Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 12, číslo 10/2010 **15. října 2010**

10/2010

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1375 registrovaných odběratelů)

Obsah: str.

A. Jak dopadla soutěž SHA-3?

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

Milí čtenáři, rád bych Vás požádal o laskavost. Věřte mi, že tenhle článek jsem neměl v úmyslu napsat a psal jsem ho na vyžádání Pavla Vondrušky. Chodí mu (a mě taky) dotazy typu „jak dopadla soutěž o SHA3 ?“, takže se pokusím odpovědět. Pavel také v kryptologických kruzích zaznamenal, že teď již nejde jen o kvalitu, rychlost a bezpečnost, ale ve hře je i politika a reklama soutěžících. Je to tak, a z toho, jak silně tohle na soutěž působí, jsem dost ohromen. U některých reakcí soutěžících člověk prostě rozšíří zorničky, otevře ústa a chvíli je neschopen reakce, protože nevěří tomu, co vidí a slyší. V honbě za pozitivními body svého kandidáta mnozí dělají podpásové kroky. Šokující je, že to dělají i univerzitní profesoři. Věci došly tak daleko, že někteří účastníci si začali téměř nadávat do hlupáků, zesměšňovali oponenty a jiní na to reagovali oprávněně, ale podrážděně anebo umírňováním a připomínáním vědecké etiky. Některé týmy neváhaly prezentovat například hardwarové srovnávací studie, které i NIST musel označit za zábavné. Například v jedné takové studii se BMW ocitl až na samém konci výkonnosti. Jak je to možné, když v jiných parametrech obsazuje přední místo? Například se to udělá tak, že se řekne, že při realizaci v hradlovém poli není důležitá jen rychlost, ale i velikost hradlového pole, kterou tato funkce zabere. A tak se zavede míra jako rychlost dělená plochou. No a daná funkce se zrealizuje potichu tak, aby měla co nejvyšší rychlost. Tedy tak, že do hradlového pole se "zadrátuje" co nejvíce operací. Tím (potichu, avšak obrovským způsobem) naroste plocha. Co to udělá s podílem rychlost/plocha je nasnadě a BMW je náhle až na konci pelotonu. Každý hardwérář vám potvrdí, že tento postup je natolik dětinský, že ani nevěří, že by někdo takto mohl postupovat. Na náš dotaz, proč je to takto děláno, nás pan profesor odkázal na studenta, který se "zabýval" BMW s tím, že to tak prostě uděláno bylo a na ladění poměru rychlost/plocha by bylo potřeba neúměrně hodně vývojářského času. Neuvěřitelné. Nejhorší je, že takové zákulisní věci nejsou vidět za super barevnými grafy a krásně zpracovanými tabulkami. Ještě horší je, že výsledky takové studie se mohou dostat na konferenci NIST. Tato konference totiž nemá programový výbor! Příspěvky nepodléhají nezávislému posouzení! A jak vidět, podle toho vypadají. Špatné je i to, že výsledky studie ve formě barevných grafů jsou snadno pochopitelné manažerům, a i když o vypovídací hodnotě jejich čísel ví třeba John Kelsey, nemusí o tom vědět jeho kolega nebo nadřízený v NISTu. Situaci mimořádně komplikuje, že i na oprávněnou kritiku jsou protiargumenty velmi dobře konstruovány a vypadají velice důvěryhodně. Je to velice složitá situace! Možná vedla k tomu, proč se NIST s výběrem finalistů zadrhl.

Článek jsem neměl v úmyslu psát, protože vše k finále jsem už napsal v prázdninovém čísle Crypto-Worldu, avšak mnohé z toho, co jsem psal, se vyvíjí jinak. NIST kdysi naznačil, že finalisty soutěže vybere velmi krátce po srpnové konferenci, ale nestalo se a nyní uvádí termín polovina prosince. Upřímně řečeno, nevím, co se děje, ale něco se skutečně u NISTu děje, ale jestli je příčinou to, co je uvedeno výše, je ve hvězdách.

17. září John Kelsey z NISTu poslal do poštovní konference hash-forum@nist.gov (může ji odebírat kdololiv) svůj příspěvek z akce ECRYPT. Z něho vyplývá, že NIST ještě tři týdny po srpnové konferenci SHA3 zvažuje množství faktorů a nemá zcela jasno, jaké funkce vybrat do finále!!!

Výtah z jeho prezentace uvádíme dále s komentářem a celou prezentaci naleznete pomocí vyhledávače na internetu v uvedené poštovní konferenci.

SHA3 Competition Status Update

	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced	*Hamsi*		*JH*		*Keccak*	*Luffa*
AES	*Shavite3*		*Echo*	*Grostl*		*Fugue*
ARX	*Skein*	BLAKE	*BMW*		*Cube*	
Logical/ ARX			*SIMD*	*Shabal*		

John Kelsey, NIST

History and Timeline

- SHA3 competition announced Nov 2007
- 63 submissions received Oct 2008
- 51 accepted for first round Dec 2008
- 1st SHA3 Conference Feb 2009
- 14 semifinalists announced July 2009
- 2nd SHA3 Conference Aug 2010
- 4-6 finalists announced by end of year 2010
- 3rd SHA3 Conference Spring 2012
- Winner announced sometime in 2012

Selection: What Do We Need?

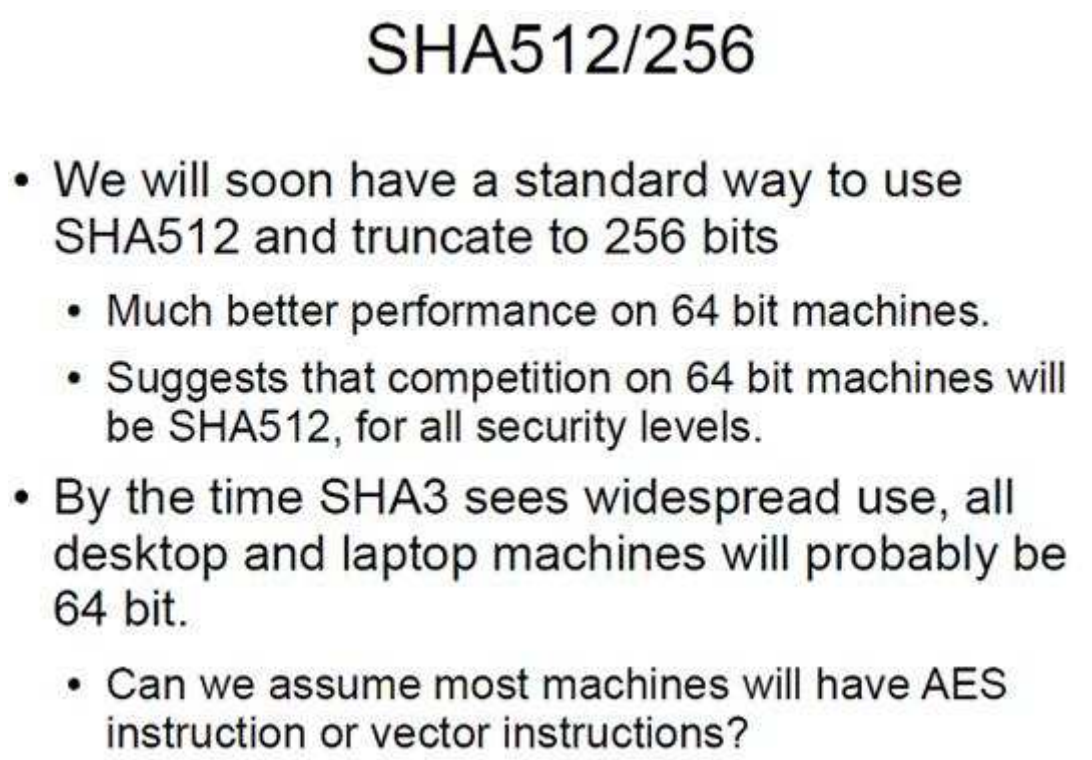
	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced	*Hamsi*		*JH*		*Keccak*	*Luffa*
AES	*Shavite3*		*Echo*	*Grostl*		*Fugue*
ARX	*Skein*	BLAKE	*BMW*		*Cube*	
Logical/ ARX			*SIMD*	*Shabal*		

Velmi důležité je sdělení na následujícím snímku:

How Will SHA3 Be Used?

- SHA2 (-224, -256, -384, -512) is already being deployed
  - This is the only thing we've had to offer anyone since the SHA1 result was announced.
- SHA3 will deploy into a world where it competes with SHA2
  - If SHA3 is much slower/bigger/etc. than SHA2, will anyone ever use it?

