Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 14, číslo 5-6/2012 **24. červen**

5-6/2012

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1314 registrovaných odběratelů)

Obsah :

A. HERMANN POKORNY - "zaslúžilý umelec" v lúštiteľskom odbore vo víre I. svetovej vojny

Jozef Krajčovič, Crypto-World, kuutekac@gmail.com , http://katkryptolog.blogspot.sk

O mužovi, ktorého mimoriadne pohnuté životné osudy chceme v tomto krátkom článku sledovať, je známe, že zastával mnohé významné vojenské a štátne posty v bývalom Rakúsko-Uhorsku. Bol zakladateľom maďarskej rozviedky, ktorú organizoval a riadil dlhé roky, pôvodom bol rodeným Čechom, presnejšie však "uhorsky cítiaci český Rakúšan", mnohými považovaný za najtalentovanejšieho spravodajského dôstojníka v odbore lúštenia a rádiového odposluchu.

Obr. 1: Hermann Pokorny

Hermann Pokorny (česky Heřman Pokorný) sa narodil v Kroměříži na Morave dňa 7. apríla roku 1882.

Mesto v ktorom sa vtedy narodil, bolo bilingválnym územím, preto už ako dieťa vynikal v znalosti nemčiny a češtiny. Neskôr počas štúdia na Viedenskej kadetnej škole pre príslušníkov Landwehru a na dôstojníckej škole pre starších veliteľov sa naučil poľštinu a bulharčinu. Svoje vynikajúce jazykové znalosti ruského jazyka získal od istého revolucionára, ktorý utiekol zo Sibíri. Keďže mal mimoriadne znalosti cudzích jazykov, preto bol v hodnosti štábneho kapitána vyslaný do Moskvy. Na začiatku I. svetovej vojny slúžil na operačnom veliteľstve Generálneho štábu, c. a k. rakúsko-uhorskej armády. Jeho hlavnou úlohou bolo viesť podrobné záznamy o "kondícii protivníka" t.j. analyzovať a vyhodnocovať správy posielané bojovými jednotkami, vojenskými atašé, zamestnancami zahraničných ambasád a tajnými agentmi.

6. september 1914 drastickým spôsobom zasiahol do života Pokorného. Od tohto dňa začala rádiová stanica patriaca vrchnému veleniu v Przemysli zachytávať a zaznamenávať ruské rádiové telegramy. Pokorny požiadal veliteľa operačného strediska aby mohol byť preradený výlučne na odposluch ruských telegrafických spojov. V tomto mu vyhovel a poveril ho touto náročnou úlohou. Doposiaľ sa toto

stredisko sústredilo len na monitorovanie telegramov v otvorenej forme, ale od tohto momentu bolo zamestnancom nariadené zaznamenávať aj šifrované telegramy.
V priebehu septembrovej ofenzívy na východnej fronte v roku 1914 teda preukázal vtedajší kapitán Pokorný vynikajúce služby veliteľstvu 4. rakúsko-uhorskej armády. Za necelé tri dni rozlúštil šifru, ktorú používala Stavka (generálny štáb ruskej cárskej armády) pre svoje najtajnejšie depeše. Skupina, ktorej velil Pokorný, tvorená nadporučíkom von Marchesettim a podplukovníkom Zemánkom, spracovávala v najrušnejších dňoch až tridsať zachytených rádiogramov aj napriek tomu, že ruské vrchné velenie použité šifry často menilo.

Obr. 2: Rádiová odposluchová služba

V sledovanom období od 6. septembra 1914 až do 1. marca 1916 dokázal Pokorný rozlúštiť všetky ruské šifrovacie systémy, celkovo 18. Mimoriadne vysoká kvalita takto získaných informácií mala značný dopad na tri z najvýznamnejších vojenských operácií Generálneho štábu rakúsko-uhorskej armády, znamenala zastavenie a prinútenie na ústup celej ruskej cárskej vojnovej mašinérie (v rámci všeobecného útoku) v období november-december roku 1914, prielom v okolí mesta Gorlice v máji 1915 a okupácia pevnosti Brest-Litovsk dňa 25. augusta 1915.

