Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 13, číslo 7-8/2011 **1. srpen**

78/2011

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 7., Šifra „Eva“

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.

7 Šifra „Eva“

Šifra „Eva“ bola typu TT. Jednalo sa o dvojitú transpozíciu. Prvá transpozícia je obrazcová (v trojuholníku) a druhá transpozícia je bežná tabuľková. Túto šifru používala napríklad rádiostanica Eva v operácii Clay. Odtiaľ pochádza aj pracovný názov uvedený v tomto článku. Je ale veľmi pravdepodobné, že šifra mala oficiálne označenie niektorým rímskym číslom, podobne ako iné ČS šifry. Popis šifry „Eva“ je uvedený v knihe [2] (str. 125–126).

7.1 Všeobecný popis a príklad šifrovania depeší

Popis tejto šifry v [2], pokiaľ sa to vyjadrí veľmi mierne, je nekompletný. Popisujú sa tam len obe transpozície. Je pritom evidentné, že sa robila aj nejaká substitúcia, prípadne kódovanie znakov. V príklade uvádzanom v [2] sa používa len 26 znakov medzinárodnej abecedy. Vzhľadom na použitý spôsob zápisu niektorých špeciálnych znakov, je ale dosť pravdepodobné, že sa používal podobný, alebo rovnaký spôsob zápisu šifrovaného textu ako pri šifre „rímska trinásť“. Čiže dĺžne sa nepísali, spoluhlásky s mäkčeňmi sa zdvojovali, číslice a niektoré interpunkčné znamienka sa zapisovali pomocou W tabuľky ([1], str. 171) a medzery sa zapisovali ako `QQ` alebo `XX`. Alternatívne riešenie by bolo písať text v angličtine, t.j. v jazyku, ktorý si vystačí len s medzinárodnou abecedou. V ďalšom popise šifrovania budeme text určený na šifrovanie prepisovať len pomocou 26 znakov medzinárodnej abecedy a špeciálne znaky budeme zapisovať pomocou W tabuľky.

W tabuľka																
.	**:**	**,**	**-**	**/**	**!**	**?**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
WA	WB	WC	WD	WE	WF	WG	WH	WI	WJ	WK	WL	WM	WN	WO	WP	WQ

V [2] sa na strane 125 uvádza, že pri šifrovaní touto šifrou sa používalo, po vzájomnej dohode, jedno z nasledovných štyroch hesiel:

1. *Už tambor bubnuje šohaj mašíruje a jeho galánka ruce zalamuje.*
2. *Kdo má počernú galánku – ligotala se hvězdička – anděl moj.*
3. *Když jsme se loučili byl smutný den.*
4. *Za bílýma za horama tancovala Majdalenka s dragounama.*

O výbere hesiel, ako aj o gramatickej správnosti uvedených štyroch hesiel[1], sa dá úspešne pochybovať. Keďže ale nemáme žiadny lepší zdroj popisujúci túto šifru, použijeme informácie, ktoré máme k dispozícii.

Postup šifrovania teraz ukážeme na príklade. Ako text určený na zašifrovanie zvolíme:

Snaž se, abys nikdy nic nedělal proti své vůli.[2]

Tento text teraz prepíšeme len pomocou 26 znakovej medzinárodnej abecedy.

`SNAZ SE,ABYS NIKDY NIC NEDELAL PROTI SVE VULI.`

Zo špeciálnych znakov sa používali len znaky `. : , - / ! ?`. Tieto špeciálne znaky a číslice sa kódovali podľa `W` tabuľky uvedenej na strane 2 a použitej aj pri šifre „rímska trinásť“. Medzery za špeciálnymi znakmi sa vynechávali a ostatné medzery sa údajne nahrádzali písmenami `Q` alebo `X`. Toto by ale nebolo práve najšťastnejšie riešenie, pretože text by potom nemusel byť jednoznačne dešifrovateľný a to ani v prípade slovenského alebo českého textu. Slová `EXTRÉM, MAXIMUM, TEXT, Q-KÓD, SQUASH, QANTAS` a iné, ktoré obsahujú znaky `Q` alebo `X`. Samozrejme pre človeka, dešifranta, by z kontextu bolo ihneď zrejmé či sa jedná o medzeru, alebo nejaké exotické slovo, ale pri strojovom dešifrovaní by to spôsobovalo problémy. Takže popis z [2] upravíme a medzery nahradíme dvojicami znakov `QQ` alebo `XX`, rovnako ako sa to robilo pri šifre „rímska trinásť“. Zvolený text teraz prepíšeme týmto spôsobom a dostávame:

`SNAZXXSEWCABYSQQNIKDYXXNICQQNEDELALXXPROTIQQSVEXXVULIWA`

[1] Uvedené heslá sú prepis z [2], strana 125.