Na dalším snímku je neočekávaný nový záměr NISTu, a to standardizovat 256 bitovou haš jako polovinu výstupu SHA-512, přestože je standardizováno SHA-256. To je ohromná zpráva pro tzv. wide-pipe konstrukci (jako má BMW), kdy hašovací funkce stále pracuje s kontextem dvojí šířka (zde 512 bitů), ale nakonec se vydává ven jen polovina. Z bezpečnostního hlediska je to velice silné protiopatření proti všem možným útokům. Připočteme-li k tomu skutečnost, že SHA-512 bude na 64-bitových procesorech rychlejší než SHA-256, je jasné, proč NIST bude standardizovat hašovací funkci, kterou označuje jako SHA512/256. Vůbec jak je vidět, bude se hodně přihlížet k realizacím na 64 bitových strojích.



Z následujícího také vyplývá, že mezi finalisty budou zastoupeny různé typy konstrukcí (ne všechny budou wide-pipe, ne všechny založeny na AES, ….).

Následující snímek říká, že odstranit monokulturu bude těžké, protože ARX funkce jsou například pro desktopové SW realizace zrovna ty nejrychlejší mezi všemi.

Shared Design Elements, Nonlinearity, Lineage

Bitsliced	*Hamsi*	*JH*	*Keccak*	*Luffa*
AES	*Shavite3*	*Echo*	*Grostl*	*Fugue*
ARX	*Skein*	BLAKE	*BMW*	*Cubehash*
Logical/ARX	*SIMD*	*Shabal*		

- JH has much in common with AES-based designs
- Keccak is an outlier in Bitsliced category
- SIMD is much closer to ARX than Shabal
- BLAKE is based on something by Bernstein
- All the AES stuff is based on something by Daemen

Další snímek upřesňuje, jaké skupiny by mohly být považovány za monokulturní:

What Makes a Monoculture?

	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced	*Hamsi*		*JH*		*Keccak*	*Luffa*
AES	*Shavite3*		*Echo*	*Grostl*		*Fugue*
ARX	*Skein*	BLAKE	*BMW*		*Cube*	
Logical/ ARX			*SIMD*	*Shabal*		

- Source of nonlinearity (AES/bitslice/ARX)
- Shared design elements
- What else?
- Similarity of domain extenders (all sponges, all HAIFA, etc.)
- Lineage

A ještě jeden pohled:

Fixed vs Keyed Permutations

Fixed Perm	Hamsi	JH	Keccak	Luffa	Grostl	Fugue	Cubehash
Keyed Perm	Shavite3	Skein	BLAKE	BMW	SIMD	Shabal	ECHO*

How Much Cryptanalysis?

- One interesting problem is that some designs have gotten little cryptanalysis, while others have gotten much cryptanalysis.
  - For example, Cube, Grostl, Blake, Skein, and BMW have all seen a significant number of published analyses.
  - Others, such as Fugue and Shavite3, have seen much less published analysis
- More analysis implies more confidence in our understanding of security.
- ...but may track with designs that are easier to attack, or simpler to understand.

Patterns that Jump Out of This Data:

- ARX algorithms often optimized for S/W, not so great on H/W
  - Skein, BMW, SIMD, Shabal
- AES-based algorithms tend to be slow in S/W
  - Not so great in H/W either
  - But AES instruction *really* speeds up SHAvite3 and Echo
- Bitsliced designs do pretty well in H/W and S/W
  - Keccak, Luffa do well, JH does okay
  - Hamsi doesn't seem to do as well

36

Poslední snímek s otazníky ukazuje opět nerozhodnost.

Questions and Wrapup

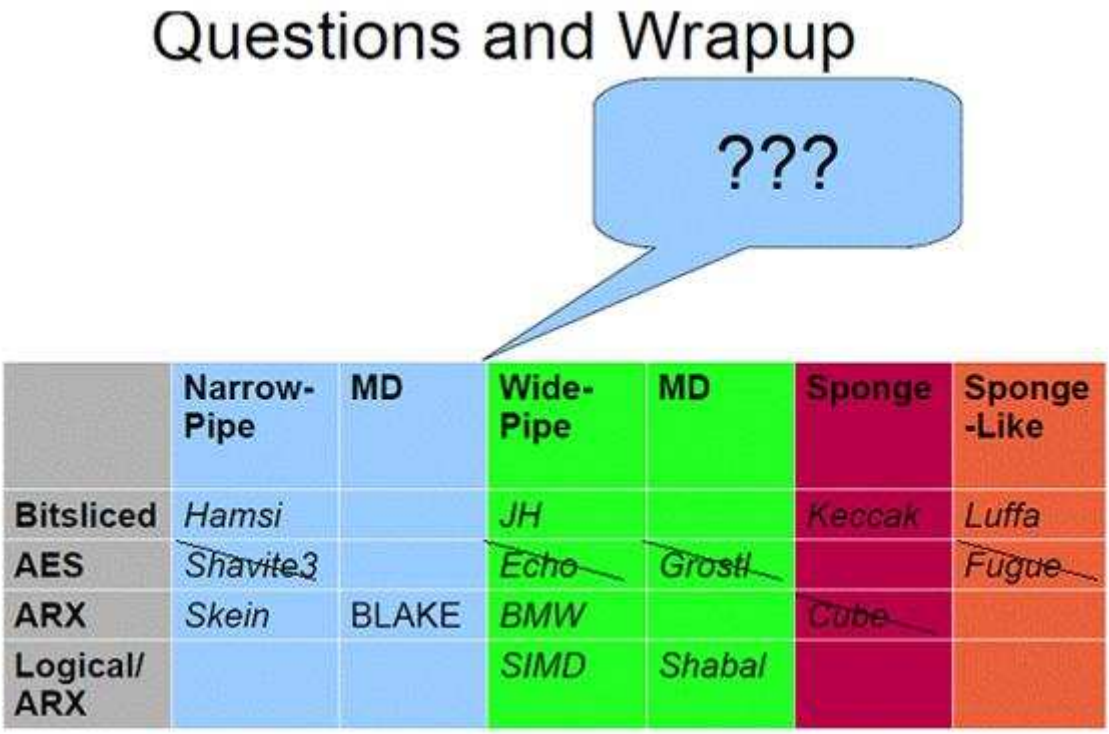
	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced	*Hamsi*		*JH*		*Keccak*	*Luffa*
AES	*Shavite3*		*Echo*	*Grostl*		*Fugue*
ARX	*Skein*	BLAKE	*BMW*		*Cube*	
Logical/ ARX			*SIMD*	*Shabal*		

Jako čirá magie se jeví možnost dešifrování toho, co si NIST (John Kelsey) myslí. Nicméně budeme kouzlit.

- Ukázalo se, že NIST podporuje silně myšlenku wide-pipe funkcí (zejména z hlediska příznivé kryptoanalýzy). Dokazuje to i záměr standardizovat SHA512/256. Čili ve

finále bude zastoupen alespoň jeden, ale pravděpodobně dva z algoritmů JH, Echo, BMW a SIMD.

- Pro odstranění monokulturnosti návrhů bude ve finále zastoupena ještě jedna, ale spíše dvě jiné formy konstrukce.
- NIST nepřipustí funkci, která bude pomalejší než SHA2 (a v SW konkrétně než SHA512 pro 64bitové procesory)
-



Fugue, Grostl, Echo a SHAvite-3 jsou pomalé v SW, proto budou vyloučeny. Rychlý Cubehash má bezpečnostní problémy (diskuse v poštovní konferenci), jako kandidát do druhého kola byl navržen Cubehash bez těchto problémů, ale ten je mimořádně pomalý, proto bude také vyloučen. Zabílením těchto funkcí dostaneme následující obrázek.

Zbývá příliš mnoho algoritmů ve skupině wide-pipe, proto bude vyloučen nejpomalejší, kterým je JH.

Také ve skupině ARX zbývá příliš mnoho algoritmů, takže jeden z trojice Skein, Blake a BMW půjde z kola ven. Bude to nejtěžší rozhodnutí, a tak lze jen hádat. BMW to možná nebude, protože je typu wide-pipe a jeho vyloučením by ve sloupci wide-pipe zůstal jen SIMD, což je málo, proto bude vyloučen buď Skein nebo Blake. Navzdory tomu, že je mi sympatický, vyloučím pomalejší, Skein.
Z typu konstrukce Bitsliced, která není protěžovaná, a všechny algoritmy jsou v ní dost pomalé, vyloučíme nejpomalejší, a tím jsou Keccak a poté Hamsi. Zůstane 5 algoritmů finalistů.

Předpověď finalistů SHA3

Protože NIST v prezentaci naznačil možnost 4-6 algoritmů, zkusíme je podle výše uvedené magie odhadnout.
Pokud by NIST vybíral 6 algoritmů, může ponechat Hamsi a finalisté budou: **BMW, BLAKE, Hamsi, Luffa, Shabal, SIMD**. Pokud bude vybírat 5 algoritmů, finalisty budou: **BMW, BLAKE, Luffa, Shabal, SIMD**. Pokud bude vybírat 4 algoritmy, půjde z kola ven jeden z algoritmů Blake a Shabal, neboť v kategorii ARX a Logical/ARX jsou po dvou, přičemž wide-pipe musí zůstat dva (preferovaná kategorie). Podle mého by šel z kola ven Blake, takže finalisty by byly: **BMW, Luffa, Shabal, SIMD**.