Dňa 25. októbra 1914 štyri divízie cárskej armády sa rozostavili v útočnej línii tiahnucej sa pozĺž čiary Varšava-Ivangorod-Sandomierz, utvoriac tak obrovský ruský vojenský "parný valec". Zaútočili ním na prvú rakúsko-uhorskú armádu a deviatu nemeckú armádu. Až do úplného zastavenia postupu ruských vojenských jednotiek

dňa 15. novembra ich pohyby boli sledované najmä vďaka obsahu 240 rozlúštených rádiogramov. Útoky spoločných rakúsko-uhorských a nemeckých vojenských síl zovreli a nepriedušne obkľúčili ruské vojenské jednotky a tým prispeli k ich úplnej porážke.

Najmä pri prielome frontovej línie pri Gorliciach zohrali rozlúštené telegramy významnú úlohu. Veliteľstvo rakúsko-uhorskej armády sa dozvedelo o tom, že Rusi mali v týchto dňoch v značnej miere podceniť zúfalý stav a krízu ich bojovej situácie, a tak Mackensenova armáda dokázala úspešne rozvinúť prielom na tomto úseku fronty.

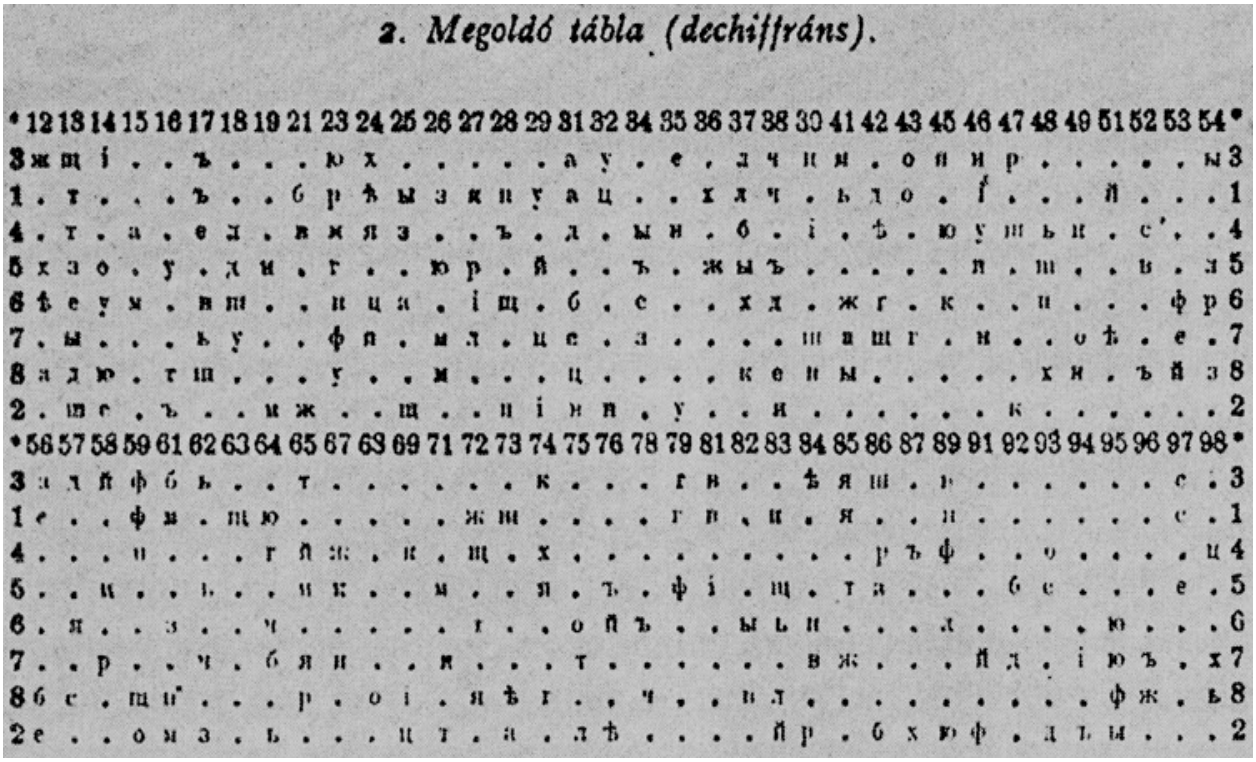
Rakúsko-uhorský generálny štáb vyjadril svoju spokojnosť s Pokorným pri zrýchlení vybavovania služobného postupu - v rámci jedného roku sa stal majorom a pred koncom vojny bol už podplukovníkom.