[2] Pôvodná verzia v latinčine: *Da operam, ne quim umquam invitus facias. Seneca (Ep.61,3)*

Je to reťazec dlhý 55 znakov. K nemu ešte budeme pridávať na začiatok 5 adresovacích znakov a na koniec 3 podpisové znaky. Adresovacie znaky pozostávali z prvých troch znakov denného hesla a bodky kódovanej podľa `W` tabuľky. Mali teda tvar `...WA`. Podpisové znaky boli tvorené prvými troma znakmi denného hesla napísanými odzadu. Bodka už na konci textu je, takže podpisové znaky nie je potrebné ešte zvlášť oddeľovať od textu. Spolu s adresovacími a podpisovými znakmi dostaneme potom reťazec dlhý 63 znakov. Tento ešte doplníme tak, aby jeho dĺžka bola násobkom 5. Môžme ho doplniť ľubovoľnými znakmi. V našom príklade budeme musieť pridať 2 znaky.

V [2] sa nepíše nič o delení textu určeného na šifrovanie. Teoreticky by sa podľa uvedeného popisu dali šifrovať ľubovoľne dlhé texty. Z hľadiska bezpečnosti šifry by delenie textov tiež nebolo nejakým významným prínosom, môžme teda od neho upustiť. V prvej fáze šifrovania sa reťazec znakov, ktorý sme dostali a doplnili jeho dĺžku na násobok 5, zapisuje do trojuholníkovej tabuľky po riadkoch zľava doprava a zhora nadol. Dĺžka prvého riadku bude 1, druhého riadku 3 a každý ďalší riadok bude mať o dve políčka viac než predchádzajúci. Takto dostaneme „rovnoramenný“ trojuholník. Podľa dĺžky reťazca určeného na šifrovanie si ľahko vypočítame potrebný počet riadkov trojuholníka, ako aj dĺžku posledného riadku. Ak má reťazec dĺžku k znakov, trojuholník musí mať aspoň n riadkov, pričom $k \leq n^2$ a berieme najmenšie prirodzené číslo n, ktoré tejto nerovnosti vyhovuje. Potom posledný riadok trojuholníka bude mať dĺžku $d = 2n - 1$ znakov. V našom príklade $k = 65$, takže $n = 9$ a $d = 17$.

Teraz ukážeme konštrukciu transpozičného hesla. Použijeme prvé z uvedených štyroch hesiel. Za denné heslo sa berie cyklický posun dohodnutého hesla. Ako prvý znak denného hesla sa berie to písmeno dohodnutého hesla, ktorého poradie zodpovedalo dňu šifrovania. Z dohodnutého hesla zoberieme toľko znakov, koľko má posledný riadok trojuholníka. Pokiaľ je tento riadok dlhší než dohodnuté heslo, tak heslo zopakujeme, aby sme dosiahli potrebný počet znakov. V našom príklade budeme šifrovať text 21. deň v mesiaci. Potom denné heslo bude začínať 21. písmenom dohodnutého hesla a bude mať 17 znakov (dĺžka posledného riadku trojuholníka). Denné heslo a jeho vyčíslenie podľa medzinárodnej abecedy budú vyzerať takto:

M	A	S	I	R	U	J	E	A	J	E	H	O	G	A	L	A
13	1	16	9	15	17	10	5	2	11	6	8	14	7	3	12	4

Prvé tri znaky denného hesla a bodka tvoria podpisové znaky, ktoré pridáme na začiatok textu. V našom prípade to bude `MASWA`. Na konci textu budú podpisové znaky `SAM`, čo sú vlastne prvé tri znaky denného hesla, písané odzadu.

