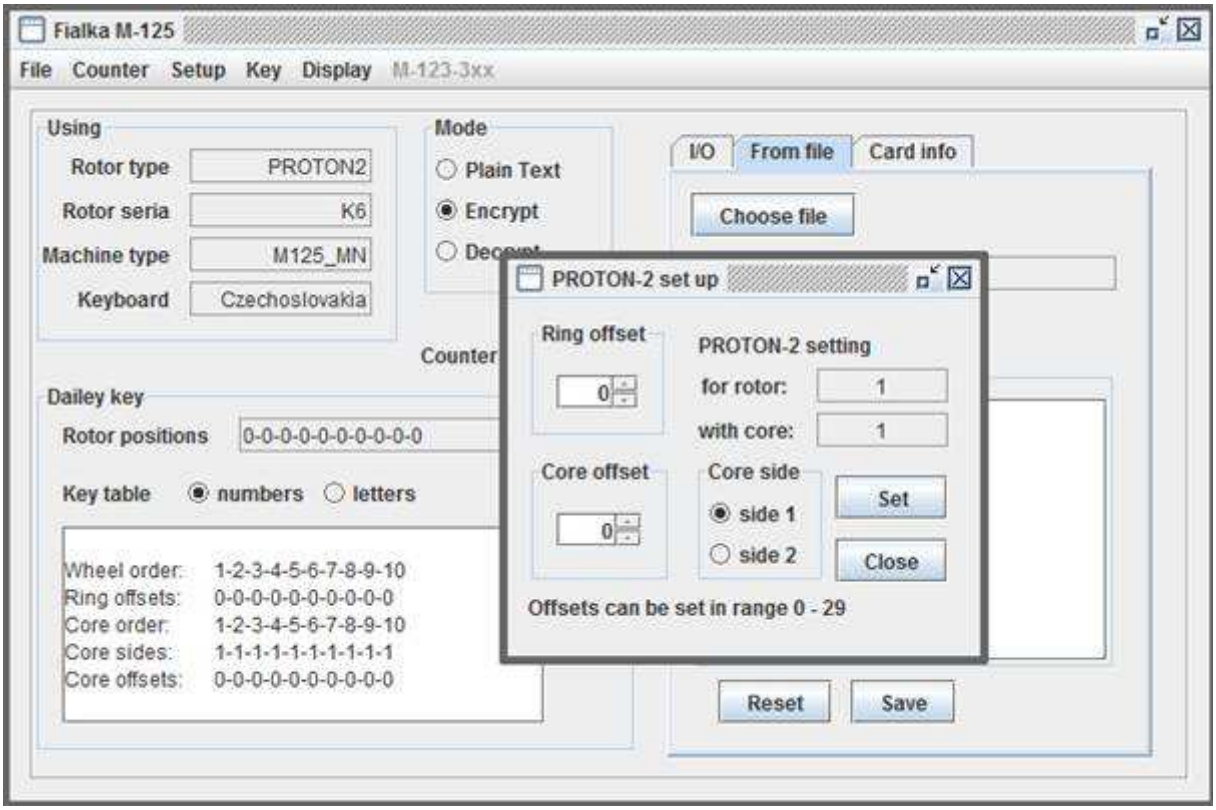
- zmenšená verzia šifry,
- verzia Fialka M-125 6K,
- komplexná verzia, ktorá zahŕňa M-125-xx / M-125-3xx (3K,6K).

Simulátory umožňujú študovať činnosť Fialky vzhľadom na rôzne vstupné nastavenia. Ovládanie programu ako aj rôzne nastavenia sú súčasťou video-tutoriálov dostupných na [3]. Ukážky rozhrania sú na obrázkoch č. 5 a 6.