Neočakávane rýchla okupácia Brest-Litovska taktiež nastala vďaka informáciám, ktoré boli získané z 53 rozlúštených telegramov týkajúcich sa presnej štruktúry a počtov nepriateľských vojenských jednotiek. Keď nemecký generál Hans von Seeckt (1866-1936) pochodoval cez túto oblasť, pri odchode sa obrátil na Hermana Pokorného so slovami "Vy viete najlepšie, za čo Vám vďačí 11. armáda." Ďalej treba poznamenať, že výdatne prispel svojim podielom mimo iného k úspešnému výsledku nástupovej operácie pri Saneme a vojenskom stretnutí na rieke Stryj.
Rusi okrem iných šifier používali nasledujúcu šifrovaciu metódu:

Orosz katonai rejtkulcs.

1. Rejtjelező tábla (chiffráns).

*	а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ю	я	ь	ъ	ы	й	і	*
3	31	61	81	79	57	35	12	56	46	74	37	41	89	43	45	47	7	65	32	59	24	39	38	86	13	84	23	85	62	17	54	58	14	3
1	31	21	81	79	42	56	72	26	63	27	37	61	89	43	28	23	97	13	29	59	36	32	38	73	63	24	64	85	41	17	25	51	46	1
4	15	37	21	64	31	17	67	25	49	69	18	23	35	93	59	86	52	13	46	89	74	98	28	47	72	42	45	24	48	87	34	65	39	4
5	96	92	52	23	18	97	36	13	46	67	54	71	19	14	65	27	93	85	16	79	12	58	76	48	83	34	26	74	62	38	37	29	81	5
6	25	31	17	42	38	13	41	61	23	45	89	15	84	75	48	54	34	73	14	53	37	24	64	18	28	12	95	57	93	78	82	76	27	6
7	41	64	84	43	92	53	85	34	67	71	27	26	46	49	24	58	31	75	18	23	98	29	62	39	42	51	95	65	17	96	13	91	94	7
8	12	56	82	74	13	38	96	54	61	37	83	26	49	68	39	65	57	16	23	95	48	31	78	17	59	73	14	72	98	52	41	53	69	8
2	73	86	31	93	42	56	21	62	19	47	75	61	32	59	28	84	14	71	35	91	87	69	16	13	25	76	89	38	64	94	95	83	29	2



Obr. č. 3: Ruský cársky vojenský šifrovací kľúč používaný v I. svetovej vojne

Šifra sa riadi logikou Trittheimovej (Vigenérovej) tabuľky. Na začiatku komunikácie sa dohodne počet písmen, ktoré sa budú nahradzovať z každého riadku. Napríklad ak to boli 4 písmená, prvé písmená otvoreného textu by sa mali brať z šifrového riadka č. 1, nasledujúce 4 otvorené písmená z šifrového riadku č. 2 a tak ďalej. Ak sa použilo všetkých 8 riadkov, vrátilo sa na riadok č. 1. (Pozri príklad uvedený nižšie).

Ak sa z tabuľky berie po troch písmenách z každého riadku, prvý riadok národnej hymny cárskeho Ruska by sa zašifrovalo nasledovne:

БОЖ	Е	ЦА	РЯ	Х	РАН	И
az 1		2	3		4	5. sz.

rejtjelszámsorból: 21 43 72 56 69 73 47 85 24 86 15 35 46

Po zahájení útočných vojenských operácií v Rumunsku sa Pokorného skupina presťahovala do Sofie a tu si jej šéf vyslúžil titul "zaslúžilého rádiového umelca". Na sklonku roka 1917 zastupoval Pokorný záujmy rakúsko-uhorského armádneho velenia pri jednaní so sovietskou delegáciou v Brest-Litovsku.