Jednotlivé stĺpce transpozičného trojuholníka očíslujeme vyčísleným denným heslo a reťazec znakov, ktorý ideme šifrovať, zapíšeme do tohto trojuholníka. Dostaneme:

								M								
							A	S	W							
						A	S	N	A	Z						
					X	X	S	E	W	C	A					
				B	Y	S	Q	Q	N	I	K	D				
			Y	X	X	N	I	C	Q	Q	N	E	D			
		E	L	A	L	X	X	P	R	O	T	I	Q	Q		
	S	V	E	X	X	V	U	L	I	W	A	S	A	M	V	
Y																
13	1	16	9	15	17	10	5	2	11	6	8	14	7	3	12	4

Teraz vypisujeme znaky z transpozičného trojuholníka po stĺpcoch zdola nahor. Poradie stĺpcov určuje vyčíslené heslo. Znaky zapisujeme do bežnej, obdĺžnikovej, transpozičnej tabuľky, ktorej šírka je rovnaká ako je dĺžka posledného riadku transpozičného trojuholníka. Znaky do tabuľky zapisujeme po riadkoch zľava doprava a zhora nadol. Stĺpce transpozičnej tabuľky sú očíslované tým istým vyčísleným heslom, ako stĺpce transpozičného trojuholníka:

13	1	16	9	15	17	10	5	2	11	6	8	14	7	3	12	4
S	L	P	C	Q	E	N	S	M	M	Q	U	X	I	Q	S	S
A	W	O	Q	I	C	Z	A	Q	D	A	T	N	K	A	E	L
Y	V	X	N	S	X	A	I	R	Q	N	W	A	W	V	Y	S
I	E	D	X	A	X	B	V	E	X	L	X	Y	X			

Z transpozičnej tabuľky vypisujeme znaky po stĺpcoch zhora nadol. Poradie stĺpcov je opäť určené vyčísleným heslom. znaky rozdeľujeme do päťmiestnych skupín:

```
LWVEM QREQA VSLSS AIVQA NLIKW XUTWX CQNXN ZABMD QXSEY SAYIX
NAYQI SAPOX DECXX
```

Nakoniec už musíme pridať len skupiny so služobnými údajmi. V [2] sa neuvádza akým spôsobom boli tieto skupiny kódované. Je tam uvedené len to, že služobné údaje boli prvé a posledné dve skupiny depeše. Obsahovali údaje o nastavení prvého písmena hesla a o výške (počte riadkov) transpozičného trojuholníka. Keďže nevieme ako tieto údaje boli zakódované, pre tento príklad zvolíme nasledovný spôsob:

Prvá pätica znakov bude pozostávať z prvého znaku denného hesla a jeho poradového čísla v dohodnutom hesle, pričom toto číslo bude kódované dvojciferným číslom podľa W tabuľky zo strany 2. Druhá pätica znakov bude pozostávať z dvojmiestného čísla určujúceho počet riadkov transpozičného trojuholníka, pričom toto číslo bude kódované podľa W tabuľky, a z jedného náhodne zvoleného znaku. V našom príklade je prvý znak denného hesla M, jeho poradové číslo je 21 a počet riadkov trojuholníkovej tabuľky je 09. Takže dve pätice služobných údajov budú: MWJWI WHWQD. Tieto služobné údaje pridáme na začiatok a koniec depeše[3]. V záhlaví depeše sa potom zrejme uvádzal pre kontrolu len počet skupín depeše, pretože všetky ostatné údaje potrebné k dešifrovaniu už máme obsiahnuté priamo v depeši. Po pridaní služobných údajov dostávame depešu:

```
017 GR
MWJWI WHWQD LWVEM QREQA VSLSS AIVQA NLIKW XUTWX CQNXN ZABMD
QXSEY SAYIX NAYQI SAPOX DECXX MWJWI WHWQD
```

ktorá je týmto pripravená na odoslanie.

7.2 Postup pri šifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii text na šifrovanie.

b. Máme dohodnuté jedno zo štyroch daných hesiel.

c. Je daný deň šifrovania.

Potom šifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Text, ktorý ideme šifrovať, prepíšeme len pomocou 26 znakov medzinárodnej abecedy.

2. Interpunkčné znamienka . : , - / ! ? a cifry zapisujeme pomocou dvojíc znakov podľa tzv. W tabuľky, uvedenej na strane 2.