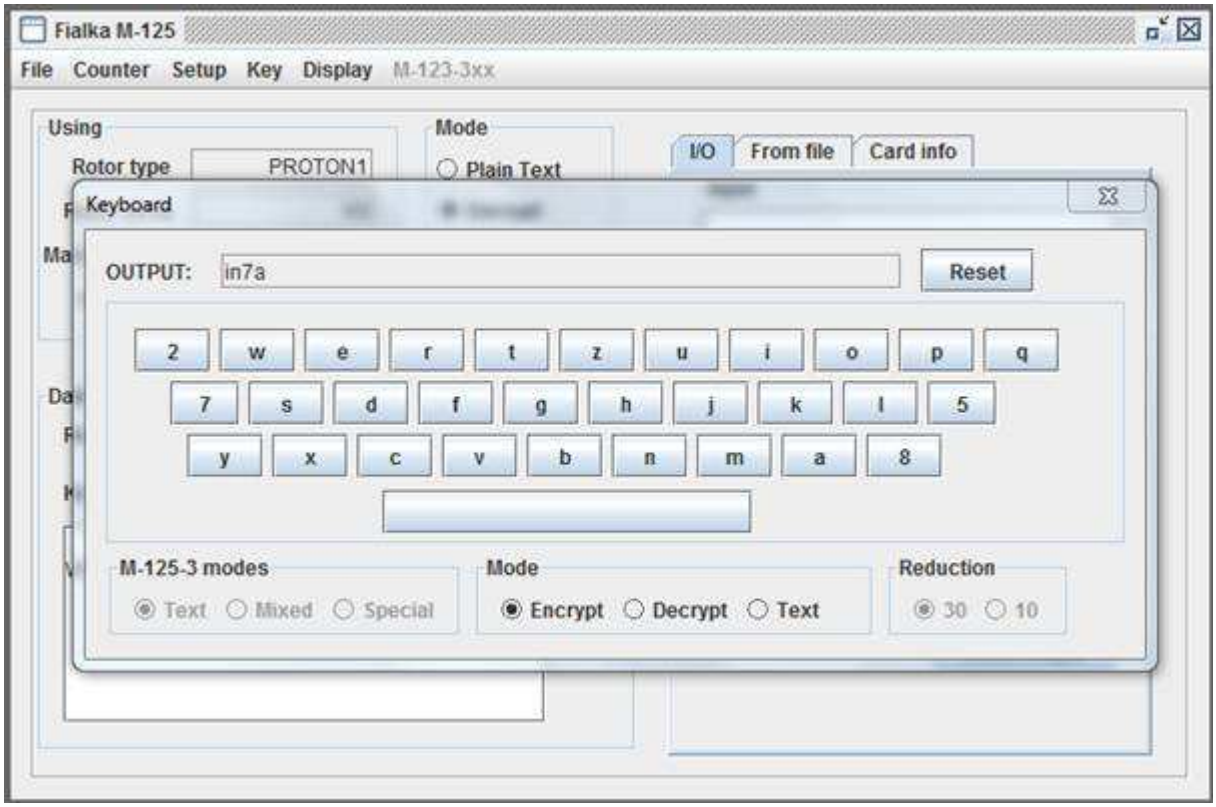
Aplikácie sú tiež voľne dostupné na internetovej stránke http://www.bc.fialka.szm.com.



Obr. 4. Porovnanie priemeru rýchlosti šifrovania AES na zostave PC2.



Obr. 5. Ukážka webovej aplikácie: nastavenie šifrátora.



Obr. 6. Ukážka webovej aplikácie: šifrovanie.

4 Záver

Rotorové šifrátory sa považujú za vrcholné dielo éry klasických šifier. Dôležitú úlohu hrali v druhej svetovej vojne a počas studenej vojny. Kvôli prechodu od analógového spracovania signálu na digitálne boli tieto stroje postupne nahradené modernými (počítačovými) šiframi.

V súčasnosti používané a navrhované šifry nosia odtlačok modernej doby, ich sila je založená na rôznych matematických konštrukciách a v ťažkých problémoch neriešiteľných v rozumnom čase.

Šifrátory typu Fialka M-125 môžeme považovať za silný prostriedok ochrany osobných údajov aj v súčasnosti napriek nepriaznivým výkonnostným parametrom. Zatiaľ nie sú známe útoky na túto šifru.

Napriek tomu, že využívanie rotorových šifrátorov čoraz viac ubúda, jestvujú isté oblasti komunikácie, v ktorých sú šifrovacie algoritmy založené (aspoň čiastočne) na rotorových šifrátoroch. Jednou z nich je napr. „lightweight kryptografia“, ktorá sa aplikuje vo vysokofrekvenčnej identifikácii (RFID). [8]

Príkladom je šifra Hummingbird. Jej šifrovací algoritmus je možné považovať za kontinuálny beh rotorovej šifry. Štyri blokové šifry pôsobia ako štyri rotory, ktoré vykonávajú permutáciu 16 bitových slov. Viac informácií z tejto oblasti je možné nájsť v [8].

