Crypto-World

Informační sešit GCUCMP

Ročník 6, číslo 11/2004 **15. listopad 2004**

11/2004

Připravil: Mgr. Pavel Vondruška

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

Obsah :

Příloha : **Crypto-World 11/2004 – speciál (24 stran)**
(obsahuje rozsáhlý článek V.Klíma : Nedůvěřujte kryptologům,
ke stažení na adrese : http://crypto-world.info/index2.php?vyber=casop6)

A. Soutěž 2004 – úlohy závěrečného kola!

Mgr. Pavel Vondruška, pavel.vondruska@crypto-world.info

Před dvěma měsíci odstartovala tradiční podzimní soutěž v luštění jednoduchých šifrových úloh, kterou náš e-zin od roku 2000 pravidelně pořádá. Děkuji vám za velký zájem a řadu zajímavých e-mailů. Z nich vím, že používáte k řešení různé programy, které jsou na Internetu dostupné, píšete vlastní pomocné programy a v několika případech řešíte úkoly dokonce kolektivně. Jeden ze čtenářů (zúčastnil se řešení všech soutěží od roku 2000) poslal seriál krásných fotografií své pomocnice. Jednu z fotografií, kde pomáhá řešit transpozici, otiskuji.

Vše však končí a blíží se i závěr naší letošní soutěže. Dnes byly zveřejněny poslední tři úlohy (14.11.2004, 10.00 hod).

S napětím očekávám, kdo dokáže jako první projít úskalím všech mnou připravených šifrových textů. Celkový vítěz bude mimo ceny, která je určena pro prvé tři soutěžící, pozván pořadatelem na mezinárodní kryptologickou konferenci, která se koná 6.-7. prosince v Praze. Pořadatel 4. ročníku konference **Mikulášská kryptobesídka** (TNS, Trusted Network Solutions, http://www.tns.cz/kryptobesidka/) hradí za vítěze registrační poplatek a zve výherce na tuto akci.

Pro určení celkového pořadí bude rozhodující stav **1. prosince 2004 ve 22.00 hod.** První tři řešitelé získají láhev whisky (Scotch Whisky William Grant´s) se soupravou dvou skleniček, které jsou ručně vyrobeny ve sklárně, která se specializuje na historické repliky - tyto sklenky na whisky jsou inspirované renesančním sklem.

Ceny získají i další tři luštitelé, kteří budou vylosování z těch, kteří dosáhli alespoň patnácti bodů. V tomto případě se cena skládá opět z láhve whisky (stejné značky), ale doplněna bude pouze jednou sklenkou na whisky.

Losování proběhne ihned poté, co bude známo celkové pořadí. Výherci společně s vylosovanými řešiteli budou informováni e-mailem a současně s nimi dohodnu způsob předání ceny.

Využívám této příležitosti a děkuji touto cestou sponzorům, kteří věnovali ceny do letošní soutěže:
TNS (Trusted Network Solutions), http://www.tns.cz
firma Dignita, s.r.o., http://www.dignita.cz
Qobchod - Internetový obchod se sklem, http://www.qobchod.cz

Řešení všech předložených úloh najdete v e-zinu 12/2004.

Do této poslední etapy vám přeji hodně zábavy a dobré nápady !!!!

Přehled úkolů - III.kolo

Keby nebolo keby, boli bysme v nebi. (Slovenské přísloví)

Pro úplnost opakuji, že po vyřešení úlohy naleznete v otevřeném textu klíčové slovo, kterým prokážete, že jste úlohu správně vyřešili. Výjimkou je poslední úloha, kde naleznete návod, podle kterého toto slovo musíte teprve vytvořit… Pokud jste zaregistrováni, přihlásíte se ke svému účtu a přes www rozhraní jej u příslušné úlohy zadáte. **Toto slovo pište vždy velkými písmeny a bez mezer !**

Skupina úloh - *„pro profesionály“*

Fleissnerova úplná mřížka (3/1)
Počet bodů: 4
Nápověda: Fleissnerova otočná mřížka, Crypto-World 11/2004, str. 7-8

```
TEKRO JDDYC MZICD TIEAE SDTEN OIUCK SAPOM UETLA MJOEC ERNVA SLTEO OHKVZ
YOST (64 znaků)
```

Jednoduchá záměna (3/2)
Počet bodů: 4
Nápověda: Jednoduchá záměna, Crypto-World 10/2000, str. 2-4

```
TQSHF SGSJX UJXDH UQDWK ETSIB YCGFC IBEDI KDWSY EDIBW SBGCE SJXUY EDCFD
IWDNB GCECY CWUTC WQUQC KWCJX DHUQD WKCHC QDNCT XCKUI TCMEK XCWMY DQGCQ
YDEKD JCQDE CKKUE UIBGC EMJXD QEYSN XDJMF GUTCW ETSNE CMJDX DNPXD YCBCY
DYCGD FWUNT CGDOU MKYCX DWDBC DGDTK CXSHC YUEDG CWCKC NTKDX CHDQY CMJXC
KUIBM QWSIB MXDQW UIBHJ XCYCJ XMFDB MYEDC FDIWD BCBGC ECYCW UWCFG CXUQD
LCMEU CWDJU HWUKC XCGUW DCOXD OCWMF MQDMH WCWCP CTCJG CKWCC EJXCY WCKCW
OXDEM EKCWC YUGHY GCEKW UYCGD FWUTC NUEUT KDXCJ XUNSN BGCEC YCWUN JXUXT
GCYED IBQYC IDKQY CBGCE MHMYD QDWSI BEKCK MXDJM FGUTC WETDN MTCWQ UQCKC
YUNSW UNCGC ECMKD HWUYE MYTCD MTCHD NYKDK CMGCH DFMQD KDZKR EPUBL IKAND
CGDJC TXCIM PDJMY CQWUK DZKTU NHUET CGKDW KCTCW QUQCK YDKEU WMYDY CGDFW
UNTCG DOUMC KUNUJ XDHUQ DWKET DTXDE GCNCY SCNDX UITSJ XDHUQ DWKKC THUET
CGYDK EUWMW DPKDE WDPEU NCWDP QUETM KCYCW DPEUN HJMEC FDNYI DGSIB QDPUW
CIBCN DXUIT SIBYC GDFZZ (740 znaků)
```