3. Medzery sa nahrádzajú dvojicou znakov QQ alebo XX a za špeciálnymi znakmi sa medzery nepíšu, podobne ako tomu bolo aj pri iných šifrách.

[3]Samozrejme, že v skutočnosti sa to robilo iným spôsobom a služobné údaje sa nejakým spôsobom maskovali, aby neboli takto nápadné. Uvedený spôsob ich zápisu je vymyslený len pre náš príklad, pretože nemáme žiadne informácie o ich reálnom kódovaní.

4. Podľa dĺžky textu pripraveného na šifrovanie určíme potrebný počet riadkov transpozičného trojuholníka. Počet znakov z bodu 3 zväčšíme o 8, t.j. 5 adresovacích znakov na začiatku a 3 podpisové znaky na konci textu. Okrem toho ak tento počet znakov nie je násobkom 5, na koniec textu náhodne doplníme potrebný počet znakov. To bude celková dĺžka šifrovaného textu k. Potrebný počet riadkov transpozičného trojuholníka bude najmenšie prirodzené číslo n, ktoré vyhovuje nerovnosti $k \leq n^2$ a dĺžka posledného riadku transpozičného trojuholníka bude $d = 2n - 1$ znakov.

5. Z dohodnutého hesla zostrojíme denné heslo. Ako prvý znak denného hesla vezmeme ten znak dohodnutého hesla, ktorého poradie zodpovedá dňu šifrovania. Od neho potom cyklicky berieme taký počet znakov, aká je dĺžka posledného riadku transpozičného trojuholníka. Ak je dĺžka posledného riadku väčšia, než je celkový počet znakov dohodnutého hesla, tak toto heslo opakujeme, kým nedostaneme potrebný počet znakov.

6. Denné heslo obvyklým spôsobom vyčíslime podľa medzinárodnej abecedy. Týmto vyčísleným denným heslom očíslujeme stĺpce transpozičného trojuholníka aj transpozičnej tabuľky, ktorá bude mať rovnaký počet stĺpcov ako je počet znakov posledného riadku trojuholníka.

7. Text určený na šifrovanie zapíšeme do transpozičného trojuholníka po riadkoch zľava doprava a zhora nadol.

8. Z transpozičného trojuholníka text vypisujeme po stĺpcoch zdola nahor. Poradie stĺpcov je určené vyčísleným denným heslom. Znaky zapisujeme do transpozičnej tabuľky po riadkoch zľava doprava a zhora nadol.

9. Z transpozičnej tabuľky text vypisujeme po stĺpcoch zhora nadol. Poradie stĺpcov je určené vyčísleným denným heslom. Znaky zapisujeme v päťmiestnych skupinách.

10. Na začiatok a koniec depeše ešte doplníme služobné údaje. **Nevieme ako sa v skutočnosti tvorili skupiny služobných údajov. Tu popisovaný postup je vymyslený! Vieme len, že služobné údaje obsahovali informáciu o prvom znaku denného hesla, počte riadkov transpozičného trojuholníka a boli zapísané v prvých a posledných dvoch skupinách depeše.** V našom príklade bude prvá pätica znakov pozostávať z prvého znaku denného hesla a dvojciferného čísla udávajúceho jeho poradie v dohodnutom hesle. Druhá

pätica znakov bude pozostávať z dvojciferného čísla určujúceho počet riadkov transpozičného trojuholníka a z jedného náhodného znaku. Všetky čísla budú kódované podľa `W` tabuľky (str. 2).

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

7.3 Postup pri dešifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii kompletný text zašifrovanej depeše.

b. Máme dohodnuté jedno zo štyroch daných hesiel.

Potom dešifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Na základe návestia overíme kompletnosť depeše (počet cifier). Návestie depeše potom vynecháme, pretože ho už nebudeme potrebovať.

2. Prvé a posledné dve pätice depeše obsahujú služobné údaje. Prvá pätica obsahuje prvý znak denného hesla a jeho poradie v dohodnutom hesle, čo je vlastne deň šifrovania. Druhá pätica obsahuje dvojciferné číslo udávajúce počet riadkov transpozičného trojuholníka a jeden náhodný znak.

3. Po získaní nastavenia denného hesla a výšky transpozičného trojuholníka môžme vynechať prvé a posledné dve skupiny služobných údajov.