Literatúra

[1] E. ANTAL: Niektoré problémy kryptoanalýzy šifry Fialka M-125. Diplomová práca, FEI STU Bratislava, 2011.

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

[3] Fialka M-125, [online], URL: http://www.bc.fialka.szm.com

[4] Clock , C++, [online], URL: http://www.cplusplus.com/reference/clibrary/ctime/clock/

[5] Prispievatelia Wikipedia: C syntax, Wikipedia the free encyclopedia, [online], URL: http://en.wikipedia.org/wiki/C_syntax#Primitive_data_types

[6] QuerryPerformanceCounter Function, The official website of Microsoft, [online], URL: http://msdn.microsoft.com/en-us/library/ms644904(v=vs.85).aspx

[7] Prispievatelia Wikipedia: Time Stamp Counter, Wikipedia the free encyclopedia, [online], URL: http://en.wikipedia.org/wiki/Time_Stamp_Counter

[8] Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices , [online], URL: http://comsec.uwaterloo.ca/researchfiles/WLC2010Final.pdf

C. Stále mám přístup k dalším CA, tvrdí útočník na DigiNotar

Ing. Jaroslav Pinkava, CSc. (jaroslav.pinkava@gmail.com)

Informace o aktivitách tzv. Comodohackera a o následně vzniklých problémech a také o hledání cest k jejich řešení zahltily zářijová média. Celé to odstartovala informace o hacknutí nizozemské CA DigiNotar. Předložený článek je shrnutím souvisejících informací (a dlouhé řady odkazů) a je mírně doplněnou verzí článku, který vyšel na Root.cz.

Comodohacker

Comodohacker (tak sám sebe označuje) se přihlásil k útoku na DigiNotar a tvrdí: stále mám přístup k dalším CA. Jmenoval také GlobalSign – Comodo hacker claims credit for DigiNotar attack http://www.networkworld.com/news/2011/090611-comodo-hacker-claims-credit-for-250454.html. Dotyčný popisuje sám sebe jako 21letého íránského studenta. Mikko Hypponen (F-Secure) však říká, že je to záhada. Jak se od hacku jednotlivce dostaneme k odposlechu íránských občanů, který měl široký rozsah? Nejspíš to bude trochu jinak.

Jeho tvrzení na Pastebin o možnostech dalších útoků komentují články:

- Claimed DigiNotar hacker: I have access to four more CAs

  http://www.theregister.co.uk/2011/09/06/comodohacker_claims_diginotar_hack/

- DigiNotar hacker: I have access to four other certificate authorities

  http://www.scmagazineuk.com/diginotar-hacker-i-have-access-to-four-other-certificate authorities/article/211291/

- Comodo Hacker Takes Credit For Massive DigiNotar Hack

  http://www.darkreading.com/authentication/167901072/security/attacks-breaches/231600865/comodo-hacker-takes-credit-for-massive-diginotar-hack.html

Hodnocení dopadů útoku se věnuje článek

- Fake SSL certificates pirate Web sites

  http://www.zdnet.com/blog/networking/fake-ssl-certificates-pirate-web-sites/1428

Reakce prezidenta společnosti Comodo:

- Comodo CEO accuses nation state of sponsoring SSL certificate attacks

  http://news.techworld.com/security/3301836/comodo-ceo-accuses-nation-state-of-sponsoring-ssl-certificate-attacks/

Společnosti, které spoléhají ve svém podnikání na SSL certifikáty, musí být připraveny na to nejhorší, zaznělo v článku Roberta Lemose:

- Are Some Certificate Authorities Too Big To Fail?

  http://threatpost.com/en_us/blogs/are-some-certificate-authorities-too-big-fail-090711

Comodohacker na Pastebin:

- Striking Back… http://pastebin.com/1AxH30em

- Another status update message http://pastebin.com/85WV10EL
- Two more little points http://pastebin.com/jhz20PqJ
- Response to some comments http://pastebin.com/GkKUhu35

Comodohacker na Twitteru:

- @ichsunx2 http://twitter.com/#%21/ichsunx2

Comodohacker odpovídá na otázky SC Magazine:

- ´Comodo Hacker´ talks to SC magazine

http://www.scmagazineuk.com/comodo-hacker-talks-to-sc-magazine/article/211443/

Komentář k jeho posledním hrozbám obsahuje článek – DigiNotar hacker threatens to expand spy attacks using stolen certificates

http://www.networkworld.com/news/2011/090811-diginotar-hacker-threatens-to-expand-250642.html

DigiNotar

Hackers steal SSL certificates for CIA, MI6, Mossad

http://www.computerworld.com/s/article/9219727/Hackers_steal_SSL_certificates_for_CIA_MI6_Mossad?taxonomyId=17

– komu všemu byly ukradeny SSL certifikáty: CIA, MI6, Mossad… Podvržených certifikátů od DigiNotar je nyní napočítáno již přes 500. Jinak podle tvůrců prohlížečů DigiNotar má smůlu, jako důvěryhodná autorita skončil.

Viz také komentáře:

- Hackers Forge Certificates to Break into Spy Agencies

http://www.pcworld.com/article/239497/hackers_forge_certificates_to_break_into_spy_agencies.html

- CIA, Mossad, MI6 targeted by Iranian DigiNotar-hackers

http://mis-asia.com/resource/security/cybercrime-and-hacking/cia-mossad-mi6-targeted-by-iranian-diginotar-hackers/

Společnost F-Secure na svém blogu oznámila, že nalezla známky, že síť DigiNotar byla hacknuta již v roce 2009 (http://www.f-secure.com/weblog/archives/00002228.html)

Jak nastalé problémy řeší nizozemská vláda – Dutch government struggles with DigiNotar hack
http://www.computerworld.com/s/article/9219814/Dutch_government_struggles_with_DigiNotar_hack?taxonomyId=17
Nizozemsko nyní zkoumá, zda nebyly hacknuty vládní weby – Dutch study possible Iran hacking of government web sites http://hken.ibtimes.com/articles/208297/20110905/dutch-study-possible-iran-hacking-of-government-web-sites.htm

Je analyzován možný podíl Íránu.

Probíhá audit DigiNotar – dostupná je částečná zpráva – DigiNotar audit – intermediate report available http://isc.sans.edu/diary.html?storyid=11512&rss. Na této stránce je několik komentářů k jejímu obsahu. Poukázaných nedostatků není málo. Samotnou zprávu najdete zde http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/fox-it-operation-black-tulip/rapport-fox-it-operation-black-tulip-v1-0.pdf

Další komentář k této zprávě je zde – DigiNotar breach report reveals lousy security practices http://www.net-security.org/secworld.php?id=11570.

Komentáře k DigiNotar:

- False SSL certificates issued for spy agencies

http://www.zdnet.co.uk/news/security-threats/2011/09/05/false-ssl-certificates-issued-for-spy-agencies-40093840/

- Iranian users were the ultimate target in DigiNotar compromise

http://www.net-security.org/secworld.php?id=11566

- #DigiNotar given vote of ´no confidence´ by internet giants

http://www.scmagazineuk.com/diginotar-given-vote-of-no-confidence-by-internet-giants/article/211274/

- Dutch government takes control of DigiNotar CA

http://www.h-online.com/security/news/item/Dutch-government-takes-control-of-DigiNotar-CA-1337286.html

- Experts suspect Iran involvement in Dutch hacking
http://www.ctpost.com/news/article/Experts-suspect-Iran-involvement-in-Dutch-hacking-2156135.php

GlobalSign

GlobalSign zastavil prodej digitálních certifikátů:

- After hacking claims, second firm pulls digital certificates

http://www.computerworld.com/s/article/9219758/After_hacking_claims_second_firm_pulls_digital_certificates

- GlobalSign Halts Digital Certificate Sales

http://www.securityweek.com/globalsign-halts-digital-certificate-sales

Firma nebere oznámení (Comodo hacker) na lehkou váhu – GlobalSign stops issuing SSL certs, probes hacker claims. Better to do it and not need to than vice versa.

http://www.theregister.co.uk/2011/09/07/globalsign_suspends_ssl_cert_biz/

Comodohacker oznámil, že ukradl GlobalSignu velké množství dat – DigiNotar hacker says he stole huge GlobalSign cache http://www.theregister.co.uk/2011/09/07/diginotar_hacker_proof/. Má prý přístup k celému serveru, zálohám databází a konfiguracím systému této americké certifikační autority. Obdobně se mu podařilo získat přístupy k datům izraelské CA StartCom. Článek také obsahuje informaci, jak tento hacker popisuje zabezpečení podepisování certifikátů u DigiNotar: „HSM, or hardware security module, ran on the OpenBSD operating

system and had only a single port open that was protected with RSA SecurID and SafeSign Token management systems“. Viz také:

- GlobalSign stops SSL certificates after hack claim

http://www.zdnet.co.uk/news/security-threats/2011/09/07/globalsign-stops-ssl-certificates-after-hack-claim-40093864/

- GlobalSign on alert after hacker´s boast

http://www.scmagazineuk.com/globalsign-on-alert-after-hackers-boast/article/211370/

A následovalo přiznání, GlobalSign oznámil průnik do svého systému – GlobalSign Acknowledges System Breach http://www.securityweek.com/globalsign-acknowledges-system-breach .

Má se to však týkat pouze webového serveru, který je fyzicky oddělen od ostatní infrastruktury. Slouží pouze pro potřeby webu www.globalsign.com.

Stanovisko GlobalSignu z konce týdne – GlobalSign to relaunch services, as Mozilla warns other CAs off Diginotar
http://www.scmagazineuk.com/globalsign-to-relaunch-services-as-mozilla-warns-other-cas-off-diginotar/article/211545/

Nejprve pak informuje - Globalsign finds no PKI compromise http://www.theinquirer.net/inquirer/news/2108549/globalsign-pki-compromise?WT.rss_f=&WT.rss_a=Globalsign%20finds%20no%20PKI%20compromise - audit nenašel žádnou kompromitaci PKI. Tj. průnik se měl skutečně týkat výlučně izolovaného webového serveru.

Viz také komentáře:
GlobalSign says ´isolated´ webserver was hacked
http://www.theregister.co.uk/2011/09/12/globalsign_security_breach/
GlobalSign finds no sign of fake certificates after hack
http://www.zdnet.co.uk/news/security-threats/2011/09/12/globalsign-finds-no-sign-of-fake-certificates-after-hack-40093904/

GlobalSign pak obnovil vydávání SSL certifikátů:
GlobalSign set to reopen Tuesday despite web server hack
http://www.computerworld.com/s/article/9219914/GlobalSign_set_to_reopen_Tuesday_despite_web_server_hack?taxonomyId=17
Certificate Authority GlobalSign Restores SSL Certifications Following Investigation
http://www.crn.com/news/security/231601260/certificate-authority-globalsign-restores-ssl-certifications-following-investigation.htm

Microsoft

Microsoft říká, že ukradené SSL certifikáty nemohou být použity k šíření malware prostřednictvím Windows Update – Microsoft: Stolen SSL certs can't be used to install malware via Windows Update

http://www.computerworld.com/s/article/9219729/Microsoft_Stolen_SSL_certs_can_t_be_used_to_install_malware_via_Windows_Update?taxonomyId=17 .

Viz také vyjádření (Jonathan Ness, Microsoft Security Response Center) na blogu Microsoftu – Protecting yourself from attacks that leverage fraudulent DigiNotar digital certificates

http://blogs.technet.com/b/srd/archive/2011/09/04/protecting-yourself-from-attacks-that-leverage-fraudulent-diginotar-digital-certificates.aspx . Situaci ohledně Windows Update rozebírá Gregg Keizer v článku Hacker claims he can exploit Windows Update http://www.computerworld.com/s/article/9219876/Hacker_claims_he_can_exploit_Windows_Update?taxonomyId=17 .
Microsoft nastálo revokoval všechny nizozemské SSL certifikáty – Microsoft Permanently Revokes All Dutch CA´s SSL Certificates http://www.eweek.com/c/a/Security/Microsoft-Permanently-Revokes-All-Dutch-CAs-SSL-Certificates-105170/ .
Titulek trochu nepřesný, ve skutečnosti (jak objasní článek) se nejedná o jejich revokaci, ale o blokaci. Viz také – Microsoft flips ´kill switch´ on all DigiNotar certificates http://www.computerworld.com/s/article/9219746/Microsoft_flips_kill_switch_on_all_DigiNotar_certificates?taxonomyId=17 . Následně pak Microsoft odstraňuje další certifikáty - Microsoft patches 15 bugs, nukes more SSL certificates http://www.computerworld.com/s/article/9219976/Microsoft_patches_15_bugs_nukes_more_SSL_certificates?taxonomyId=17 – jedná se o ty certifikáty DigiNotar, které jsou ještě přepodepsány dalšími certifikačními autoritami (Entrust a GTE) a podotýká, že problémy se netýkají jiných certifikátů těchto dvou autorit.