	Narrow-Pipe	MD	Wide-Pipe	MD	Sponge	Sponge-Like
Bitsliced						*Luffa*
AES						
ARX		BLAKE	*BMW*			
Logical/ ARX			*SIMD*	*Shabal*		

Ani z jedné z těchto voleb nemám radost, ale magickým postupem výše, když bychom realizovali to, co NIST chce při výběru zohlednit, bychom my dostali tyto sady. Neobsahují nejlepší 4 nebo 5 nebo 6 algoritmů ze 14, ale vyhovují podmínkám na sadu, jakou chce mít NIST ve finále. Jedno je tedy z prezentace jisté: nebudou vybráni nejrychlejší kandidáti, ale sada, která vyhovuje jako celek více kritériím. Konkrétně, aby nedošlo k monokultuře ve vybrané sadě, musí být vyřazen jeden z pětice nejrychlejších a nejbezpečnějších kandidátů (BMW, BLAKE, Shabal, Skein, SIMD), což žádného z nich nepotěší, ba ani kryptologickou obec.

B. Podzimní *Soutěž v luštění 2010* jde do finiše

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Vážení soutěžící, děkuji za zajímavé a podnětné e-maily, které jste mi během soutěže zaslali. Nejvíce připomínek / komentářů došlo k nepravidelnému zveřejňování úloh. Problém je, že úlohy připravené v zásobě nemám. Na začátku soutěže jsem si pouze připravil jakýsi scénář a ten průběžně „sehrávám“. Musím tedy vždy podle něj připravit soutěžní úlohu a doprovodný příběh, úlohu a příběh zveřejnit na webu soutěže, otestovat funkčnost, v NEWS zveřejnit nápovědu, v aktualitách přidat informaci o dalším kole. Ne vždy se mi podařilo uvolnit tak, jak jsem si původně sám plánoval. Snad po tomto vysvětlení mi odpustíte tu nepravidelnost. Přes všechny problémy s časem se blížíme k závěru. Dnes máte možnost řešit další dvě úlohy (úkol 12 a úkol 13).

Termín zveřejnění závěrečné úlohy
Závěrečné dvě úlohy, které rozhodnou o vítězi letošní soutěže, budou zveřejněny **v sobotu 23. 10. 2010 v 19.00 hod.**

Termín ukončení soutěže
Pro určení celkového pořadí je rozhodující stav **v době oficiálního ukončení soutěže**. Letos bude soutěž ukončena **v neděli 7. 11. 2010 ve 20.00 hod**. Krátce po té budou na webu soutěže uveřejněny loginy tří vylosovaných řešitelů, kteří společně se třemi nejlepšími soutěžícími obdrží ceny. Přehled cen viz http://soutez2010.crypto-world.info/index.php?crypto=ceny

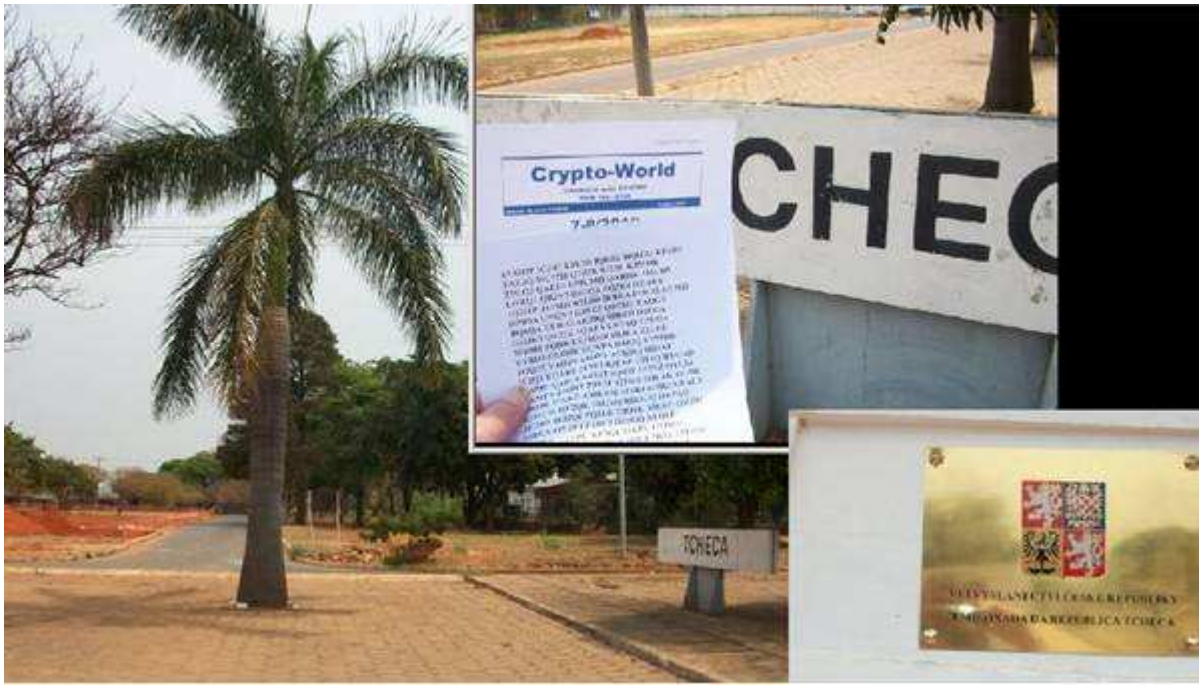
Lze se ještě přihlásit do soutěže?
Ano. Do soutěže se lze přihlásit kdykoliv do 7. 11. 2010. K registraci slouží kód, který byl rozeslán s údaji ke stažení e-zinu 9/2010 a ke stažení tohoto čísla 10/2010.

Kde se všude luští
Využívám této příležitosti a děkuji soutěžícímu s loginem „hodiny“, který zaslal zajímavé fotografie ze své služební cesty. Fotografie slouží jako důkaz, že naše soutěž je „světová“ – tedy alespoň co do lokalit.
Tato jeho iniciativa mne tak zaujala a nadchla, že jsem následně zaslal všem soutěžícím výzvu k zaslání fotografie z lokality, kde úlohy řeší. Na fotografii by měla mimo lokalitu být i nějaká „vazba“ na Crypto-World nebo přímo na soutěž (úloha).
Zaslané fotografie budu průběžně zveřejňovat na webu soutěže (sekce Aktuality, odstavec - **Kde všude se letos luštilo!**)

Přikládám přehled dosud vystavených fotografií. Mimo dvou exotických zemí (Brazílie, Mongolsko) byla sbírka doplněna o originální fotografii luštitele z Hradce Králové, který do fotografie přidal jako malý bonus lehkou šifrovou úlohu.

a) Mongolsko, Ulan Bator

b) Brazílie, Brasilia



c) Česká republika, Hradec Králové (+ BONUS – úloha k luštění)

Výzva k zaslání informací o řešení úloh

Prosím řešitele, tak jako každoročně, o zaslání stručných komentářů k úlohám, které řešili. Komentář se může vztahovat nejen k postupu řešení, ale i k hodnocení úlohy, může obsahovat postřehy, komentáře k chybám apod.

Všem soutěžícím přeji dobrou zábavu a těším se na letošního vítěze!

C. Doprovodné příběhy k jednotlivým úlohám Soutěže v luštění 2010

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Následující doprovodné texty jsou sestaveny pro účel této soutěže. Vycházejí z historických událostí a vystupují v něm (většinou) reálné osoby, ale konkrétní skutečnost byla přizpůsobena našemu soutěžnímu vyprávění. Vstupní text je však až na tvrzení, že se, ve kterém chtěl uvést některé ze svých životních příběhů, které ve svých Pamětech vynechal (Příběh mého života - *Histoire de ma vie).*

C1. Úvodní doprovodný příběh k soutěži a doprovodné texty k úlohám 1-3

Úvodní doprovodný příběh byl společně s životopisem Giacomo Casanovy a Jana Josefa Kittela zveřejněn v e-zinu Crypto-World 9/2010: str.

Dále byly v tomto čísle uveřejněny i doprovodné texty k soutěžním úĺohám 1, 2 a 3.