4. Poznáme počet riadkov trojuholníka a teda aj dĺžku jeho posledného riadku, čo je zároveň šírka transpozičnej tabuľky. Poznáme aj dĺžku depeše bez služobných údajov, takže vieme ktoré stĺpce tabuľky a trojuholníka sú kratšie.

5. Zostrojíme a vyčíslime denné heslo a označíme ním stĺpce trojuholníka a tabuľky.

6. Znaky depeše zapisujeme do tabuľky po stĺpcoch zhora nadol. Poradie stĺpcov je určené vyčísleným heslom. Pritom rešpektujeme dĺžku jednotlivých stĺpcov, ktorú poznáme.

7. Z tabuľky vypisujeme znaky po riadkoch zľava doprava a zhora nadol. Zapisujeme ich do trojuholníka po stĺpcoch zdola nahor. Poradie stĺpcov je určené vyčísleným heslom. Pritom opäť rešpektujeme dĺžku jednotlivých stĺpcov, ktorú poznáme.

8. Z trojuholníka vypisujeme znaky po riadkoch zľava doprava a zhora nadol. Dostávame tým text depeše.

9. Na začiatku a konci depeše sú adresovacie znaky vytvorené z prvých troch znakov denného hesla. Tieto môžme vynechať. Na začiatku je za týmito znakmi ešte bodka v tvare `WA` a na konci môžu byť za týmito znakmi ešte nuly. Tieto samozrejme tiež vynecháme.

10. Dvojice `QQ` a `XX` predstavujú medzery. Zapíšeme ich v pôvodnej podobe. Podobne niektoré špeciálne znaky a číslice sú kódované podľa `W` tabuľky (str. 2). Tiež ich zapíšeme v pôvodnej podobe.

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

7.4 Lúštenie

Táto šifra je transpozičná. Je to síce pomerne „komplikovaná“ transpozícia, ale v konečnom dôsledku len transpozícia. Znamená to, že ak si vezmeme dva rovnako dlhé texty a zašifrujeme ich tým istým heslom, zašifrované texty budú mať rovnaký anagramový sled. Na lúštenie môžme pri rovnako dlhých textoch a rovnakom šifrovacom hesle použiť anagramovú metódu.

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. sCrib –Hardwarový správce hesel aneb kapesní Enigma

Dan Cvrcek, Smart Architects (Cambridge UK)
e-mail dan@smartarchitects.co.uk

Problém

Loni v létě jsem přemýšlel do jakého problému se pustit. Hledal jsem něco co by bylo zajímavé pro mě, ale také něco co by řešilo problém počítačových uživatelů. Celkem rychle jsem došel k tomu, že problém se kterým se snad všichni potýkáme jsou hesla. Kromě toho, že jich potřebujeme stále více, tak se také staly jedním z hlavních cílů hackerů.

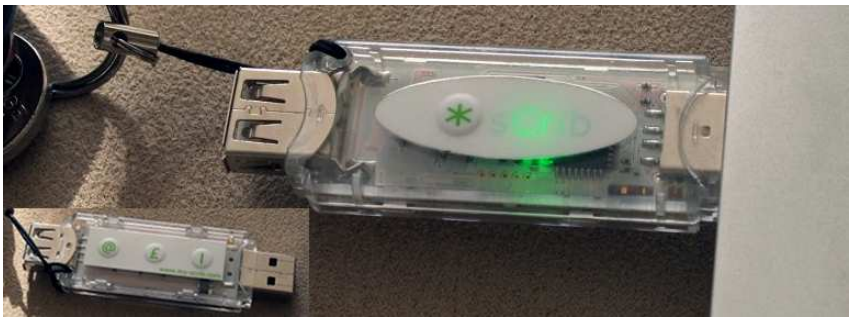
Samozřejmě existuje množství různých autentizačních systémů, které se snaží nahradit hesla; od biometrických čteček, přes čipové karty, po generátory jednorázových hesel. Jejich společným jmenovatelem je, že vyžadují speciální server, bez kterého jsou bezpečnostní tokeny nepoužitelné.

Otázka kterou jsem si kladl byla jestli možné zlepšit bezpečnost hesel a přitom zachovat jejich univerzálnost a snadnost používání.