Google

Okolo 300 000 íránských IP adres bylo pravděpodobně kompromitováno – Nearly 300,000 Iranian IP addresses likely compromised http://www.networkworld.com/news/2011/090611-nearly-300000-iranian-ip-addresses-250411.html
Oznámila to bezpečnostní firma Fox-it. Seznam adres byl předán společnosti Google s tím, že tato bude uživatele varovat (v kritické době mohly být jejich e-maily odchyceny). Viz také:

- Inside ´Operation Black Tulip´: DigiNotar hack analysed

  http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/
- Hackers spied on 300,000 Iranians using fake Google certificate

  http://www.computerworld.com/s/article/9219731/Hackers_spied_on_300_000_Iranians_using_fake_Google_certificate?taxonomyId=17
- DigiNotar breach fallout widens as more details emerge

  http://www.scmagazineus.com/diginotar-breach-fallout-widens-as-more-details-emerge/article/211349/
- DigiNotar breach due to disastrous security – Update

  http://www.h-online.com/security/news/item/DigiNotar-breach-due-to-disastrous-security-Update-1337573.html
- Could DigiNotar Hack Lead to a Cyberattack on You?

  http://www.foxnews.com/scitech/2011/09/06/hacked-turkish-business-diginotar-could-spell-disaster-for/

Celou záležitost vyšetřuje nizozemská tajná služba – Dutch launch Iran IT hacking probe http://en.trend.az/regions/iran/1927842.html .
Společnost Google kontaktuje své íránské uživatele – Google contacts Iranian users to secure Gmail accounts http://www.networkworld.com/news/2011/090911-google-contacts-iranian-users-to-250653.html , blog Google – Gmail account security in Iran http://googleonlinesecurity.blogspot.com/2011/09/gmail-account-security-in-iran.html .

Apple, Adobe

Na hlavu společnosti Apple se snášela kritika (nebyly vidět její reakce):

- Researcher raps Apple for not blocking stolen SSL certificates
  http://www.computerworld.com/s/article/9219838/Researcher_raps_Apple_for_not_blocking_stolen_SSL_certificates?taxonomyId=17

- Apple Delays DigiNotar SSL Update, Partners ´Not Surprised´
  http://www.crn.com/news/security/231601066/apple-delays-diginotar-ssl-update-partners-not-surprised.htm

Oproti tomu Adobe reaguje – Adobe Says It Is Breaking Ties To Diginotar http://threatpost.com/en_us/blogs/adobe-says-it-breaking-ties-diginotar-090811 .

Ale nakonec – Apple strikes stolen SSL certificates from OS X http://www.computerworld.com/s/article/9219892/Apple_strikes_stolen_SSL_certificates_from_OS_X?taxonomyId=17 – Apple reagovalo v třikrát kratší době než tomu bylo u hacku společnosti Comodo.

Symantec

Symantec oznamuje – naše SSL CA zůstávají bezpečné – Symantec responds to ‚panic' around DigiNotar hack http://www.networkworld.com/news/2011/090811-symantec-responds-to-panic-around-250610.html . Společnost odpovídá na vzniklou „paniku". Rooty VeriSignu, Thawte, GeoTrustu a RapidSSL zůstávají bezpečné.Viz také komentář Diginotar hacker threatens SSL attacks in US, Europe and Israel http://www.theinquirer.net/inquirer/news/2107876/diginotar-hacker-threatens-ssl-attacks-europe-israel , ve kterém je zmínka o nástroji užitečném pro obranu před podvrženými certifikáty – Convergence http://convergence.io/ (Moxie Marlinspike). K tomuto nástroji se pak obrací vyjádření Google – Google: SSL alternative won´t be added to Chrome http://www.theregister.co.uk/2011/09/08/google_chrome_rejects_convergence/ .