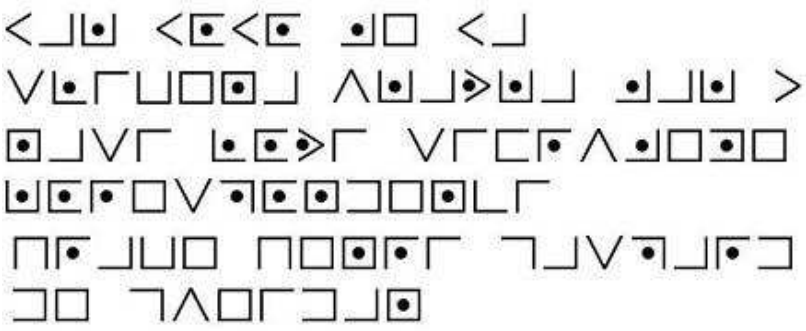
Z tohoto důvodu zde uvádíme již pouze odpovídající soutěžní úlohy 1, 2 a 3, které v e-zinu 9/2010 uvedeny nebyly.

Všechny úlohy a doprovedné texty jsou k dispozici na webu soutěže v příslušných sekcích http://soutez2010.crypto-world.info/index.php

Úloha č.1 - Kittlův dopis

HPESOJ ERACITNEMID IAM ORTOP NON KRUBMUS ELATAN ESEAP OIM LEN IUQ ENOSREP EL ETTUT ID AIROMEM AL E AIROMEM AIM ALLEN ERPMES REP ARRAMIR ERBMETTES A OSOIROLG ONROIG LEUQ OTSERRAD ATUTTAB ANU REP INOIZADNAMOCCAR ID ESAB ALLUS EM REP ITTEFFE NI OIGGAIV OUS LEN EROTAREPMIL EROTAREPMIL NOC OSSECCUS OIM ID ERALRAP E EM ID IDROCIR IT EHC OTLOM OIZARGNIR AL OCIMA ORAC

Úloha č.2 - Zednářská lóže 1



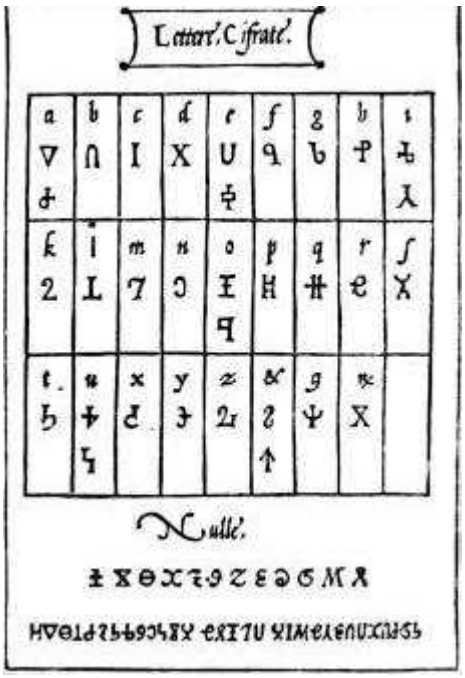
Úloha č.3 - Zednářská lóže 2

Šifrový text

```
NQRBM ZZISB EVAOJ YETKR EWDUP LMAZW
UFIPC VMVOB AEQQC RQAVC NPMTQ EVMFS
SQXUR ADQRC NMROH ONMIB YBWYH UBZKG
EZQBW GQVKF OHIYW FDWBS HAAEG TQUAG
PQZOC DUKQM MTMYZ EYIZC NMHGY LMLKO
NMTEN YHHJO LQVUG TUUKN IAXGY OHITW
MUDYW FDWBS MFMDH UFMTH OAJPS VZMHM
LLIZW MZQQR EBCHZ IWWBO NBZKR SFIBW
TQTKB AEQRC ZQXGH RUUKN IFGQH EDQHM
LUABM SXMJY EYAKN NMUKB IBZUH OFCZC
SUNXI NQXUI ZUDGA EYQRM GUIIC MABKR
TQVZC TQFZN AEQLF UVQYD EDQUR IOSEA
HQARS MMUOU OMXXS DHMJI TURGY JQRRN
EXMNQ EHGRI SFQZX
```

C2. Úkoly ze šuplíku – Adelaide de Gueidan

Když si Giacomo prohlédl dokumenty z doby, kdy jej hrabě Henri Gaspard de Gueidan zasvětil do tajů šifrování v lyonské Lóži Svobodných zednářů, pečlivě je vrátil zpět do šuplíku. Jeho myšlenky jej přenesly ke sličné sestřenici hraběte - jeho milované Adelaide de Gueidan. Seznámil se s ní počátkem roku 1749. Na rozdíl od jiných jeho mnoha prchavých známostí, byla tato sličná dívka jeho opravdovou láskou. Nade vše ji miloval. Celý svůj život se ve svých vzpomínkách k ní stále vracel. Společenské postavení mu však nedovolovalo se veřejně k této vznešené dámě z Aix-en-Provence hlásit. Z tohoto důvodu ji také ve svých oficiálních vzpomínkách *Příběh mého života* (Histoire de ma vie) nazývá raději pseudonymem jako Henriette. Svoji lásku museli před veřejností úzkostlivě tajit. Věděli o ní jen jejich nejbližší přátelé a z příbuzných Adelaidy o ní věděl jen její bratranec Henri.



Z tohoto důvodu si oba milenci spolu vyměňovali dopisy psané šiframi. Giacomo pro tyto účely nechtěl použít šifry Svobodných zednářů a vyzradit tak tajemství, do kterého byl zasvěcen. Giacomo proto raději Adelaidu seznámil s tím, co se dozvěděl od svého benátského chráněnce Matteo Bragadiniho. Seznámil ji tak s tvorbou převodových tabulek jednoduché záměny, které byly pro větší bezpečnost rozšířeny o homofony nejčetnějších znaků otevřeného textu. I když jednu takovou tabulku pro Adelaidu vytvořil, přesto ji nepoužila a napsala mu dopis zašifrovaný pomocí jiné homofonní tabulky, kterou si pro tuto korespondenci sama připravila.

Giacomo si dopis, který mu tehdy zaslala, schoval na památku. Vyndal jej z šuplíku a při pohledu na něj se široce usmál. Adelaide sice sestavila převodovou tabulku jednoduché záměny s homofony, ale dopustila se při jejím vytváření (v části homofonů) chyby, díky které Giacomo vyluštil dopis, který mu poslala, aniž by její převodovou tabulku potřeboval a to dokonce ještě rychleji než kdyby to byla obyčejná jednoduchá záměna.

Když se s ní setkal, tak mu Adelaide začala vysvětlovat, že zaslala dopis zašifrovaný novou tabulkou a to její vlastní převodovou tabulkou. Nechtěla ji samozřejmě k dopisu přiložit a čekala na vhodnou příležitost, aby mu ji mohla předat. Tuto tabulku chce i nadále používat. Jaké však bylo její překvapení, když ji Giacomo ujistil, že tabulku nepotřebuje. Již si ji sestavil sám a to na základě dopisu, který mu zaslala a který vyluštil!
Giacomo dopis od Adelaidy, na který si tehdy po vyluštění poznamenal její převodovou tabulku, pečlivě schoval a vrátil jej zpět do šuplíku. Chvilku se pak v něm dále prohraboval, až našel, co hledal, jinou podobnou převodovou homofonní tabulku, která byla na rozdíl od těch, které s Adelaidou používali, ještě vylepšena o tzv. klamače, tedy znaky, které nemají žádný význam, ale vkládají se do šifrového textu, aby zmátly luštitele. Tuto konkrétní převodovou tabulku mu prozradil jeho benátský chráněnec, který ji náhodou našel v benátském archívu. Prozradil mu také, že ji používal v 15.století Giovani Battista Palatino.

Úloha č.4 - Adelaide de Gueidan

```
EUGOP ICJB2 E1E2D IQBJK HQHR3 KP4R4 ZAE3Q MCIZH Q2RIB RJEIE KJMHR Z1GQ3
QAEF4 UMCMH QARHK JMCD5 LHRQ1 QR2V3 DIGQA EQ3K4 ODARV 1QHTP JVIMH R2L5D
B6BRA P45GQ HE3O2 DPIOA GHQVJ G3VDI QRFHC FAOG2 BQ1QA EF4UQ ARBIQ RIBRH
O2EGA GHJK3 QV3EZ 1QAFA L5OAQ EJMO4 MBIRI ZQHKJ EJMHR 1RJEA R2LUB YVBD3
OUO4K HQKPA DJZ3Q UPMHR 1GQ3Z VAO2V 6M4VF AEKHQ HIDAF IF2Q1 EQARB 2F3R3
RJFAP 1BF5Q RYOAD IL6MC QARIB R4RJZ 5QRIF 1F2VZ OYL1Z KAMFA ZIQHT PJV2F
12FHB O4FAK 4VJDI F6Q3R JFAKP AMRAM 4Z1R4 RIBRI GFACJ R3MCM HF2QK IRGAQ
RDHGQ HKPAD JZ3DO 4KHQI ZQ1ER 2BQ1K RIERU Q3QRJ RIBRA OY2FJ P4ZCJ ODIGQ
AEQ1Z ARVUG F2VPC KP3GE 5IKPV FHPHH GF4VJ 5FAOA D3KP3 G1OUZ 2RALJ 5FID4
V1MBY ZIEAM 1BRVA CJKPH RADAZ UQR2F 5RIEQ R1LJU KP1QF JMIDA QDHLE HZAF3
BEUIF HBOY4 R4EF1 L5O1Q F3MVY KP2VA REHD2 MBUEJ MQ1R1 Q3EDI QB4E4 G1RV2
CJD5L HMBIX
```