Úvodní nápad

Odpověď na svoji otázku jsem „našel“ v klávesnici. Klávesnice je zařízení, které funguje na každém počítači. Umožňuje posílat data do počítače a pokud se lidská ruka nahradí procesorem, tak rychlost psaní umožňuje přenést dost informací pro většinu bezpečnostních aplikací. Tak vznikl první návrh sCribu (smart crib = chytrý tahák).

Současná implementace sCribu reprezentuje nejjednodušší variantu, ale i tak obsahuje několik zajímavých bezpečnostních aspektů. Fyzická implementace obsahuje dva USB porty. Jeden pro připojení k počítači, druhý pro připojení ke klávesnici při používání stolního počítače doma, nebo v kanceláři. Tlačítka umožňují vybrat jedno z devíti až dvanácti hesel (až tři hesla je možné vyměnit za OTP generátory). Tři hesla pod každým tlačítkem je kompromis mezi použitelností a požadavkem na co největší počet hesel. Pokud je připojena klávesnice, tak je možné používat klávesové zkratky pro výběr hesla.



sCrib také nabízí až 3 generátory jednorázových hesel (OTP), které implementují standard OATH HOTP [1]. sCrib vygeneruje při inicializaci OTP generátoru počáteční tajemství a vypíše ho do počítače. Jakmile jej obdrží server, tak dojde k synchronizaci mezi sCribem a serverem a uživatel může začít používat vybraný OTP generátor pro přihlašování.

Kryptografie

Základem všeho je 160 bitový náhodný řetězec, který pochází z mikrosekundového časovače. Z hlediska kryptografie jsou statická hesla a OTP generátory nezávislé. Hesla jsou generována z náhodného řetězce vytvořeného při inicializaci sCribu, zatímco inicializace OTP generátorů používá řetězec, který se aktualizuje s každým připojením sCribu k počítači. Statická hesla jsou generována diverzifikací základního řetězce pomocí hašovací funkce.

Všechna statická hesla jsou odvozena z jednoho 160 bitového řetězce. Tento řetězec je možné vytisknout a vytvořit tak záložní kopii pro případ ztráty sCribu.

Derivace hesel používá vyhledávací tabulku se znaky, které se mohou vyskytnout v hesle (aktuálně je to 78 znaků) a následující algoritmus.

1. H_0 – úvodní řetězec
2. $H_1 = H(H_0)$
3. $H_2 = H(H_0 \,||\, H_1 \,||\, 0)$ – úvodní diverzifikace oddělující použití H_0 pro statická hesla.
4. Pro každé heslo – *index = 0 .. N* vygeneruj K_N znaků; počítadlo znaků – *delka* – je inicializováno na nulu
    a. $Hx = H(H_2 \,||\, N \,||\, delka \,||\, ID_N)$
    b. *Counter = 0*
    c. Další znak
        i. Pokud už nemáme dostatek bitů pro další znak, aktualizuj $Hx = H(H_2 \,||\, N \,||\, delka \,||\, ID_N)$ a *Counter=0*
        ii. Index = 7 bitů z *Hx* počínaje bitem *Counter*
        iii. Pokud je *Index* > znaků v tabulce tak *Counter = counter + 1* a opakuj od kroku i.
    d. Najdi znak v tabulce na pozici *Index*
    e. Pokud parametry hesla s novým znakem nesplňují požadavky, tak jdi zpět na krok c.
    f. Přidej nový znak k heslu a jdi na krok c. dokud nemáme potřebnou délku hesla *delka = delka + 1*

Funkce *H()* je v současné době SHA-1. Parametr jehož význam jsme ještě nezmínili je ID_N. ID_N je pořadové číslo verze hesla s indexem *N*. Pořadové číslo je 0 na počátku a zvětší se o 1 pokaždé když uživatel změní dané heslo (požadavek firem na pravidelnou změnu hesla).

Algoritmus je navržen tak, aby znalost jednoho hesla neprozradila nic o žádném jiném hesle – předpokládáme, že funkce *H()* je kryptograficky bezpečná jednosměrná funkce. Kroky 2 a 3 nejsou nutně potřebné a jsou přidané jako pojistka proti implementačním chybám. Zabrání kompromitaci hesel při náhodném použití H_0.