Po vojne Pokorný zorganizoval cyklus prednášok na tému tajomstiev úspešného lúštenia šifier. Šifrovanie a dešifrovanie závisí na zložitosti použitého šifrovacieho postupu. Podľa jeho názoru boli najdôležitejšími predpokladmi pre úspešné zvládnutie šifier dokonalá znalosť použitého jazyka, značné intelektuálne schopnosti a trpezlivosť. Naviac pripúšťal, že pri týchto situáciách hrá významnú úlohu aj šťastie. V prvej polovici septembra 1919 Rusi šifrovali svoje telegramy iba pomocou jednopísmenného substitučného šifrovania a šifrovali len ich časť. Z kódových skupín bolo jasné, že iné písmená nejakým spôsobom nahradzovali určité písmená v texte.

Pokorný dokázal tento problém vyriešiť pomocou nedávno zachyteného telegramu. Odhalil trik tzv. kruhových šifrových abecied tak, že si povšimol že niektoré písmená sa periodicky opakovali. Podstata systému bola že ruská abeceda, ktorá obsahuje 35 písmen, sa zredukovala na 24 písmen a chýbajúcich 11 písmen sa rovnomerne rozdelilo medzi týchto 24 písmen ako dodatočné písmená.

Ďalšej výzve, ktorej čelil Pokorný bol systém číselných kódov. Riešenie bolo dosiahnuté čiastočne vďaka nedbalosti ruskej strany. Otvorený telegram, ktorý bol zachytený už predtým, bol znovu poslaný v zašifrovanej forme. Pokorný dokázal poľahky kód dešifrovať porovnaním týchto dvoch telegramov.

V lete roku 1918 Pokorný mal urobiť dôležité životné rozhodnutie. Rozhodoval sa o občianstvo ktorého nástupníckeho štátu by sa mal uchádzať. Keďže pôvodne pochádzal z Moravy, domnieval sa že v Rakúsku bude považovaný za občana druhej kategórie. Keďže jeho materinským jazykom bola nemčina nechcel sa stať ani českým občanom. Kedže ho rozpad rakúsko-uhorskej monarchie ťažko zasiahol, stiahol sa do ústrania, na dlho prerušil staré kontakty a nové nenadväzoval. Ani jeho najbližší známi a spolubojovníci nevedeli, kam sa podel. Koncom roka 1918 však prejavil oňho a jeho schopnosti záujem generál Alois Podhajský. Dozvedel sa totiž od plukovníka Vitouška, ktorý kedysi s Pokorným študoval na viedenskej Vojenskej akadémii, že sa tento vyhlásený šifrant usadil s najväčšou pravdepodobnosťou v Maďarsku. Bratislavský zemský veliteľ vtedy poveril Vitouška, aby svojho spolužiaka čo najskôr našiel. Ale až v januári roku 1919 sa zistilo, že hľadaný sa nedávno presťahoval na svoj statok v Gödöllő východne od Budapešti. Generál Podhájsky si okamžite sadol k stolu a poslal Pokornému písomnú ponuku. Prišla - ako sa hovorí -

pár sekúnd po dvanástej, pretože krátko predtým sa rozhodol prevrátiť list a požiadať o maďarské občianstvo. Kontaktoval maďarský generálny štáb, kde bol ochotne prijatý. Bol povýšený do šľachtického stavu, dostal menšie dedičné panstvo aj s pozemkami v Gödöllő, stal sa najlepšie honorovaným zamestnancom štátneho aparátu a ani dlho nečakal na generálsky patent. Dočasne bol zamestnaný na maďarskom likvidačnom úrade v novembri 1918. Neskôr bol pridelený k organizácii a vedeniu tzv. "skupiny S" (skupiny pre zber spravodajských informácií). Maďarské občianstvo získal dňa 5. marca 1919. Z poverenia maďarskej vlády strávil sedem rokov na Kryme ako neoficiálny vojenský pozorovateľ. Až do svojho odchodu do výslužby v roku 1930 pracoval v štáboch tzv. maďarských brigád pohraničnej stráže. Ako vyslúžilý generálporučík, poverený správou vojenských archívov, sústavne vyhodnocoval, sumarizoval a prekladal sovietsku vojensku a politickú literatúru. Ako prvé podrobne rozpracoval z vojensko-historického hľadiska tému obsadenia oblasti Bácska maďarskou armádou v roku 1941.