Jednoduchá záměna (3/3)
Počet bodů: 6
Nápověda: Jedno-dvoumístná záměna , Crypto-World 11/2004, str. 5

```
70866 51748 67591 82170 17117 63090 85907 03075 32471 84916 26911 34908
27010 12459 09134 47184 91867 58285 16017 64717 49071 84707 53267 43686
68548 54758 22576 18575 70671 43463 21823 43691 63657 57148 53075 32757
09070 76536 85344 74519 17490 07436 85750 15109 16540 71753 46827 63684
75362 70768 48568 51568 28567 15907 64307 50309 06918 54747 04827 57068
56321 32404 34676 15906 01764 71746 67606 82656 74186 76170 18518 56913
16858 53682 91186 17184 75534 48676 68675 76827 52170 17675 47667 17418
47507 52368 53663 09091 82186 75075 84858 67558 56714 50425 34486 75702
56344 86758 28517 01854 51851 60176 47174 90718 43218 23475 51743 46217
01763 64766 74367 21341 76685 67167 65176 68460 63413 44867 66708 21867
58275 30341 91130 90700 75236 85363 07532 75706 85476 13018 57570 17451
76436 86767 18485 49131 68585 36829 11867 61826 01764 71747 53675 31134
91470 75363 41709 08575 36714 85702 67491 14347 14821 34590 70075 23685
36322 75367 09076 69110 86758 28675 76907 09130 75367 61347 13607 01316
85853 68291 42513 23413 26747 57013 16858 53682 91491 43217 00752 36853
60347 58475 23634 34452 74907 18403 62854 03682 34123 46217 01763 60752
36853 67090 30367 18485 63075 03063 60425 13467 06365 75075 30485 36707
57460 91474 36748 29074 75851 08676 75324 91821 85747 53470 75324 76671
74167 60682 90916 54034 13443 26234 19182 62418 18685 75911 70909 16826
85634 13267 41753 01548 23412 30908 54703 07532 47184 70131 68585 36829
14916 30454 82706 86764 28536 23447 14601 76471 74134 60757 63448 61718
47559 07451 76191 62684 85709 03036 71848 67582 75067 17436 70907 67530
13413 46857 59118 48518 26349 02753 65191 34474 75823 21916 76746 80496
(znaků 1380)
```

Šifra (systém neuveden) (3/4)
Počet bodů: 8
Nápověda: Nihil novum sob sole!

```
ESERZ DEJIN ILTON UHCYV ETHOL UOSOT OEZET ETSIP INVRP EMSIP SODAN TENAT
KLECE MSOME PTCAN NEMSI ZINYN SHCIN VATSE ZANET OVDYV KSECU EMHCY ATATS
OPOTK ATIZU EMSIP SEZAN NIPUK DNYVY ZETJE JAVYB IPICI ANEMS UKSEV SENIP
DIRTE EBAET ENDEC AKSIZ TERYN PCEZE NEMSI ELHEJ KENAD ORTNO LSINL OPOVO
NDELS HOLUI TNETY ETERO AZCEZ ETJED DOKAJ ZZAKU ETSJE SERYV TIILI OPOTU
NDELS HOLUI ISANU ETUOS ALBEZ ERPOH MAVIJ (znaků 335)
```

Průběžná statistika soutěže

Stav po zveřejnění závěrečných tří úloh soutěže (14.11.2004, 10:00)

Celkem soutěžících:	**96**
Počet soutěžících, kteří vyřešili alespoň 1 úlohu:	80
Počet soutěžících, kteří splnili podmínku k zařazení do slosování o ceny:	40
Nejvyšší počet dosažených bodů:	32
Celkem publikovaných úloh:	19
Maximální počet bodů, které lze dosáhnout:	50

Aktuální pořadí je k dispozici na stránce soutěže:
http://soutez2004.crypto-world.info/index.php?crypto=zebricek

B. Jedno-dvoumístná záměna

(vysvětlení principu úlohy 3/3)

Nápověda pro řešitele Soutěže 2004 (http://soutez2004.crypto-world.info/)

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

O tomto, v praxi běžně využívaném šifrovém systému, se stručně zmiňuje např. Jiří Janeček ve své knize Odhalená tajemství šifrovacích klíčů minulosti, Naše Vojsko, Praha 1994.

Další informace můžete najít v článku V. Klímy: Utajené komunikace - 5.díl: Šifry první světové války a další rozvoj kryptologie, Chip, září 1994, str. 210 - 215.
Systém je stručně popsán v odstavci *Převodové tabulky*, který začíná na straně 213 dole. Na straně 214 je pak uvedena autentická převodová tabulka známého revolucionáře Che Guevary (viz obrázek).
ftp://ftp.decros.cz/pub/Archiv/Publications/1994/chip-1994-09-213-213.jpg
ftp://ftp.decros.cz/pub/Archiv/Publications/1994/chip-1994-09-214-214.jpg

	8	2	0	6	4	9	1	3	7	5
	E	S	T	A	D	O	Y	-	-	-
3	b	c	f	g	h	i	j	.	;	,
7	k	l	m	n	'	p	q	/	/	
5	r	u	v	w	x	z				

Při této šifrové transformaci se převádí otevřený text na šifrový text opět pomocí substituce. V tomto případě se nahradí každé písmeno abecedy buď jednociferným nebo dvouciferným číslem. Aby byl text jednoznačně dešifrovatelný, musí se při sestavování tabulky vzít do úvahy, že číslice, které se vyskytují na „desítkových místech“ šifry již nelze využít pro jednotková místa šifry.

Počet řádků se u různých tabulek liší a kolísá od dvou do 4 (výjimečně do pěti). Závisí to samozřejmě na tom, kolik znaků má být tabulkou kódováno. Mimo abecedy se někdy do tabulky vkládají i znaky (viz tabulka Che Guevary) nebo dokonce číslice. Pro kódování číslic se někdy využívá pouze jeden znak, který pokud se použije, znamená, že následují číslice, a po jeho dalším použití se opět přechází do kódovaných znaků… Možných variant je celá řada.