OTP generátory potřebuje pro svou inicializaci počáteční tajemství. Toto tajemství je výstup z hašovací funkce: $H(H_{OTP} \,||\, index \,||\, index)$, kde index je pořadové číslo OTP generátoru – sCrib umožňuje používat až 3 OTP generátory, takže uživatel může používat 3 různé servery.

Kvalita hesel

Hlavním problémem je fakt, že některé servery omezují sílu hesel. Ať je to jejich délka, nebo množina znaků, které je možné použít. Implicitně generuje sCrib hesla o délce 20 znaků, ale

jedna skupina hesel má délku jen 14 znaků (maximální délka hesel ve Windows až do verze NT a následně v množství dalších aplikací – např. SAP neumožňuje delší hesla) a jedno heslo je jen 12 znaků dlouhé a neobsahuje žádné speciální znaky.

Kvalita hesel je taková, že se obvykle nebojím, když někdo vidí moje heslo na obrazovce. Zapamatovat si „1ZRy8.-9UYGv-W:+8WS0", "3vu_P_zE1A2-pR0YOsNx", nebo "3K_Pa-9ND?Vw-/ar5F]2O" není jednoduché.

Správa klíčů ... vlastně hesel

Ve chvíli kdy jsou hesla na tokenu místo v hlavě, tak je možné začít budovat kompletně nový systém pro správu hesel ať už by tento systém byl centralizovaný, nebo decentralizovaný. sCrib podporuje centrální správu jednak tím jak odvozuje hesla a také tím, že je možné sCrib inicializovat tajemstvím vygenerovaným jiným zařízením.

Token je možné předávat mezi uživateli, např. administrátory pracujícími na směny. Předáním sCribu je možné omezit přístup do určitých systémů časově. Pokud nakonfigureme interní čítač, tak můžeme omezit počet použití hesla.

Síla hesel je ekvivalentní síle kryptografických klíčů, takže je možné hesla použít jako součást kryptografických protokolů. Toto je možné téma pro diplomovou práci, nebo i výzkumný projekt v oblasti bezpečnostních protokolů s omezenou rychlostí komunikace.

V komerční praxi jsem se setkal s několika případy, kdy bylo potřeba zajistit přítomnost dvou osob pro určitou funkci (dual control), kde takový požadavek před tím neexistoval a autentizace vyžadovala jen jedno heslo. Dva USB porty sCribu umožňují propojit dva sCriby za sebe a zajistit dual control i v případě, že autentizace je pomocí jednoho hesla.

Dalším příkladem je situace, kdy je určitý systém spravován skupinou administrátorů, kteří sdílí jedno heslo (od Windows serverů, přes aktivní síťové prvky po kryptografické systémy). Pokud jeden z administrátorů opustí firmu, tak by se heslo mělo změnit a všichni administrátoři by se měli naučit nové heslo.

Pokud jsou hesla na tokenu jako je sCrib, tak aktualizace hesel je jednoduchou záležitostí, buď si všichni aktualizují příslušné heslo, nebo se existující tokeny znovu inicializují pomocí centrální administrace.

Jak se sCrib používá

sCrib je navržen tak, aby jeho používání bylo co nejjednodušší a určité vlastnosti chování je možné změnit jednoduchou konfigurací sCribu při jeho výrobě.

Po prvním připojení k počítači sCrib automaticky nasbírá potřebné množství náhodných dat a vygeneruje úvodní množinu hesel. V této chvíli je možné ho začít používat. Pokud se ovšem chcete pojistit proti ztrátě sCribu, tak doporučujeme vytištění, nebo bezpečné uschování inicializačního tajemství. Toto je možné vytisknout stiskem vrchního tlačítka (∗). Vyvinuli jsme jednoduchý Javascript program pro rekonstrukci hesel z inicializačního tajemství, který budou uživatelé moci používat.

Na spodní straně jsou tři tlačítka, pro tři kategorie hesel. Každé tlačítko je možné stisknout jednou, dvakrát, nebo tříkrát pro vyvolání jednoho ze tří hesel. Další tři hesla je obdobně možné vyvolat horním tlačítkem.