C3. Úkoly ze šuplíku – Francesca Buschiniová

V šuplíku měl i řadu milostných dopisů, které mu zasílala Francesca Buschiniová. Patřila také mezi jeho velké lásky. Udržoval s ní rozsáhlou korespondenci od svého druhého vyhoštění z Benátek. Dopisy, které mu psala, byly plné dojemné upřímnosti a něhy.
Zpočátku se ji snažil naučit nějaký jednoduchý šifrový systém, ale Francesca byla sice krásná, hodná a milá dívka, ale šifrování a dešifrování jí moc nešlo. Brzy to tedy vzdal a nadále si psali své dopisy plné vášně nezašifrovaně.
Přesto si schoval jeden krátký dopis, který Francesca neuměle zašifrovala pomocí dvou velmi lehkých šifer, které jí ukázal.
Giacomo si pomyslel: „I přes jednoduché šifry to bylo docela těžké rozluštit, tak proč jej také nezařadit do připravované knihy *Tajnosti mého života.* Dopis pečlivě složil a vrátil zpět do šuplíku mezi dokumenty určené k použití v knize.

Úloha č.5 Úkoly ze šuplíku – Francesca Buschiniová

DFVHFQDUI DYW DELO RQWXPV LP HM HV LYCR PLVRUS VHQDWVRG HY-LUGMHQ RF XVLSRG N HV HC PDIXRG D ODG LP LVM XRUHWN XVHUGD DQ LVLS HEHW R HV PLMRE VDYBCRHQ HV RKXROG HW LMXEHUWRS RQWXPV LP HM HQDOG LFLMDNVDO D DWVX DYW LP LEBKF LVMHOLPMHQ MXP

C4. Rekapitulace 1

Jindy tichý Duchcov byl plný života a shonu. Na zámek opět po delší době přijel hrabě Valdštejn. Na jednu stranu byl Giacomo Casanova rád. Hrabě byl jeho ochránce a sluhové, se kterými Giacomo v poslední době hrubě nevycházel, mu předním prokazovali náležitou poctu a vyhnuli se možným konfliktům, které byly v poslední době mezi ním a některými z nich na denním pořádku.

Na druhou stranu Valdštejnova společnost Giacomovi příliš nevyhovovala. Stalo se zvykem, že spolu trávili společně večery a Giacomo tak neměl čas na psaní svých *Příběhů mého života*. Nemohl se ani procházet a třídit materiál pro svůj další projekt *Tajnosti mého života*. Jeho díla nevznikala nijak snadno. Společnosti v Teplicích, kam rád docházel, se zmínil: „Když nespím, tak sním. Když mne sny unaví, popisuji list za listem, ale po přečtení většinu vyhodím.“. Nemluvil však pravdu, část schovával do svého šuplíku.

Jenže návštěva hraběte jej v přípravě dalšího díla zdržovala. Giacomo tak velmi přivítal, když ve středu večer hrabě musel narychlo odjet na důležité setkání do Teplic.

Giacomo se rozhodl udělat si stručný přehled podkladů, které si vybral pro svoji připravovanou knihu *Tajnosti mého života*. Přemýšlel, jak je třídit, zda podle let, ale pak si řekl, že životopisné pořadí obsahuje jeho kniha *Příběhy mého života*; zde bude materiály třídit jiným způsobem. Označil si je a setřídil podle šifrových systémů. Získal tak prvních pět příspěvků:

1) Naivní šifra - sem zařadil Kittelův dopis psaný jeho slabou italštinou a zašifrovaný tím nejjednodušším způsobem.

2) Jednoduchá záměna – grafická abeceda, základní šifra, kterou používali v Lóži Svobodných zednářů v Lyonu a se kterou jej seznámil hrabě Henri Gaspard de Gueidan.

3) Periodická šifra – zašifrovaný text, který použil hrabě Henri Gaspard de Gueidan když jej zasvětil do tajemství Lóže a předvedl mu, jak lze takovou šifru poměrně snadno vyluštit. V tomto případě tomu pomohlo také to, že se jednalo o krátké periodické heslo délky 5.

4) Homofonní šifra – zástupce této šifry byl dopis od Adelaidy, na který si tehdy po vyluštění poznamenal její převodovou tabulku. Adelaida svoji převodovou tabulku nesestavila příliš šikovně. Nejprve si připravila tabulku jednoduché záměny a pak pro šest samohlásek přidala homofon. Tyto přidané homofony byly číslice 1-6. Ve svém důsledku toto neobratné rozšíření převodové tabulky mělo za následek, že Giacomo její dopis snadno vyluštil.

5) Se zařazením dopisu od **Francesci Buschiniové** měl problém. Francesca použila najednou hned dva jednoduché systémy, které od Giacoma znala. Jednak naivní systém a jednak jednu z nejznámějších a nejjednodušších verzí jednoduché záměny. Po dlouhém váhání dopis přidal do hromádky naivních šifer.

V tom otevřel dveře lokaj Jan Bauer a s úsměvem houkl na Giacoma: „Nechaj ty krámy a maj ihned jít za panem hrabětem. Právě se nám vrátil z Teplic a chce s Vámi mluvit. Jo a při té učené rozpravě se neožerte ať Vás zase nemusím tahat do schodů do vaší cimry.“

A bylo po pohodě a Giacomo s lítostí zase vše uložil zpět do šuplíku s tajnostmi, které si připravil pro svoji další knížku.

C5. Cesta do Ruska

Giacomo svoji starou korespondenci celá léta úzkostlivě schovával a vozil s sebou z místa na místo. Nyní si vzpomněl na jeden z dopisů, který by v ní měl být uložen a který chtěl zařadit do svého připravovaného spisu *Tajnosti mého života*. Po důkladném hledání dopis v truhle našel.
Obdržel jej na podzim roku 1764. V té době plnil pro Benátskou republiku drobné úkoly špionážního charakteru. Většinou měl za úkol kontaktovat někoho vlivného a díky svému šarmu se mu vnutit do přízně a pak se pokusit jeho rozhodování ovlivnit ve prospěch Benátské republiky nebo zájmů jejích obchodních spojenců.
Na dopis, který konečně našel, si velmi dobře pamatoval. Byl psán jednoduchou klasickou šifrou, kterou se zde před svým odchodem naučil. Jednalo se o úplnou transpozici, kde transpoziční heslo bylo předem domluveno a měnilo se podle dohodnutého scénáře.
Když tehdy dopis dešifroval, byl rozechvěn. Čekala jej dlouhá cesta a setkání s korunovanou hlavou velké země. Pamatuje si, jak se nedočkavě se na tuto dlouhou a romantickou cestu vstříc novým dobrodružstvím vydal.

Úloha č.6 - Cesta do Ruska

```
DAAEK ENKZZ YRAPC MIPJP YVCCH NZRSV UTAAE VMSKD NUVPJ ALDEO TEOTE OTRTD
UPTDE RIVYD NXDRT NETEV EINTR UDSNO RAHEL PIUPE AIRIA DCNDI MAAKA VOAVR VE-
IEK ODEEI IOYOE OUEVI OSUJO LEHDY NEBVA EEVNV ARACN JJRLD LSRCE ZTOEE EARZA
EVUAP LPAKL ONUDT AOZIV TESKA YKIHA RJNAT VTSRV MEYNL SHOKE SDHZS SSSUS
NNSLA CDEEV ORKTE RTUKA NEEAT HNIJY MALDS NTASN ENOZN SFMRE STOKO KAEIC VE-
UBD ANEAM TEDMA KLRIP ZTAAT DEOIN EARPI RHRST EAKEK RITCE TUSIY RBIVP AETTS
KSCIR CIOOE OUBET OEMEH CERTE CEVLL OBAUA VPATR HPTET RSOAE OEAEL OSDBU VE
```

C6. Madam de Urfé

Sbírka jeho šifrované korespondence, kterou chtěl v díle Tajnosti mého života (Secrets de ma vie) použít, by nebyla úplná, kdyby nezařadil dopis, který mu kdysi ukázala markýza Jeanne de Urfé.

Rád vzpomínal na tuto velmi bohatou a extravagantní šlechtičnu, s níž udržoval dlouhý vztah. V té době mu to umožnilo rozhazovat značné sumy peněz, které mu ochotně poskytovala. Okouzlil ji nejen svojí galantností, ale i rozsáhlými znalostmi magických rituálů, na které byla tak zvědavá. Nutno říci, že si řadu z nich zcela vymyslel.