Systém byl v praxi používán ještě přibližně před dvaceti lety tajnými službami (BND, CIA apod.). Sloužil k převodu otevřeného textu do číselné podoby. Protože by byl takto text lehce luštitelný (jak jste se sami mohli přesvědčit…), následovalo přičtení dohodnuté číselné sekvence – hesla. Pokud byla dodržena určitá pravidla a heslo nebylo kompromitováno, byla výsledná šifra při záchytu nerozluštitelná….

Blíže např. P. Vondruška: Soutěž 2001, II.část - Absolutně bezpečný systém, Crypto-World 10/2001. V tomto článku také najdete další příklad převodové tabulky jedno-dvoumístné záměny…

Jednoduchý příklad použití

I. Otevřený ukázkový text:
Jen malá ukázka, jak vypadá výsledný šifrový text.

Použitá převodová tabulka jedno-dvoumístné záměny

	0	1	2	3	4	7	8
	A	E	I	O	U	V	T
5	B	P	C	Q	D	R	F
6	G	S	H	U	J	W	K
9	L	X	M	Y	N	Z	

II. Úprava textu před převodem:
a) odstranění interpunkce a diakritiky:
Jen mala ukazka jak vypada vysledny sifrovy text

b) převod na velká písmena:
JEN MALA UKAZKA JAK VYPADA VYSLEDNY SIFROVY TEXT

III. Převod na šifrový text pomocí výše uvedené tabulky:
64194 920900 468097680 64068 793510540 79361901549493 61258573793 81918

IV. Závěrečná úprava šifrového textu (rozpis do pětimístných skupin):
64194 92090 04680 97680 64068 79351 05407 93619 01549 49361 25857 37938 1918 (64 znaků)

Při luštění je potřeba nejprve zjistit, které cifry jsou „desítkové“…. (zkuste se zamyslet např. nad otázkou, zda může být v našem konkrétním příkladě číslice 8 desítková ?)

Můžete se dále pokusit např. desítkové číslice tipovat a zjistit, kolik by vzniklo různých znaků otevřeného textu (očekávaná hodnota musí odpovídat mezinárodní abecedě – prozradím, že tabulka použitá v soutěžní úloze obsahuje pouze abecední znaky a jeden speciální znak a to pro konec textu…). Dále je vhodné se podívat, zda vyhovuje statistika rozložení takto získaných znaků rozložení v českém jazyce (soutěžní úloha je v českém jazyce) ….

Pokud se vám podaří odhalit desítkové číslice, máte vyhráno, další postup je již zcela shodný jako při řešení klasické jednoduché záměny.

C. Fleissnerova otočná mřížka

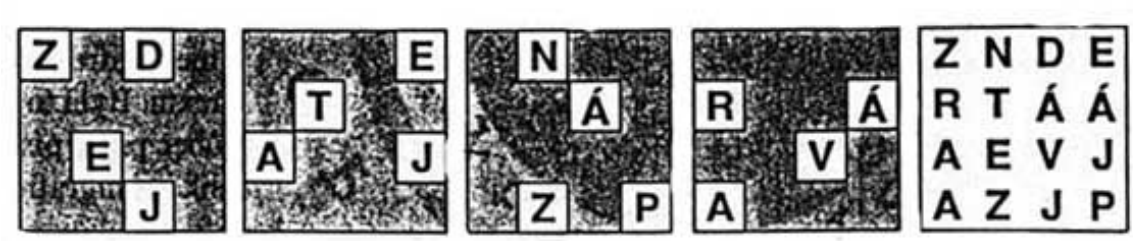
Nápověda pro řešitele Soutěže 2004 (http://soutez2004.crypto-world.info/)

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Nejprve se seznamte s citací jednoho z mála článků v češtině, který se Fleissnerově systému věnuje a který lze na Internetu vyhledat. Tímto článkem je **V. Klíma: Utajené komunikace - 4.díl : Od novověku do 20. století, CHIP č. 8, srpen 1994, str. 118 - 121.**
ftp://ftp.decros.cz/pub/Archiv/Publications/1994/chip-1994-08-120-120.jpg

Fleissnerova otočná mřížka

Tuto velmi hezkou transpoziční šifru popsal jako první Fleissner von Wostrowitz ve své knize o kryptografii v roce 1881. Po spartském dřevěném válci "Skytalé" je to druhá známá mechanická pomůcka realizující transpozici. Princip je velmi jednoduchý. Ve čtverci n x n políček vystřihneme n x n/4 políček tak, aby při postupném otáčení vždy o 90 stupňů vzniklé otvory ukazovaly vždy na jiná políčka (viz obrázek). Vzniklou mřížku přiložíme na papír, do okének vpisujeme otevřený text a poté mřížkou otáčíme vždy o 90 stupňů. Nakonec na papíru vznikne čtverec souvisle vyplněný písmeny. Šifrový text se z něho vypisuje po řádcích. Šifra se zalíbila nejen J. Vernerovi, který ji použil v "Matyáši Šándorovi", ale i Němcům, kteří ji jeden čas používali v první světové válce jako polní šifru.



OT: Zde je tajná zpráva
ŠT: ZNDE RTÁÁ AEVJ AZJP

Obr. Fleissnerova mřížka.

č. 8 - Srpen 1994

Nyní se seznámíme se stručným návodem, jak lze luštit tento systém.
Pro jednoduchost budeme tyto rady konkretizovat pro mřížku uvedenou v citovaném článku:

1) Rozdělíme si šifrový text na sekvence délky 4 (obecně délky n)
ZNDE
RTÁÁ
AEVJ
AZJP

2) Odhadneme, kolik znaků bude z každého úseku v hledaném otevřeném textu.
Víme, že při každém přiložení mřížky je potřeba přečíst 4 znaky otevřeného textu (jedná se o úplnou mřížku, tj. po čtyřech otočeních se vyčerpají všechny znaky tj. 16).
V jednom řádku lze tedy očekávat průměrně 1 znak otevřeného textu (přijměme hypotézu, že počet znaků otevřeného textu kolísá od 0 do 2 znaků).

3) Pokusíme se podle pravidel v bodě 2 sestavit čitelné slovo nebo alespoň úsek čitelného slova.