Když se rozhodnete používat sCrib pro přihlášení k určitému účtu, tak je třeba změnit stávající heslo na heslo ze sCribu. Postupujete jako při obvyklé změně hesla a když jste vyzváni zadat nové heslo, stisknete tlačítko, které chcete používat pro daný účet. Nové heslo je vypsáno do formuláře a můžete dokončit proces změny hesla. Při přihlášení pak už jen stisknete tlačítko se správným heslem.

OTP generátory jsou přístupné přes horní tlačítko (∗) až po inicializaci – současný stisk jakýchkoliv dvou tlačítek po dobu 3 sekund (signalizace pomocí modré diody) a následný výběr OTP generátoru jedním, dvěma, nebo třemi stisky tlačítka (∗). Tato sekvence způsobí vypsání inicializačního tajemství OTP generátoru do počítače. Od té chvíle je dané statické heslo nahrazeno OTP generátorem.

Co dál

V současné době plánujeme několik rozšíření sCribu. Nejjednodušší varianta je přidání funkcí pro protokoly typu výzva-odpověď, které umožňují implementovat autorizaci transakcí. Uživatel přepíše výzvu na klávesnici a sCrib ji doplní kryptografickou odpovědí.

Z hlediska uživatelského rozhraní uvažujeme také o implementaci jednoduchého programu pro počítač, který by pomohl vybrat správné heslo pro danou internetovou aplikaci. Na jednu stranu nechceme příliš omezit univerzálnost sCribu, ale např. diverzifikace hesel podle URL se zdá být pro některé uživatele zajímavé.

Původní návrh sCribu předpokládal, že bude používat čipovou kartu pro kryptografické operace a pro uložení klíčů a hesel. Tuto variantu jsme otestovali ve vývojovém prostředí a sCrib pak v této konfiguraci poskytuje ochranu dat na úrovni certifikace čipové karty (obvykle podle standardu FIPS140-2).

sCrib má svůj web – www.my-scrib.com, s aktuálními informacemi.

[1] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen: HOTP: An HMAC-Based One-Time Password Algorithm, RFC 4226, 2005.

C. 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
21. - 22.09.2011	09:00–17:00	Pavel Vondruška	17	

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/

D. KEYMAKER – studentská soutěž v rámci workshopu Mikulášská kryptobesídka 1.–2. prosinec 2011, Praha , http://mkb.buslab.org/

Mikulášská kryptobesídka přichází letos již v 11. ročníku. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *1. prosince 2011* a půldne prezentací příspěvků a diskusí v pátek *2. prosince 2011*. Pro workshop jsou domluveny zvané příspěvky:

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

KEYMAKER – Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie, počítačové a komunikační bezpečnosti a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Příspěvek pro KEYMAKER má 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. Přijímány jsou články, bakalářské či diplomové práce, nebo jiná kvalitní ucelená díla, kde v případě rozsahu nad 15 stran požadujeme výtah podstatného obsahu v max. rozsahu 8 stran, s vlastní prací jako přílohou.

Mezi autory nejlepších příspěvků PV rozdělí *finanční odměny v celkové výši 105 tisíc Kč*. Oceněno bude min. 3 a max. 7 příspěvků. Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *31. října 2011*. Příspěvek pak musí být prezentován na workshopu.

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 PDF, příp. RTF a to tak, aby na uvedenou adresu přišly nejpozději do *3. října 2011*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2011 – navrh prispevku KEYMAKER“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Důležité termíny

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

Programový výbor

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

E. O čem jsme psali v létě 2000 – 2010

Crypto-World 78/2000

Příloha : 10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 78/2001

Příloha : priloha78.zip (dopis pana Sůvy - detailní informace k horké sazbě, viz. článek Záhadná páska z Prahy, Crypto-World 6/2001)

Crypto-World 78/2002

Crypto-World 78/2003

Crypto-World 78/2007

Crypto-World 78/2008

Crypto-World 78/2009

Přílohy: Simulátor šifrátoru ŠD-2 http://crypto-world.info/soutez2009/sd2/cti.txt
(viz článek Rekonstrukce šifrovacího stroje ŠD-2)
Program RSAM.EXE (viz článek Malá soutěž v luštění RSA – řešení).

Crypto-World 7-8/2010

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

Všechna práva vyhrazena. Tato publikace ani žádná její část nesmí být reprodukována nebo šířena v žádné formě, elektronické nebo mechanické, včetně fotokopií, bez písemného souhlasu vydavatele.

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