Šlechtična mu však bezmezně věřila. O jeho schopnostech a znalostech magie a esoterických věd vůbec nepochybovala. O jeho schopnostech ji utvrzovalo to, že byl člen Zednářské lóže a pak jedna příhoda, ke které se právě vztahoval dopis, který Giacomo nalezl a chystal se jej uložit do šuplíku k ostatním materiálům.

Jednalo se o opis dopisu, který mu ukázala markýza de Urfé. Dopis obsahoval intimní korespondenci s její velmi mladou přítelkyní, milenkou jejího kadeřníka. Tuto mladou dámu se markýza rozhodla podporovat. Byla nejen nevšedně krásná, ale i velmi dobrosrdečná. Po několika letech se tato mladá dívka, po velmi složité životní cestě, stala milenkou samotného krále a stala se tak známou nejen ve Francii, ale i v celé Evropě.

Markýza si myslela, že tajemství v dopise je bezpečně chráněno jedním z typů periodické šifry, kterou pro tyto účely použily. Jaké však bylo její překvapení, když Giacomo dopis, který mu zapůjčila, dokázal přečíst! To mohl bez znalosti hesla provést opravdu jen muž nadaný přímo až nadpřirozenou mocí a schopnostmi. Od této chvíle po celá dlouhá léta byl pro ni Giacomo ve věcech tajemna autoritou …

Giacomo vyluštil tuto šifru díky postupu, který mu v opilosti prozradil hrabě Henri Gaspard de Gueidan. Postup luštění periodických šifer byl jedním z velkých tajemství Lóže Svobodných zednářů v Lyonu a trvalo ještě více než 100 let, než byl jiným členem Lóže pruským důstojníkem Kasiskim vyzrazen a veřejnost zjistila, že tento údajně neprolomitelný systém je ve skutečnosti lehce luštitelný.

Giacomo si s chutí dopis po létech opět přečetl. Něčím mu byla ta mladá naivní dívka, která dopis markýze psala a svěřovala se tam o tajemstvích svého mladého života, blízká.

A to ještě netušil, že za několik dní mu jeho přátelé zašlou velmi smutnou zprávu. Dívka, kterou znal právě jen z uvedeného dopisu, se z bezpečí Anglie, kde v tu dobu pobývala, celkem z nepochopitelných důvodů vrátila zpět do revoluční Francie. Zde byla uvězněna a odsouzena k trestu smrti gilotinou. Poprava byla veřejně vykonána 8. 12. 1793 v půl páté odpoledne.

Úloha č.7 - Madam de Urfé

```
BMSQQ GSOYX EWJCA SCJKR GNNUM KSAPH CZLOC OEWWJ OCMHA KKSLO MJBFB IDOKA
CGIOI VWPBO DVESL OMENB XCNDQ GUVEV DSAJQ NXDBF FOVDA WSIYB LGLAG AKTLK
GHOLP NVEMD EIIQN XPCAK XQHZN BJCUA KCOZM KUWQU TWKKN NUMKM CQUHK LTJCP
ACFIX VAKSO ZVOTA JNBCR GCUEG RUOTI NAAOL BJZEU SFRTC UJMUD VOXDT RJBYC
QKAOY MJCAB FOUEG EGLKZ CMRBY XZFVV OCJVF XDUDD TJXKC SJOXB CFZCV VXGEJ
LKGDX DLFVO OSTII UPKQO SPPQX LTNZC BPTUA GVDKM MMKKQ OWAPG GNRJQ QWZZW
KPZRU NBSJG SKUQX KWNGZ GIDZU WWGOG JOPQK VZMDU FOOZP OMQVP ETXOE TBABC
ECDCN VIOZS AYJYB DNPDS ZAZIQ AROLT PCRUI ACPFO ZMWFC DXRLM GUROB OVAPM
RVGMD OESOV VOXHN RTSPG TUUXO VJGMK UZULT NVOHD IJBHJ GLENT OCNVH XUKFZ
LAGGP QWAID IIPCN XPKFK WGUIN ZXAGO XZWAY GHQRF BKFKF NNVQN ABOCO PGYJH
NRUVZ PCOAE TEIXI TORAE KGOFF NRUQK SOFLS DNLWI HYCVD JBQKR KSRWP GRWJL
EWYNP BUDLP ZNXKP NDXXF IWPNF DSFRD MRAAH DXDOZ OFVWI USKIZ WAXLR CACUP
GBACO AKANN NHCTP FJBAE NGMJK ROABF ESBRO PNAJD ZHZOD AOZZB HYHPA KBOWY
ZFTSQ CDGAM OVDAW GUZGS ALHZK GNAMG JXZNZ TSDRY MZQKV QKGAG OEOWQ UCZMO
SKPGH PHNII VPBJT HOZUN TIIVD VFBIA WFZDJ OXPPG APBXU MCQTK KXJNS CEJFC
RYDDT NVSVR DRJQQ WZLZW ZOGNX NKROL VJXSW WNHXU IXFBN ZBKOB WJBUZ DXFPO
POJRJ QQWKX NTKDR LWQWA HAKSK ZDNUN XZDZP CFBSC ENBTZ OVELJ XSLRS AYMRO
RGYXK WENQB VYBQK VBSWN CASCY COXZW ZKQFP XCCVF WLKBB TBLQU KVVEJ CSTRK
SQUQG IKLBS PJBAG KROLV JXFGP GPNVP GBGLH ELFNH RWSVZ XNWOH NOQDC JXPFF
DSOCN JBRUD DFVKG NTCAC ZEESO AOXKZ JPXFL ALVWK PGRVA IWCBD VZVEW CNJIU
PWTKY XEWYW WYMHE SOVVO XNEIX IKGQK BALDR YJNCJ KOXFT UEEZG IFLGL DNFAK
FUAPU RKTKO BSDDV HXISV ZXJFA AXFLK GBKEB JPOBT NHNBL KCOFW HKPGH TSPQD
VZBSE ANPNZ KEZCK TEXNY JTIOB ZTFLS BNBSQ ATGBK UNYEA JIQMQ ODPYG XOFNX
NCJOS AVKGG WUMPB OWRKW UXQQZ JOQHP AKCOF GINQG MJKKO DCSCR UQBHY CDTVA
YMRVN NCJGO XNMKO YNQSC QKLKB UAKGN LNCHK RBNTB OYTBR JCWKK WOTOP FHCMH
GKFNE EZDTP TSPGO XZLST RLQBI EWSGB WOPNS WJZEM WZNVF OPUSQ QJKBH EWOCW
JPPMS XDWAO JWNBF DCOED CNCPA HZNBJ OUOAV VSTXA MJMQW IKYDS TNSPB CEWBK
VOFKS SCJGS KWALK HOFNO RDCWQ KZMKW OCMHN ECVXN WSCJN MGURB FAMDK MNEIP
URQRG YGLOF FNBBH OMGSK BGFOW JQPQQ GSWOP FJNTL CEIGU KTOFF PNZCD LKKAG
BNSAJ KCLZX AGIJJ HGKGR ORKUC KCDGM YMPDD WDQGB NUARQ HQJMF DZAFT HNKLO
LBJCY ERKWK HUMTK BUBKF JIQAH QRQVD ODREI XIPKT ACGIB DSCZN IMZWT EZKAJ
RJQQC VCZTS WRSAJ MAHOX FVODH PNGWD EPUVK HOJVA PUPOL AMKYL WZJBF LQRKC
```

```
QXKGD CHCNK BHAKJ TJLWJ HCLKK AEZKA PRJQQ UAKCO HOENL NCRKA QFTSC RUMHS
YWIBJ CTNTC CGJCW FUYXS TNACI USOCQ OLBLD CGOQZ NDDJW DDTSA QWCZJ WZNKD
TEARG SLFNP NUDTO FXRPU KQAKY CTVPO QCTZW YKQHX OSSMK DDCJV TKFES CFYVR
KVGQU YZIXZ KOTBJ DKNJE WUGQO KMJTU MJGAQ UKGRB JBSUG FYTNR OLGUK GBNVL
TJCDD OAOTT RCAPH YMPUW AYLNS QNACZ PNJHH GPFFX JQGIO BLOEX ESCQT WKKVK
GBNOA JBCDD FVVOB NEWOK LOLBN OHKJV PXSVK KBNTS WNAAG VZQPL NBSFN NNOQ
```

C7. ICOSAMERON - písmo Megamikrů

Giacomo se rozhodl mezi materiály do své knížky tajností zařadit i možný způsob šifrování, který sám vymyslel. Šifra vychází z popisu jazyka Megamikrů z knihy Icosameron, kterou zrovna nedávno dopsal a s nepříliš velkým úspěchem na své náklady vydal.