4) Zkontrolujeme správnost naší volby tím, že se podíváme jaké slovo by vznikalo

otočením o 90, 180, 270 stupňů …

5) Nesmíme zapomenout, že otočením souvislého úseku délky menší než 4 (obecně pro tabulku n*n, úseku menší než n*n/4) nemusí vzniknout řetězec, který je „souvislý“, tj. v otočení mohou nějaké znaky chybět !
(porovnej: otočením písmen ÁZP (z třetí polohy uvedené mřížky), která v otevřeném textu za sebou následují , dostanu písmena RVA ve čtvrté poloze mřížky, která za sebou v otevřeném textu nenásledují!)

6) Řetězce, které získáme otočením čitelného úseku, se snažíme doplnit – rozšířit na slovo v čitelné podobě (samozřejmě, že vybíráme již pouze s písmen, která nebyla dosud použita ani v jednom z otočení námi vytipovaného řetězce).

7) Potvrzené slovo dále rozšiřujeme, resp. rozšiřujeme řetězce získané otočením a postupně takto rekonstruujeme celý text.
Vyzkoušejte si na příkladě, který je v článku uveden!

Pomocný program na řešení úlohy 3/1 naší Soutěže 2004 na Fleissnerovu mřížku **připravil Pavel Hoffmann**, jeden z řešitelů probíhající soutěže. Rozhodl se poskytnout jej jako užitečnou pomůcku i ostatním soupeřům. Jeho nabídku rád zveřejňuji…

Date: Fri, 29 Oct 2004 22:40:22 +0200
To: <pavel.vondruska@crypto-world.info>
Subject: Re: Chyba v programu

Dobrý večer,
... na http://www.ngi.cz/fleissner.exe jsem umístil novou verzi programu.
Myslím, že tato verze již jako skutečná pomůcka sloužit může, takže pokud program shledáte jako užitečný, budu rád, když ho uveřejníte. Snad to někomu pomůže.

Jen stručný popis:
- zašifrovaný text je vypsán hned nahoře
- okno obsahuje 4 tabulky
- 1 zleva představuje základní polohu mřížky
- 2 zleva je otočení mřížky o 90°
- 3 zleva je otočení mřížky o 180°
- 4 zleva je otočení mřížky o 270°
- po kliknutí na znak v libovolné tabulce se aktualizuje mřížka a znak se probarví černě, zároveň se červeně probarví pozice téhož znaku při ostatních natočeních
- pod každou tabulkou se průběžně vypisuje text který je skrze mřížku "vidět"
- pokud v dešifrovaném textu před konkrétním znakem může ještě ležet znak jiný, tak se před tímto vypíše tečka ".X"
- pokud v dešifrovaném textu za konkrétním znakem může ještě ležet znak jiný, tak se za tímto vypíše tečka "X."
- pokud dva znaky budou v dešifrovaném textu ležet bezprostředně vedle sebe, tak se mezi nimi tečka nevypíše "XX"
S pozdravem
Pavel Hoffmann

Literatura

[1] V. Klíma – Utajené komunikace, 4. díl, CHIP 8/1994, str. 120, ftp://ftp.decros.cz/pub/Archiv/Publications/1994/chip-1994-08-120-120.jpg

[2] Program Pavla Hoffmanna na luštění Fleissnerovy mřížky, http://www.ngi.cz/fleissner.exe

D. Kryptografie a normy
Formáty elektronických podpisů
(dokument ETSI TS 101 7733 - Electronic Signature Formats)

Jaroslav Pinkava, PVT a.s.

1. Úvod

Dokument, kterým se budeme v tomto článku (a v jeho pokračováních) zabývat, má za sebou již poměrně dlouhou (a dynamickou) historii. Vznikl [1] v rámci pracovní skupiny ETSI (http://portal.etsi.org/esi/el-sign.asp), první verze byla publikována v květnu 2000.

V dnešní době existuje již pátá verze tohoto dokumentu (prosinec 2003) a existuje také informativní [2] RFC s pořadovým číslem 3126 (září 2001), které odráží tehdejší (rok 2001) stav materiálu. Dokument má charakter technické specifikace. Z hlediska obsahu definuje celou řadu formátů elektronických podpisů a to včetně podpisů, které zůstávají v platnosti po dlouhou dobu. Zahrnuje to i důkaz platnosti těchto podpisů a to včetně situací, kdy se podepisující se či ověřující strana budou později pokoušet popřít platnost podpisů. V současné době je to jediný materiál, o který se lze opírat při konstrukcích formátů podpisů tak, aby tyto formáty odrážely potřeby dlouhodobé práce s elektronickými podpisy. Existuje řada implementací doporučení, která jsou v TS 101 733 obsažena. Materiál je také referencí, na kterou se odkazují v dalších normativních pracích, které jsou prováděny v oblasti archivace elektronických dat (materiály skupiny IETF-ltans, XML podpisy).

2. Východiska

Základní strany, které se podílí na dění okolo konkrétního elektronického podpisu (např. při obchodní transakci), jsou následující:
- podepisující strana (the Signer);
- ověřující strana (the Verifier);
- poskytovatelé důvěryhodných služeb (Trusted Service Providers - TSP);
- arbitr (the Arbitrator);

Podepisující strana - to je entita, která vytváří elektronický podpis. Jestliže podepisující strana podepíše digitální data prostřednictvím předepsaného formátu, pak toto reprezentuje závazek podepisující entity vzhledem k podepisovaným datům.

Ověřovatel - to je entita, které ověřuje (vyhodnocuje) elektronický podpis, může to být jedna konkrétní entita či to může být několik takovýchto entit.

Poskytovatelé důvěryhodných služeb - to je jedna či více entit, které pomáhají vytvořit důvěryhodné vztahy mezi podepisující se stranou a ověřovatelem. Podporují podepisující stranu a ověřovatele prostředky podpůrných služeb jako jsou certifikáty uživatelů, křížové certifikáty, časové značky, CRL, ARL, odpovědi OCSP.