Symantec chce zorganizovat centrální správu veškerých SSL certifikátů - Symantec Launches Cloud-Based SSL Certificate Management Service http://www.eweek.com/c/a/Security/Symantec-Launches-CloudBased-SSL-Certificate-Management-Service-205222/ . A to bez ohledu na to, kdo je vydal. Jedná se o službu (v cloudu) Certificate Intelligence Centre - CIC. Služba má za cíl zjednodušit správu certifikátů u organizací. Viz také komentáře:

- Symantec Announces Cloud-Based Solution to Keep SSL Certificates In Order
  http://www.securityweek.com/symantec-announces-cloud-based-solution-keep-ssl-certificates-order
- Enterprise-level management and control of SSL certificates
  http://www.net-security.org/secworld.php?id=11614

Mozilla

Mozilla chce, aby všechny CA, které má na svém seznamu důvěryhodných, prošly auditem – Burned by DigiNotar, Mozilla tells cert cops to audit security http://www.theregister.co.uk/2011/09/08/mozilla_certificate_authority_audit/ . Na programu Mozilly se podílí 54 certifikačních autorit s celkem 147 kořenovými certifikáty.
Komentář k situaci – GlobalSign: Hacker´s Claims ´Represent An Industry Wide Attack´ http://www.darkreading.com/authentication/167901072/security/attacks-breaches/231601068/globalsign-hackers-claims-represent-an-industry-wide-attack.html

Chytré mobily a SSL certifikáty

Na chytrých mobilech se nedaří revokovat SSL certifikáty od DigiNotar – Google and Apple fail to revoke DigiNotar SSL certificates on smartphone http://news.techworld.com/security/3301828/google-and-apple-fail-to-revoke-diginotar-ssl-certificates-on-smartphone/ .

Ani tedy pro systémy s Androidem či pro iPhone. Microsoft má tu výhodu, že nezahrnul DigiNotar do svého seznamu důvěryhodných CA pro Microsoft Windows Phone.

Další informace z médií

New York Times: Nizozemský hack ukazuje na slabé stránky bezpečnosti internetu - Hacking in Netherlands Points to Weak Spot in Web Security

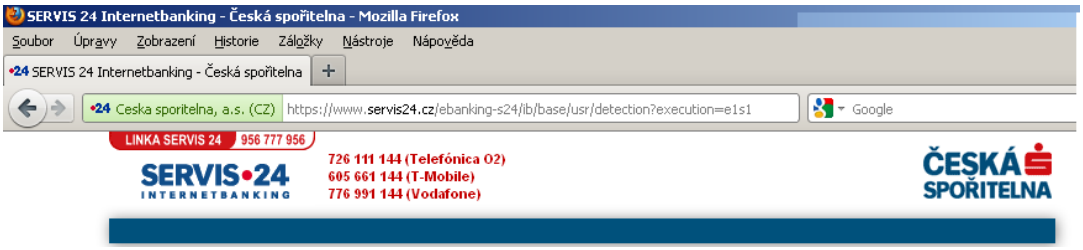
http://www.nytimes.com/2011/09/13/technology/hacking-in-netherlands-points-to-weak-spot-in-web-security.html?_r=1 . Komentář k celkové situaci napsal Kevin J. O´Brien. Její podstatu velmi dobře vystihuje tato autorova formulace: "*Hacknutí DigiNotar je důsledek dvou věcí, jednak jsou to špatně interně prováděné kontroly DigiNotar a druhým rozhodujícím faktorem je cílevědomý hacker.*"

Doporučení (uživatelům)
Jak se chránit před zloději certifikátů – How to Protect Yourself From Certificate Bandits
http://www.pcworld.com/article/239766/how_to_protect_yourself_from_certificate_bandits.html

John P. Mello Jr. (PCWorld) uvádí tato doporučení:

- Udržujte svůj prohlížeč v aktualizované podobě
- Povolte ve vašem prohlížeči revokaci certifikátů
- Uzpůsobte seznam kořenových certifikátů ve vašem prohlížeči
- Vždy se dívejte, zda se v adresovém řádku prohlížeče objeví zelená barva

(Poznámka redakce: poslední rada je bez dalšího vysvětlení zavádějící, tak tedy vlemi zjednodušeně , zelená barva se jménem vlastníka certifikátu se objeví jen v případě že je použit tzv Certifikát SSL EV (EV = extended validation). Za něj si u poskytovatelů, kteří SSL certifikáty vydávají, ovšem připlatíte, na oplátku tito vystavitelé slibují i významně náročnější přístupy při ověřování vlastníka vydávaného certifikátu). Kompletní infromace je dostupná v dokuementu („standardu“) Guidelines for Extended Validation Certificates vydaným o udržovaným skupinou CA/Browser Forum http://www.cabforum.org/Guidelines_v1_3.pdf. Naleznete zde i seznam všech poskytovatelů, kteří EV certifikáty vydávají. Mezi nimi jsou věak i výše zmíněné autority DigiNotar a GloablSign.)