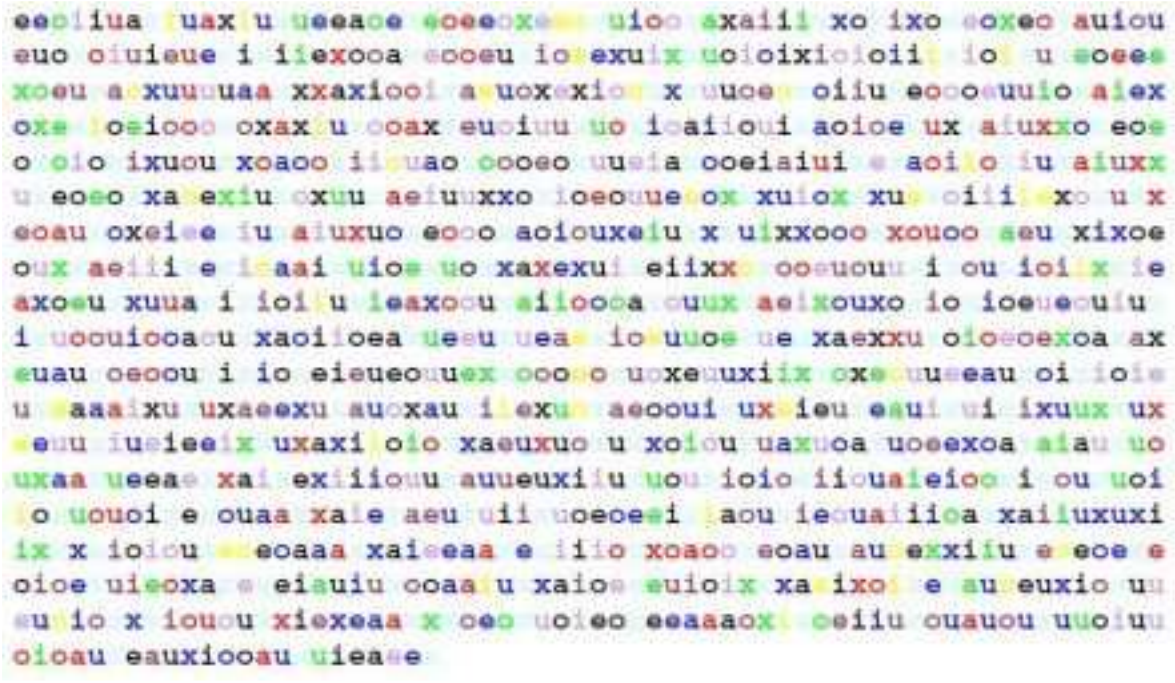
V knize popisuje jazyk Megamikrů včetně ukázek na více místech.
Jeho nápady lze shrnout asi takto:
- Megamikrové umějí vyslovit jen 6 samohlásek a žádné souhlásky,
- pět samohlásek je shodných s našimi a jsou to a,e,i,o,u a šestá pak není podobná žádné z našich,
- každou ze samohlásek vyslovují Megamikrové v jiné výšce,
- výšek, které při tom používají, je celkem 7.

Z popisu je vidět, že mají k dispozici celkem 42 různých zvuků. Aby mohli Megamikrové text zapsat, používají k tomu šest znaků pro samohlásky a sedm různých druhů barevného inkoustu.
Jazyk je však mnohem složitější než popsané písmo. Jeho součástí jsou i gesta, tanec, úsměv apod. Výška vybraného tónu závisí na tom, s kým mluvíme, kdo rozhovor začal, na společenském postavení apod.

Casanova se oprostil od jazyku Megamikrů a využil k šifrování pouze zápis jejich písma. Písmo má 42 různých znaků a to mu bohatě postačilo na zápis 26 písmen mezinárodní abecedy. Proto si také mohl dovolit k některým znakům abecedy přiřadit další znak z abecedy Megamikrů. Tím vznikl zajímavý homofonní šifrový systém.

Nápad se Giacomovi natolik líbil, že do knihy Icosameron vložil hned několik textů zašifrovaných pomocí této své homofonní šifry. Bavila jej myšlenka, že při čtení nikoho nenapadne, že nejde o vymyšlený text v jazyce Megamikrů, ale o zašifrovanou zprávu, ve které popisuje hulvátské chování sluhů na Duchcově. Nemýlil se, nikoho dosud nenapadlo, že Isocameron mimo fantastického příběhu obsahuje i jeho žalobu na duchcovské sluhy adresovanou čtenářům v daleké budoucnosti.

Úloha č.8 - ISOCAMERON - písmo Megamikrů



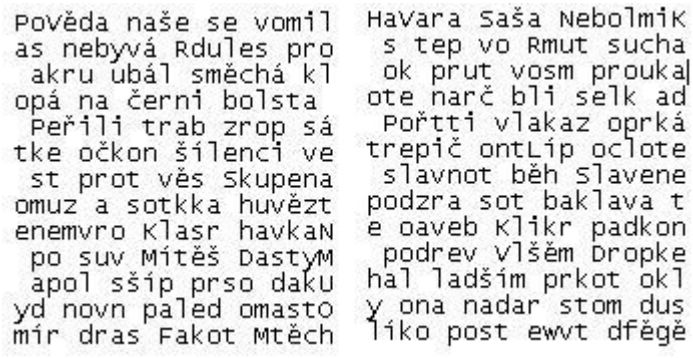
C8. Tři šifry z let 1765 - 1767

Když Giacomo třídil svoji starou korespondenci, našel tři zašifrované zprávy, které spolu částečně souvisely. Navíc se vztahovaly k události, která zásadně ovlivnila jeho život a která jej málem stála život. Na druhou stranu se díky této události seznámil se svým přítelem léčitelem Kittlem.

Nová mise – zpráva 1

V Rusku se mu mise dařila. I když se dostal do Petrohradu teprve koncem roku 1764, přesto se mu díky kontaktům, šarmu a své pověsti, která jej předcházela, podařilo dostat již v prosinci na velký dvorní ples. Na plese byl představen dokonce samotné carevně Kateřině Veliké. S carevnou se pak ještě několikráte setkal.
V Rusku se mu líbilo. Byla to obrovská země, kde šlechta trávila svůj čas způsobem, který se Giacomovi zamlouval. Lovy, plesy, popíjení, milostné aféry. Navíc řada šlechticů uměla dobře francouzsky, a proto neměl problém s domluvou. Na výuku francouzštiny jedné šlechtičny i po letech rád zavzpomínal…
Z toho příjemného lenošení jej však vytrhl úkol, který mu byl z Benátek zaslán. Jeho mise po ročním působení v Rusku byla u konce a on se měl odebrat na další cestu, kde jej čekal úkol, o němž ještě netušil, že jej bude málem stát život.
Dopis byl zašifrován tehdy relativně oblíbenou šifrou - pomocí Cardanovy mřížky. Mřížka se jednoduše položila na list papíru a do vystříhaných polí se doplnila zpráva. Po zvednutí mřížky se písmena zprávy obklopila libovolnými písmeny, nejlépe však tak, aby slova tvořila čitelnou zprávu. Giacomo věděl z dob přípravy na profesi špióna, že systém je velmi bezpečný, pokud mřížka obsahuje málo otvorů vzhledem k celkovému výslednému textu. Na

druhou stranu věděl, že bývají problémy s dešifrováním. Různé písmo, rozházené řádky a další nedbalosti v psaní měly za následek, že po přiložení mřížky bylo obtížné zjistit, která písmena přesně patří do vystřižených otvorů a tvoří šifrovou zprávu. Proto bylo doporučeno, aby …. A právě toto opatření vedlo k tomu, že zpráva byla nejen dobře dešifrovatelná, ale nedělala ani problém luštitelům, kteří díky tomuto „zlepšení“ jinak poměrně bezpečný systém dokázali vyluštit během pár vteřin.



Mise v Polsku - zpráva 2

Koncem roku 1765 se přesunul do Polska. I zde se stýkal s předními polskými šlechtici a jeho život plynul v různých radovánkách. Plnil zde drobné úkoly. V roce 1766 jej však zastihla zpráva zašifrovaná Fleissnerovou mřížkou, která obsahovala příkaz k velmi nebezpečné akci. Měl vyhledat záminku k souboji s hrabětem Branickim, který byl významným šlechticem z okruhu krále Stanislava II. Poniatowského. Byl také schopný generál, a právě proto měl být odstraněn.
Giacomo se pohyboval ve společnosti, jejichž oslav a setkání se tento významný šlechtic také zúčastňoval. Čekal proto jen na vhodnou záminku. Ta se mu naskytla, když hrabě napadl čest jedné benátské baleríny Anny Binettiové tím, že ji označil slovy ta benátská matrace.
Casanova toho ihned využil a vyzval hraběte na souboj s pistolemi. Podnik to byl velmi riskantní, protože jak v případě porážky, tak i vítězství, se dalo čekat, že se mu přátelé hraběte okamžitě pomstí.
Giacomo hraběte Branického v souboji velmi těžce zranil. Hrabě byl čestný muž a požádal své přátele, aby nechali soupeře odejít, neboť soupeř jednal podle pravidel souboje.
Giacomo úkol splnil. Hrabě byl na dlouhou dobu upoután na lůžko a z armády pro svůj zdravotní stav musel odejít. Schopný a poctivý generál tak uvolnil místo nerozhodnému Janu Waleskému.