Jsou využívány následující typy poskytovatelů důvěryhodných služeb:
- certifikační autority, poskytují uživatelům certifikáty veřejného klíče a revokační službu;
- registrační autority, umožňují provést identifikaci a registraci entit před tím, než CA vygeneruje certifikát;

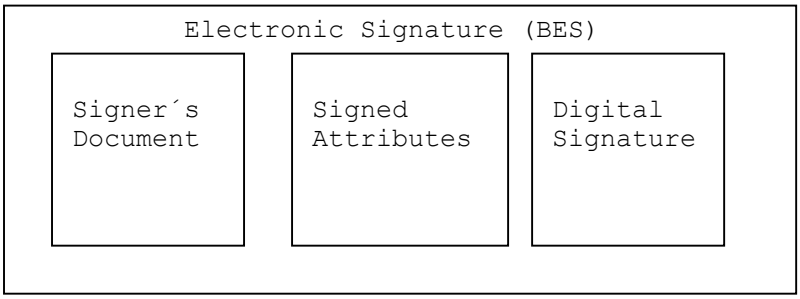
- důvěryhodná úložiště (repository authorities), např. adresáře; publikují CRL vydaná CA, podpisové politiky vydané vydavatelem podpisových politik a případně i certifikáty veřejného klíče;
- autority časových razítek;
- vydavatelé podpisových politik, definují podpisové politiky, které budou používat podepisující strany a ověřovatelé;
- v některých případech budou používány i atributové autority, které poskytují uživatelům atributy (vázané prostřednictvím atributových certifikátů na certifikáty veřejného klíče);

Arbitr je entita, která rozsuzuje v situacích, kdy vznikne nesouhlas mezi podpisující stranou a ověřovatelem.

3. Základní elektronický podpis - BES

Formát BES (basic electronic signature) - základní elektronický podpis, který obsahuje:

- podepisovaná data uživatele (např. uživatelův dokument) dle definice CMS (rfc.3369);
- soubor povinně podepisovaných atributů dle definice CMS (rfc.3369) a ESS (rfc.2634);
- další povinně podepisované atributy (definované dále);
- hodnotu digitálního podpisu spočtenou nad daty uživatele a případnými podepisovanými atributy dle postupu v CMS (rfc.3369);



Podle tohoto dokumentu ETSI ([1]) může základní elektronický podpis (BES) obsahovat také soubor dalších podepsaných atributů, případně i soubor nepodepsaných atributů.

Povinně podepsanými atributy jsou:
- Content-type (dle definice v rfc.3369 - specifikuje, že typem obsahu ContentInfo jsou "signed-data";
- Message-digest (dle definice v rfc.3369 - specifikuje, že je podepisován otisk zprávy z eContent OCTET STRING uvnitř encapContentInfo;
- ESS signing-certificate OR other-signing-certificate (dle definice v rfc.2634).

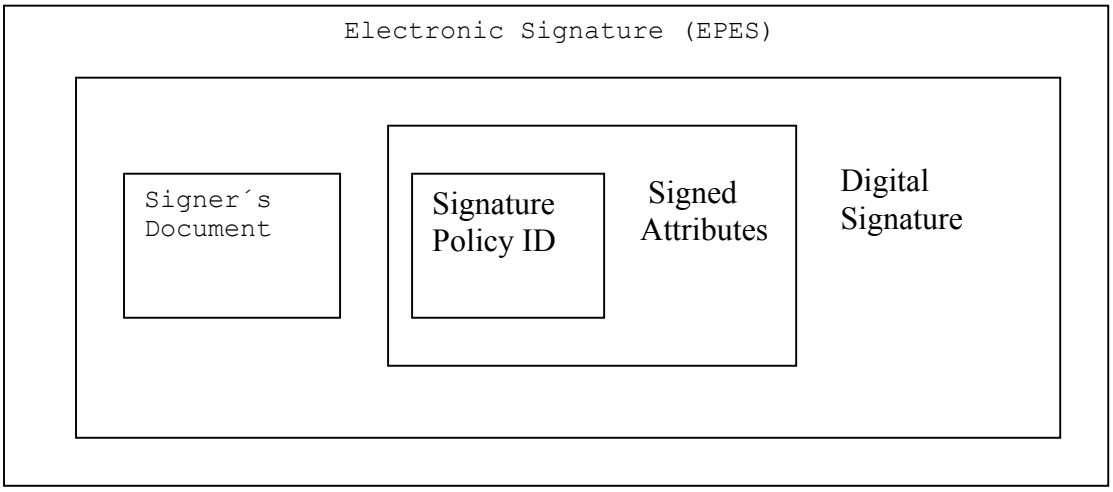
Nepovinné podepisované atributy mohou být:
- signing-time (rfc.3369);
- content-hints (dle ESS - rfc.2634 - informace k formátu podepisovaného obsahu);
- content-reference (dle ESS - rfc.2634 - spojuje žádosti a odpovědi při dvoustranné komunikaci);
- content-identifier (dle ESS - rfc.2634 - identifikátor pro předchozí atribut);

a další (commitment-type-identification; signer-location; signer-attributes; content-time-stamp).

BES může také obsahovat nepodepisované atributy (dle CMS, rfc.3369 a dle rfc.2634):
- CounterSignature (je-li požadován včleněný podpis).

BES je minimální formát elektronického podpisu, který je generován podepisující stranou. Neobsahuje dostatek informací, které jsou nezbytné pro jeho ověřování (z dlouhodobého hlediska), např. informace o revokacích. BES naplňuje požadavky kladené na elektronické podpisy definované Směrnicí Evropské Unie. Poskytuje základní prostředky pro autentizaci a ochranu integrity.

4. Elektronické podpisy s explicitní politikou - EPES



Formát EPES (Explicit Policy-based Electronic Signature) rozšiřuje definici elektronického podpisu tak, aby odpovídala identifikované podpisové politice. Zahrnuje v sobě podepsaný atribut (signature-policy-identifier), který je indikátorem, že má být použita specifikovaná povinná podpisová politika pro vytváření a ověřování podpisů.