(Bácska je oblasť s rozlohou 8 750 štvorcových kilometrov medzi riekami Dunaj a Tisa, z ktorej 25% patrí k Maďarsku, 75% k Vojvodine (Srbsko). Väčšia časť bola po prvej svetovej vojne pripojená k Juhoslávii. V apríli 1941 sa Maďarsko pripojilo k nemeckým vojenským silám pri útoku na Juhosláviu s cieľom opätovného získania Bácska, čo aj dosiahlo. Dňa 28. apríla maďarská vláda nariadila, aby sa celá srbská populácia z Bácsky vysťahovala (približne 150000 ľudí).)

Boris Michailovič Šapošnikov, maršál Sovietskeho zväzu, sa s veľkým uznaním vyjadroval na adresu Pokorneho úspechov na poli lúštiteľského umenia. Vo svojej knihe "Géniovia armády" hodnotil úspechy a zlyhania vojenských operácií I. svetovej vojny. Na konci II. svetovej vojny sa Pokorny stretol s maršálom Malinovskym. Jednou z hlavných tém ich rozhovoru bolo lúštenie šifrovaných ruských telegramov.

Pokorný bol zvláštnym zamestnancom Ministerstva zahraničných vecí až do svojho konečného odchodu do dôchodku v roku 1949. Pri jeho odchode do výslužby dostal hodnosť generálplukovníka a získal najvyššie maďarské vojenské vyznamenanie Rád za zásluhy. Medzi rokmi 1950 až 1955 sa dokonca nedokázal vyhnúť politickým perzekúciám, bol mu odobratý výsluhový dôchodok. Zomrel vo veku 78 rokov roku 1960 v Budapešti. Záverom je treba taktiež spomenúť na jeho bratranca, majora

poľskej armády Franciszka Pokorného, ktorý sa po skončení I. svetovej vojny stal hlavou Biuro Szyfrów (Úradu pre šifry) pri poľskom generálnom štábe a bol jedným z troch prednášateľov v tajnom kryptologickom kurze vedenom v roku 1929 na Univerzite v Poznani, z ktorého vyšli traja úspešní frekventanti, známi neskôr ako pokoritelia nemeckého šifrovacieho stroja Enigma, Marian Rejewski, Jerzy Różycki a Henryk Zygalski.

Literatúra

[1] Révai, Zoltán, Titkosírások, Fejezetek a rejtjelzés történetébol, I. vyd. Budapest, Szegedi Kossuth Nyomda Kft, 1978, II. vyd., Szeged, Koyvkiadó, Lazi Bt., 2001, 300s. (slov. Tajné písmo, Kapitoly z histórie kryptografie), ISBN 963-9227-82-X, str. 254-259

[2] Pokorny, Hermann, Emlékeim, A láthatatlan hírszerzo, (slov. Moje pamäti, Tajný agent na neviditeľnom fronte), 1936, ISBN 963-9267-03-01

[3] Fárek, František, Stopy mizí v archivu, Praha: Vyšehrad, 1975, 256s. str. 13-15,

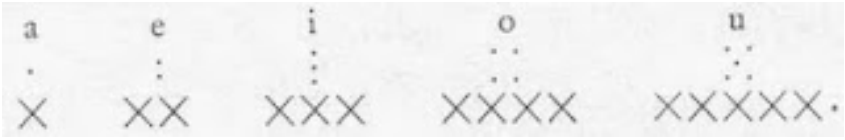
[4] Pacner, Karel, Československo ve zvláštních službách, díl I. - 1914-1939, Pohledy do historie československých výzvědných služeb 1914-1989, Praha: Themis, 2001, 528s., str. 158-159