Při souboji však byl vážně zraněn na paži i Casanovova. Přesto se rozhodl z Polska raději co nejdříve odejít. Přešel hranice do Čech. Ruka mu natékala a bylo nutné vyhledat ošetření.

Úloha č.10- Mise v Polsku

Šifrový text

```
MEEVJ YBTCV OREEA MFLRE KAAJT VNANS EITCS IKOIS XVUMB ENOLJ EKKES MZAXA
ABOID MHEWR JTENA ERJAE B
```

Jan Josef Kittel - zpráva 3

Casanovova měl i tentokráte štěstí. Když překročil hranice Polska, dostal se do blízkosti Šumburku. Zde se dozvěděl o českém léčiteli Janu Josefu Kittlovi. Vyhledal jej a ten jej začal léčit.
Ne nadarmo se o tomto českém lékaři říkalo, že je černokněžník. Paže se Giacomovi začala po důkladném ošetření rychle hojit.
Večery trávili tito dva vzdělaní muži společně. Byli si tak vzdáleni a tak blízcí. Spojoval je jejich zájem o tajemství života.
Josef Kittel ukázal Giacomovi i svoji největší vzácnost tzv. „smržovský griomár“. Po té co v této knize listovali, a snažili se najít skutečný význam zde uvedených čarodějnických formulí, se dostali k tématu šifrování. Giacomo totiž tvrdil, že skutečný význam textů v knize je jistojistě nějak zašifrován. Téma šifrování měl Giacomo velmi rád, a tak několik dalších večerů spolu na toto téma diskutovali. Několik jednoduchých systémů Giacomo Kittlovi ukázal. Ten zase na oplátku vzal papír a napsal na něj šifrový text, který teď po letech držel Giacomo v ruce a chystal se jej uložit k materiálům ke své chystané knize.
Tuto šifru prý pradědovi Jana Kittla prozradil jeden švédský voják, kterého jeho praděd vojenský lapiduch léčil. Šifra to byla jednoduchá. Na první pohled však řešení vidět nebylo. Giacomo tehdy v ten večer Kittlovi vysvětlil, že to není klasická šifra, protože vlastně nemá žádný klíč. Je to šifrový systém, kde vyzrazení principu šifry vede přímo ke kompromitaci. Pamatuje si, jak přirovnal tuto šifru k Césarově šifře.

Úloha č.11 Jan Josef Kittel

Šifrový text

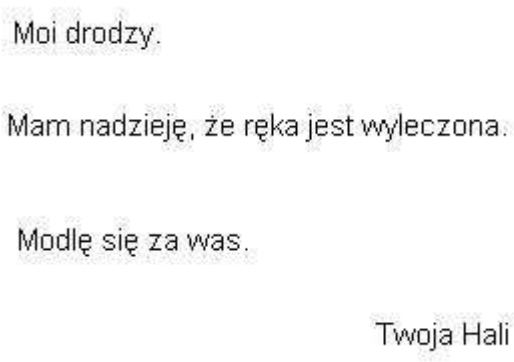
```
PBPHG FYHVX FLEEO SEJLB PVIJM GUPBQ EROAH NFLER DPPVB XDDVP INRPX SSWGK SD
```

Giacomo dovzpomínal, všechny tři zašifrované zprávy pečlivě složil a zařadil mezi již připravené šifry. Líbilo se mu, že se jedná o systémy, které ještě v připravované knize neměl dosud zařazeny, a proto je vhodně doplňují. Zavřel šuplík, dopil sklenku vína, vstal ze svého oblíbeného křesla a šel spát. Ve snu znovu prožil souboj, který jej stál málem život…

C9. Stín hraběte Branického

Giacomo si prohlížel text dalšího dopisu, kerý měl schován na památku. Váhal, zda jej má zařadit do připravované knihy *Tajnosti mého života* a zda jej má přidat do šuplíku k ostatním textům.
Byl to dopis, který jej zastihl v Šumburku, kde se léčil se svojí zraněnou paží u známého léčitele Jana Kittla.
Nakonec se rozhodl, že i velmi jednoduché šifry, kam řadil i klasické šifry, ale třeba i tajné inkousty, steganografické metody apod. mají v jeho knize své místo, a vložil tento dopis do šuplíku k ostatním textům.

Úloha č.12 Stín hraběte Branického



C10. Adelaide de Gueidan podruhé

Giacomo usedl do svého oblíbeného křesla v knihovně duchcovského zámku a začal pročítat poštu, kterou mu právě dovezl kurýr z poštovního úřadu v Teplicích.
Mezi došlými dopisy byl opět jeden z Francie. Nebylo to až tak nic moc divného. Giacomo udržoval rozsáhlou korespondenci se svými známými a právě teď, ve dnech pro Francii tak bouřlivých, si s nimi horlivě dopisoval a navíc zajišťoval pro své známé i drobné služby.

Jeden dopis jej však na první pohled zaujal. Jako odesílatel byla uvedena hraběnka Adelaide de Gueidan. Dívka, kterou miloval téměř před padesáti lety. Patřila mezi jeho skutečné lásky. Vzhledem ke společenskému postavení však byla pro něj nedostupná. Navzdory tomu jí vděčil za mnohé. Byla to ona, kdo mu pootevřel dveře do nejvyšších společenských kruhů ve Francii, byla to ona, kdo jej seznámila se svým bratrancem Henrym a ten jej pak díky ní pozval do společenství Svobodných zednářů.

Blesklo mu hlavou: „Ona ještě žije! Pane Bože, vždyť je to již tak dávno.“
Nedočkavě dopis otevřel a s překvapením zjistil, že obsahuje text napsaný šifrou. Díval se na něj a přemýšlel, jaký systém mohla asi Adelaide zvolit. Klíč v dopise nebyl. Určitě však chtěla, aby si zprávu přečetl.

Pak mu konečně došlo. Ta moje milovaná zlatá chytrá hlavička!

Rychle a nedočkavě začal její dopis dešifrovat …

Úloha č.13 - Adelaide de Gueidan podruhé

```
63 2 3 64 21 91 28 659 6 303 122 614 32 56 47 313 314 129 4 309 216 658 111
404 52 73 662 651 148 657 301 49 73 88 601 29 60 77 78 410 82 26 30 203 72
123 145 505 138 611 39 413 506 615 511 652 524 135 217 303 520 129 217 98
222 307 669 11 56 34 212 602 140 78 515 216 131 514 127 658 49 317 318 315
49 55 76 512 655 101 9 29 304 305 28 501 418 143 619 613 620 611 619 616
612 617 620 611 524 502 514 522 521 413 505 305 507 418 506 309 219 137 322
139 99 324 203 85 94 117 214 25 91 106 417 625 614 150 149 127 659 518 77
307 72 602 56 660 206 419 410 607 501 415 302 143 95 43 662 64 111 223 25
401 86 306 602 17 106 317 44 422 215 39 57 201 80 4 2 13 70 301 59 658 615
201 100 501 4 115 87 306 84 304 209 417 210 78 111 15 74 311 202 93 224 56
106 83 19 517 103 317 312 91 213 99 26 316 112 313 88 94 72 129 101 657 96
140 71 85 144 517 95 317 218 311 105 324 78 127 668 119 81 411 108 652 215
```

D. 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.

Garant: **Pavel Vondruška**

Cena Základní cena: 4 000,00 Kč
Základní cena včetně DPH: 4 800,00 Kč
Čtenář Crypto-Worldu 50% sleva

Datum	Čas	Lektor	Volná místa	Přihlásit
24.-25.11.2010	09:00–17:00	Pavel Vondruška	?	http://www.nic.cz/akademie/course/15/detail/

Pozor – zájemci z řad registrovaných čtenářů e-zinu Crypto-World mají možnost získat 50% slevu. Postup: zájemce požadá e-mailem (ezin@crypto-world.info) o zaslání slevového kódu (kupónu). Tento jedinečný kód mu zajistí uplatnění slevy. Více informací na kontaktech akademie.

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 certifkát 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/

E. O čem jsme psali v říjnu 2000 – 2009

Crypto-World 10/1999

Crypto-World 10/2000

Příloha : ZoEP.htm

Dnešní užitečnou přílohou je plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000.

Crypto-World 10/2001

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)

(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

Crypto-World 10/2002

Crypto-World 10/2003

Crypto-World 10/2004

Crypto-World 10/2005

Crypto-World 10/2006

Crypto-World 10/2007

Crypto-World 10/2008

Crypto-World 10/2009

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
Stálí přispěvatelé:	Vlastimil Klíma
	Pavel Vondruška
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info