5. Elektronické podpisy s časem - ES-T

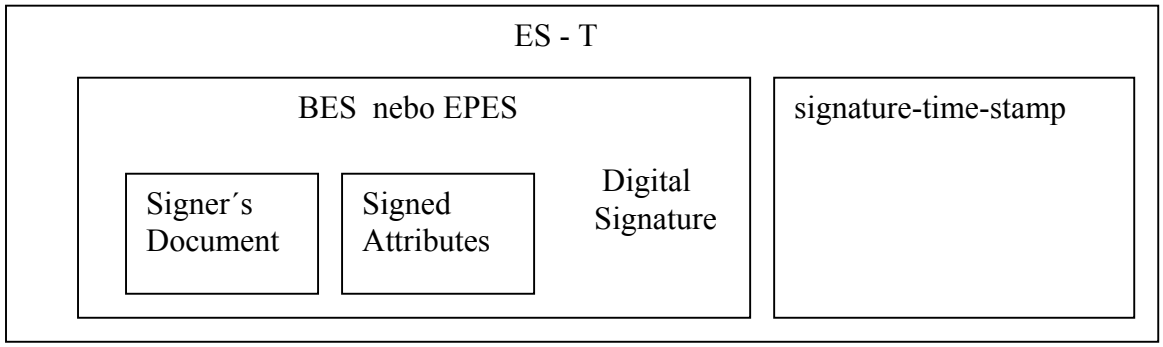
Kromě dvou výše popsaných výchozích formátů pro elektronický podpis popisuje dokument celou řadu dalších formátů, které již obsahují některé informace potřebné pro ověření elektronického podpisu. Tato data nazývá ověřovacími daty (validation data) a patří k nim:

- certifikáty veřejných klíčů;
- informace o revokačním statutu pro každý certifikát veřejného klíče;
- důvěryhodné časové značky;
- nebo i detaily podpisové politiky, která má být použita při ověřování elektronického podpisu.

Prvním z takových formátů je formát ES-T (Electronic Signature with Time), který obsahuje důvěryhodný čas asociovaný s elektronickým podpisem. Autoři dokumentu rozlišují dvě varianty:

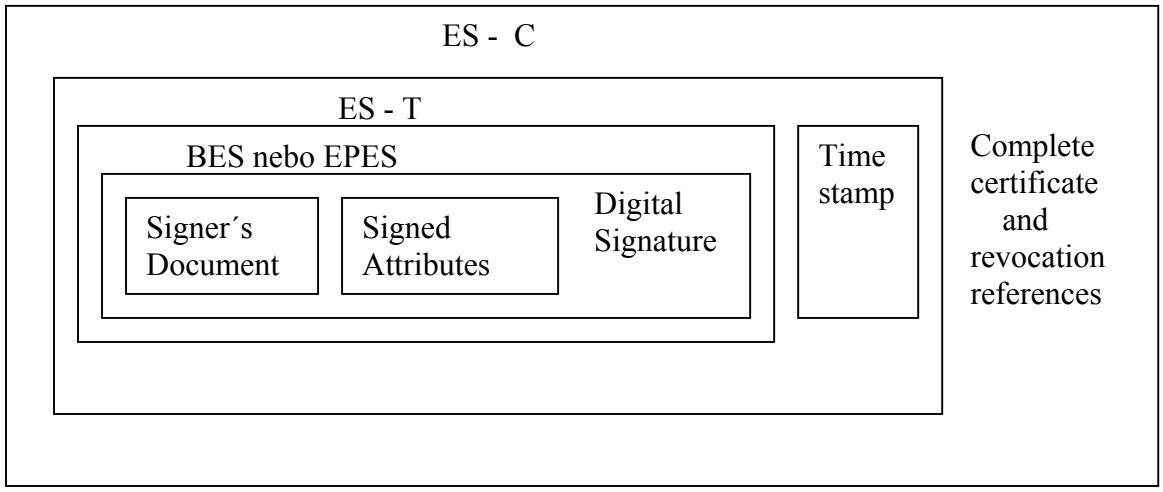
- situace, kdy časová značka (signature-time-stamp) je jako nepodepisovaný atribut přidávána k ES.
- časový marker poskytovaný důvěryhodným poskytovatelem času. Zde není k podpisu přidáván žádný atribut, ale je závazkem TSP poskytnout příslušný důkaz v situacích, kdy to bude vyžadováno.

Důvěryhodný čas je prvním krokem k poskytnutí ověření v dlouhých časových intervalech.



6. Elektronické podpisy s úplnými odkazy pro ověřování - ES-C

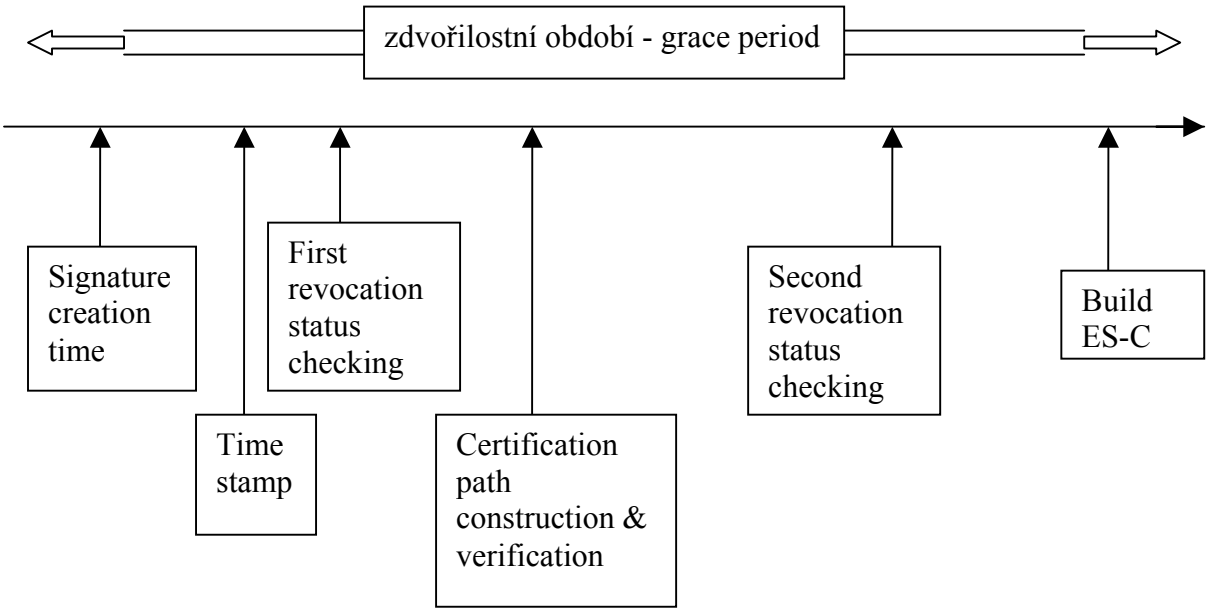
Tento formát ES-C (Electronic Signature with Complete validation data references) přidává k formátu ES-T ještě atributy complete-certificate-references a complete-revocation-references, které jsou definovány v tomto dokumentu ETSI ([1]).
První z těchto atributů (complete-certificate-references) obsahuje odkazy na všechny certifikáty v příslušné certifikační cestě, která je používána pro ověření podpisu.
Druhý atribut (complete-revocation-references) obsahuje odkazy na CRL a/nebo odkazy na odpovědi OCSP, které jsou používány pro ověření podpisu. Tím, že jsou zvlášť (kdekoliv) uloženy tyto odkazy, je umožněna redukce nezbytné velikosti ukládaného formátu elektronického podpisu.