[5] Wikipedia, heslo Franciszek Pokorny

B. Najstaršia zašifrovaná písomná pamiatka v Čechách

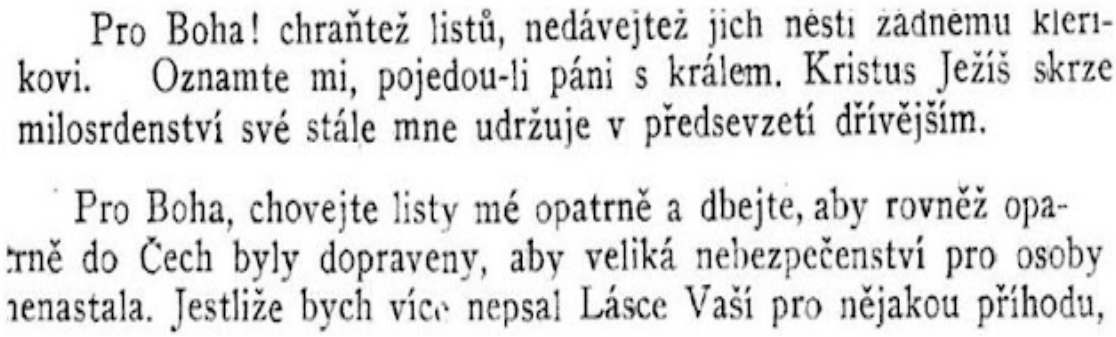
Jozef Krajčovič, Crypto-World, kuutekac@gmail.com , http://katkryptolog.blogspot.sk

Za najstarší doklad používania šifier a kódov vo svete, objavujúci sa v dobách vrcholného stredoveku, a to konkrétne v benátskych archívoch bola zrejme slabá politická kryptografia v podobe substitúcie samohlások bodkami alebo krížikmi v niekoľkých roztrúsených slovách.



A ďalej systém krátkeho zoznamu mien používaný v pápežskej kúrii v prvej polovici XIV. storočia a prv spočíval v zámene niektorých slov inými, dohovorenými. Tak napríklad miesto "*guelfovia*" sa písalo "*Synovia Izraela*", miesto "*ghibellíni*" - "*Egypťania*", miesto "*Rím*" - "*Jeruzalem*" atď." Doposiaľ sa za prvý dochovaný doklad o požívaní šifier v Čechách považovali listy **Majstra Jána Husa** z Kostnice z roku 1415. Jeho šifrový systém bol veľmi jednoduchý, šifroval iba samohlásky, a to tak, že ich nahradil písmenom, ktoré ho v abecede nasleduje. Miesto A písal B, miesto E napísal F atď. OKO, ALBATROS by zašifroval jako PKP, BLBBTRMS. Systém je samozrejme z kryptologického hľadiska veľmi slabý.

Čo je naozaj zaujímavé je, že Hus doporučoval svojim priateľom, aby listy nezverovali nedôveryhodným osobám (klerikom, atď.) a úzkostlivo dbal na spôsob a podmienky ich prepravy.



Pro Boha! chraňtež listů, nedávejteż jich nésti žádnému kleri-
kovi. Oznamte mi, pojedou-li páni s králem. Kristus Ježíš skrze
milosrdenství své stále mne udržuje v předsevzetí dřívějším.

Pro Boha, chovejte listy mé opatrně a dbejte, aby rovněž opa-
rně do Čech byly dopraveny, aby veliká nebezpečenství pro osoby
nenastala. Jestliže bych více nepsal Lásce Vaší pro nějakou příhodu,

Veľmi múdre rady Majstra Jána Husa svojim priateľom (Jánovi z Chlumu a Petrovi z Mladenovíc).

Avšak známy predvojnový český historik a povojnový disident Zdeněk Kalista tvrdil v recenzii knihy *Šifrování*, ktorej autorom bol Jaromír Lichtner, že **najstarším dokladom šifrovej korešpondencie v Čechách je jedna z listín či listov z formulárovej zbierky Jána z Přímdy**, datovanej koncom 14. storočia (presnejšie rokom **1389**, nachádza sa v Archíve Pražského hradu v knižnici metropolitnej kapituly, pod ozn. **I 40/2**). Taktiež uvádza ako prvý príklad najstaršieho známeho dochovaného úplne zašifrovaného dokumentu niekoľko depeší v listári neapolského arcibiskupa **Petra de Gratia** z rokov 1363-1364 (nachádzajúcich sa vo Vatikánskom archíve).