Na stránce **Compromised certificate authorities: How to protect yourself** (http://www.techrepublic.com/blog/security/compromised-certificate-authorities-how-to-protect-yourself/6521) lze nalézt další doporučení, Patrick Lambert zde populární formou vysvětluje podstatu problému.

D. Podzimní *Soutěž v luštění 2011*, úvodní informace

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).

V prvních letech (2000-2004) byly úlohy zaměřeny na klasické šifrové systémy. Od roku 2005 jsou úlohy doprovázeny komentáři a nápovědami v NEWS na naší domovské stránce.

V roce 2006 úlohy spojoval vymyšlený doprovodný příběh. Jednalo se o drobné epizody ze života detektiva kapitána Cardy. Příběh vyústil v lov na chameleóna rasy Cryptomelon Pragensis.

V roce 2007 byl použit rozsáhlý doprovodný fiktivní příběh historické osoby matematika Štěpána Schmidta, který se odehrával v době Marie Terezie. Příběh z 18.století byl zkombinován s fikcí, která popisovala jeho údajné působení v Černé komnatě – luštitelském pracovišti na tehdejším císařském dvoře ve Vídni.
http://soutez2007.crypto-world.info/index.php?crypto=pribeh

V roce 2008 soutěž provázel fiktivní příběh z druhé světové války. Odehrával se kolem snahy vyluštit důležitou depeši odvysílanou 15. října 1941. Společně s britským důstojníkem Johnem Wellingtonem jste tak mohli postupně odhalovat záhadu nového neznámého německého šifrovacího zařízení - šifrátoru SZ 40. Simulátor tohoto zařízení je dostupný na stránce našeho e-zinu. http://soutez2008.crypto-world.info/index.php?crypto=pribeh

V roce 2009 se pak doprovodný příběh k soutěži odehrával v Československé republice koncem padesátých let. Jednalo se o příběh se špionážní zápletkou. Hlavní postavou byl kryptolog Václav Prokopec. V soutěži sehrál důležitou úlohu šifrátor ŠD-2. Simulátor je pro zájemce opět k dispozici na stránce e-zinu.
http://soutez2009.crypto-world.info/index.php?crypto=pribeh ¨

V loňském roce 2010 byl doprovodný příběh k soutěži inspirován životními osudy známého dobrodruha a svůdníka Giacoma Casanovy (1725-1798). Ve vymyšleném autobiografickém dílku Tajnosti mého života (Secrets de ma vie) jste se mohli postupně seznamovat s jeho osudy, které byly spojeny s vymyšlenými událostmi, které vždy nějak souvisely s šiframi té doby a mohli jste postupně řešit až do samého finále ve které byla Casanova kniha o šifrách zničena …
http://soutez2010.crypto-world.info/index.php?crypto=pribeh

Letošní soutež bude poněkud „chudší“. Bude se skládat z řady postupně zveřejňovaných lehkých úloh.

Přesná pravidla, ceny a prvé úlohy soutěže najdete v příštím čísle našeho e-zinu Crypto-World 10/2010, který by měl vyjít v neděli 16. 10. 2011. Všechny informace budou současně dostupné i na našem webu v sekci věnované soutěžím http://crypto-world.info/souteze.php nebo přímo na připravované stránce http://soutez2011.crypto-world.info/ .

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

E. O čem jsme psali v září 2000 – 2010

Crypto-World 9/1999

Crypto-World 9/2000

Příloha : gold_bug.rtf
Dnešní přílohou je klasická povídka The Gold Bug od Edgara Allana Poea
(další informace k příloze viz závěr článku "Část I.- Začínáme steganografií" , str.10) .

Crypto-World 9/2001

Crypto-World 9/2002

Crypto-World 9/2003

Crypto-World 9/2004

Crypto-World 9/2005

Crypto-World 9/2006

Crypto-World 9/2007

Crypto-World 9/2008

Crypto-World 9/2009

Crypto-World 9/2010

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí e-ziny, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály: http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška 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