Úplné odkazy (na certifikáty a revokace) jsou přidávány k ES-T jako nepodepsané atributy.

Z důvodů minimalizace rizika popření tvorby podpisu by měl být příslušný důvěryhodný čas (v ES-T) co nejblíže časovému momentu, kdy byl podpis vytvořen. Časová značka v ES-T musí být vytvořena dříve, než je certifikát (veřejného klíče párového k použitému podpisovému klíči) odvolán či vypršela jeho platnost.

Formát ES-C vytváří podepisující strana (či TSP) z důvodů minimalizace rizika (že podpis nebude ověřen). Ověřující strana by měla vytvořit ES-C, jestliže jsou již požadované komponenty ES-C dostupné. S tímto cílem je třeba také zvažovat určité "zdvořilostní" časové období (anglicky grace period), kdy je třeba počkat, až budou příslušné revokační informace k dispozici. Takto bude zajištěno, že certifikát nebyl odvolán v době, kdy byl podpis označen časovou značkou. Hodnoty velikostí těchto časových intervalů mohou být specifikovány v podpisové politice. Toto ilustruje následující obrázek.



V následujícím pokračování budou popsány tzv. rozšířené formáty elektronických podpisů.

7. Literatura

[1] ETSI TS 101 733, V.1.5.1, Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
[2] RFC 3126, Electronic Signature Formats for long term electronic signatures

E. Elektronická faktúra a elektronické daňové priznanie aj bez zaručeného elektronického podpisu

Ing. Radimír REXA, CSc. (R.Rexa@e-unicom.sk)

Novelami zákonov č.222/2004 Z.z. o dani z pridanej hodnoty a č.511/1992 Z.z. o správe daní a poplatkov, ktoré dňa 26.10.2004 schválila NR SR, sa zjednodušujú pravidlá pre nahradenie klasických papierových faktúr a daňových priznaní faktúrami a priznaniami elektronickými.

Dva roky od prijatia zákona č.215/2002 Z.z. o elektronickom podpise sa ukazuje, že na Slovensku bol týmto zákonom a jeho výkladom vytvorený model elektronického podpisu, ktorý je **zložitý**, veľmi **nákladný**, **nekompatibilný s Direktívou** 1999/93/EC Európskeho parlamentu a Rady už v základných pojmoch a naviac **má diskriminačný charakter**.

Iba šesťmesačné výsledky **Sociálnej poisťovne** s elektronickým zberom hlásení za zamestnancov jasne ukazujú, že používanie elektronických dokumentov je možné aj bez zložitej slovenskej mutácie zaručeného elektronického podpisu, a to i vo verejnom sektore. Niekoľkomiliónové úspory, ktoré táto elektronická agenda štátu prináša, boli silným argumentom aj pre **daňovú správu**, ktorá sa už dlhší čas snaží zjednodušiť a zefektívniť zber daňových priznaní a umožniť elektronický zber nie iba top klientom, ale čo najširším masám daňovníkov, pre ktorých používanie zaručeného elektronického podpisu sa ukazuje príliš nákladné a zložité. Ani pri klasických papierových daňových priznaniach neskúmame, akým perom (bezpečným zariadením), akým štýlom (bezpečnou aplikáciou) ho daňovník vyplnil, resp. podpísal. Prečo by sme pri elektronických podaniach mali vyžadovať vlastniť takéto zariadenie a aplikáciu, keď zo zaručeného elektronického podpisu nevieme overiť, či boli vôbec použité. Tým, že priznanie daňovník podá a daň zaplatí, si svoju daňovú povinnosť splní.

Keď si uvedomíme, že **klasická** papierová **faktúra** podpis obsahovať nemusí, bolo tiež nelogické, aby u faktúry elektronickej musel byť použitý iba najzložitejší druh podpisu elektronického. V záujme akceptovateľnosti elektronickej faktúry v členských krajinách EÚ je však potrebné rešpektovať Direktívu 2001/115/EC, ktorá vyžaduje garanciu **autenticity pôvodu** a **integrity obsahu** faktúry. Pre toho, kto nevie, ako tieto dve požiadavky splniť bez zaručeného elektronického podpisu, doporučujeme orientovať sa na tento zložitejší druh podpisu. Prijaté novely zákonov č. 511/1992 Z.z. a č. 222/2004 Z.z. takúto možnosť nezrušili.

Prijaté novely môžu byť námetom na zamyslenie či predsa len nie je vhodné **zjednodušiť slovenský model elektronického podpisu,** aby tí čo majú záujem šetriť štátny, či podnikový rozpočet zavádzaním jednoduchých elektronických agiend a služieb nemuseli rôznymi okľukami obchádzať diskriminačný § 5 ods.1, prípadne neprimeraný výklad zákona 215/2002 Z.z. zo strany NBÚ. Pri prípadnej novele je vhodné tento zákon viac priblížiť Direktíve 1999/93/EC, poučiť sa zo skúseností z okolitých krajín a nepodceňovať analýzu implementácie Direktívy v jednotlivých členských krajinách EÚ. Nepočúvaním a nerešpektovaním názorov z praxe bude totiž zákon odtrhnutý od reality a ostane iba brzdou elektronizácie, ktorú tí, ktorí problematike trochu rozumejú, budú obchádzať rezortnými zákonmi, resp. vlastnými podnikovými predpismi, či partnerskými zmluvami.

Na záver je dobré si uvedomiť, že bezpečnosť informačných technológií je veľmi dôležitá. Úroveň bezpečnosti však vždy musí byť kompromisom zohľadňujúcim potenciálne riziká, prínosy z elektronizácie a náklady pri danej úrovni bezpečnosti. Určitým zákonom globálne pripúšťať iba tú najvyššiu úroveň bezpečnosti je nesprávne.

F. Nedůvěřujte kryptologům

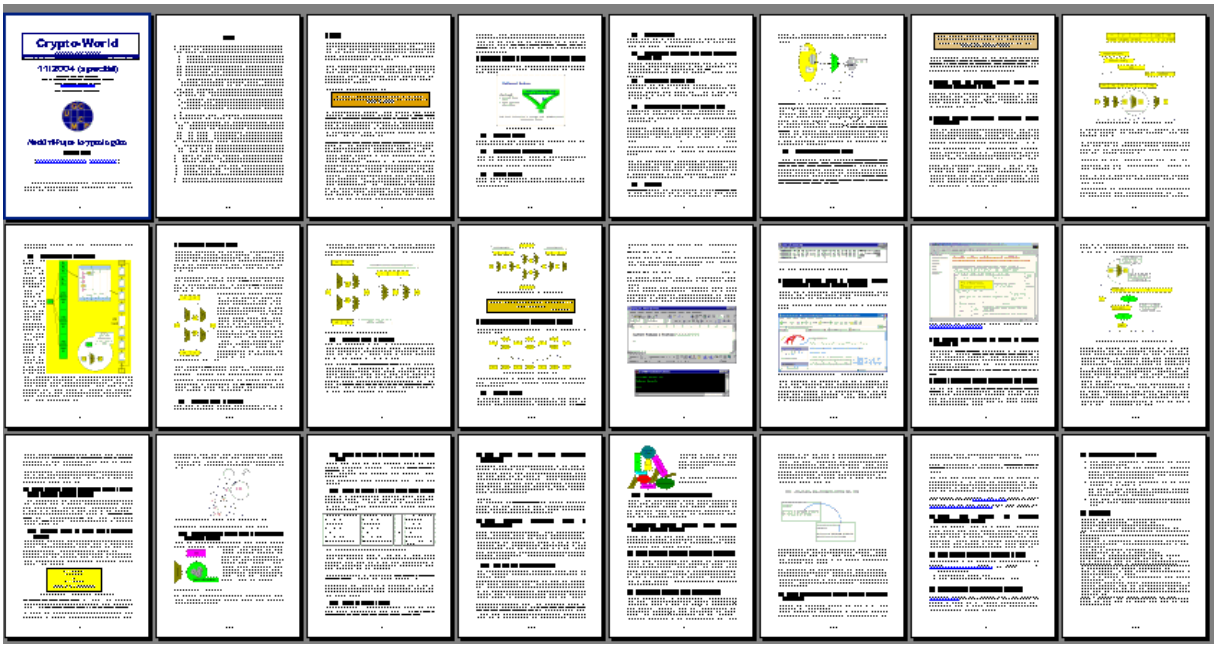
Vlastimil Klíma, v.klima@volny.cz

Příspěvek je určen těm, kdo nemají podrobné znalosti o hašovacích funkcích, ale přitom se jich nějakým způsobem týká jejich bezpečnost, poněkud otřesená v srpnu t. r. nalezením kolizí u několika hašovacích funkcí.

Abstrakt

Srpen t. r. přinesl nové objevy v kryptoanalýze, které budou mít vliv na bezpečnostní praxi v sektoru IS/IT. Jedná se o **prolomení několika hašovacích funkcí (MD5, MD4, SHA-0, HAVAL-128, RIPEMD)** v období konání konference CRYPTO 2004 v srpnu t. r., komplikované o to, že čínský výzkumný tým nezveřejnil metody prolamování, ale jen své výsledky. V příspěvku jsou uvedeny vlastnosti a různé způsoby využití hašovacích funkcí v moderních protokolech a aplikacích, **jsou vysvětleny a komentovány výsledky prolomení a jeho praktické důsledky**. Příspěvek vybízí k tomu, aby se změnil postoj ke kryptografickým technikám jako k něčemu zvláštnímu a pracovalo se s nimi jako s jakýmikoliv jinými bezpečnostními nástroji, to znamená a priori jim nedůvěřovat, sledovat vývoj v dané oblasti a běžně provádět update nebo upgrade. Na základě vývoje kryptologie v posledních desítkách let je vyvozen obecný závěr o nutnosti vyvíjet nové aplikace kryptograficky modulárně. Protože se to tak nedělalo, bude nyní obtížné vyměnit prolomené hašovací funkce, zejména MD5. V příspěvku se vysvětluje, kde je nutné MD5 vyměnit a kde ještě lze MD5 používat.
Těm, kdo nemají čas číst takový dlouhý dokument, je věnováno pětibodové manažerské shrnutí v závěru příspěvku.

Vybrané partie příspěvku byly předneseny v rámci vystoupení autora na konferenci IT & Security Conference, DCD Publishing, Hotel Diplomat, Praha, 10. - 11. 11. 2004



Tento rozsáhlý příspěvek vyšel jako Crypto-World 11/2004 – speciál. Zájemci si jej mohou stáhnout na adrese : http://crypto-world.info/index2.php?vyber=casop6

G. O čem jsme psali v listopadu 1999 – 2003

H. 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 P.Vondrušky a 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 sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:

http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze **jméno a příjmení, titul**, pracoviště (není podmínkou) a **e-mail adresu** určenou k zasílání kódů ke stažení sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info . Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
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@pvt.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/