Literatúra

1. Kahn, D.: *The Codebreakers*, New York: Scribner, 1996, s. 106-7,

2. Ryba, Bohumil: *K tajnému písmu v listech Husových*. In. Sborník historický č.1, r. 1953, s. 46-52,

3. Vondruška, Pavel: *Šifry používané československými osobnostmi*, MKB 2011, prezentácia

4. Kalista, Zdeněk: recenze knihy Lichtner, Jaromír : *Šifrování. Úvod do kryptografie chemické i grafické se 40 šifrovými klíči*. Praha, komise- Al. Srdce 1939. 108 s. In. ČČH [45], 1939, č. 2, s. 428-429.

C. Nízkoriziková kryptografie

RNDr. Vlastimil Klíma, nezávislý kryptolog – konzultant, KNZ s.r.o., v.klima@volny.cz

Nízkoriziková kryptografie (Low Risc Cryptography) je pojem, který jsem si vymyslel a netuším, jestli je vhodný. Takže popíši, jak jsem k němu dospěl. Čas od času zjišťuji, že AES nebo SHA-2 je strašně pomalé nebo nevýhodné pro prostředí, do kterého navrhuji nějaké kryptografické nástroje nebo služby. Obojí to jsou nástroje, určené pro široké spektrum prostředí a podmínek, a tak byly také navrhovány. Samozřejmě při návrhu těchto kryptografických nástrojů (například AES, SHA-2) bylo jasné, že pokud by bylo prostředí pro jejich použití definováno úžeji a přesněji, mohl by být příslušný standard rychlejší, kompaktnější apod. Ukazuje se, že rozdíly mezi výkonností „specializovaných“ nástrojů a obecných nástrojů mohou být i sto nebo dvě stě procent!

Z podobného důvodu vznikla oblast Lightweight Cryptography – Lehká kryptografie, která je určená do prostředí nejmenších myslitelných čipů (RFID), kam se třeba AES prostě nevejde. A najednou je možné, aby klíč byl pouze 80bitový a šířka bloku blokové šifry 64 bitů, tedy čísla, která jsou jinak a jinde zavrhována. Proč? Ve skutečnosti k tomu nedošly žádné velké bezpečnostní analýzy, ale prostě skutečnost, že potřebná plocha křemíku na realizaci paměťových buněk pro velké klíče nebo šířky bloku je prostě velká. Proto byly sníženy nároky. Na druhé straně pro způsob, rozsah a účel použití je toto dostatečná bezpečnost, alespoň si to myslím. Samozřejmě mohou být výjimky, potvrzující pravidlo.
Nízkoriziková kryptografie je podobná, je to kryptografie pro prostředí, kde útočník nemá tolik možností, jako „obecný útočník“ v obecné kryptografii. Jestliže Lehká kryptografie měla „definované podmínky použití“ omezené na nejmenší čipy RFID, pak Nízkoriziková kryptografie má definované podmínky použití, které nějakým způsobem snižují možnosti útočníka.

Pro oblast nízkorizikové kryptografie je právě typické, že v bezpečnosti může jít „dolů“, protože útočník má z důvodu způsobu použití méně možností než obecně uvažovaný útočník. Tato omezení se mohou týkat počtu operací nebo omezených možností provádět útoky:

- se znalostí otevřeného textu
- s možností volit otevřený text
- s možností volit šifrový text

a / nebo

- omezeným množstvím použitých klíčů
- omezeným množstvím použitých otevřených textů.

Nízkorizikové nástroje budou pravděpodobně navrhovány přímo pro nějaký konkrétní systém, i když poté mohou být použitelné i v jiném nízkorizikovém systému. Snad je tu tedy i možný prostor pro určitou standardizaci, která bude mít spíše formu toho, že nějaký publikovaný nízkorizikový nástroj se bude moci využít i jinde než pro prostředí, kde byl navrhnut. Tedy asi žádné masové použití.

Co je však společného pro obecnou a nízkorizikovou kryptografii, je garance bezpečnosti a vědecký přístup. Stejně jako u obecného nástroje, i u nízkorizikového nástroje budeme definovat podmínky použití (například snížený počet otevřených textů, klíčů, sníženou požadovanou bezpečnost, konkrétní snížené možnosti útočníka) a dokazovat stupeň bezpečnosti, který daný nástroj poskytuje.

LR-AES aneb Nízkoriziková náhrada AES

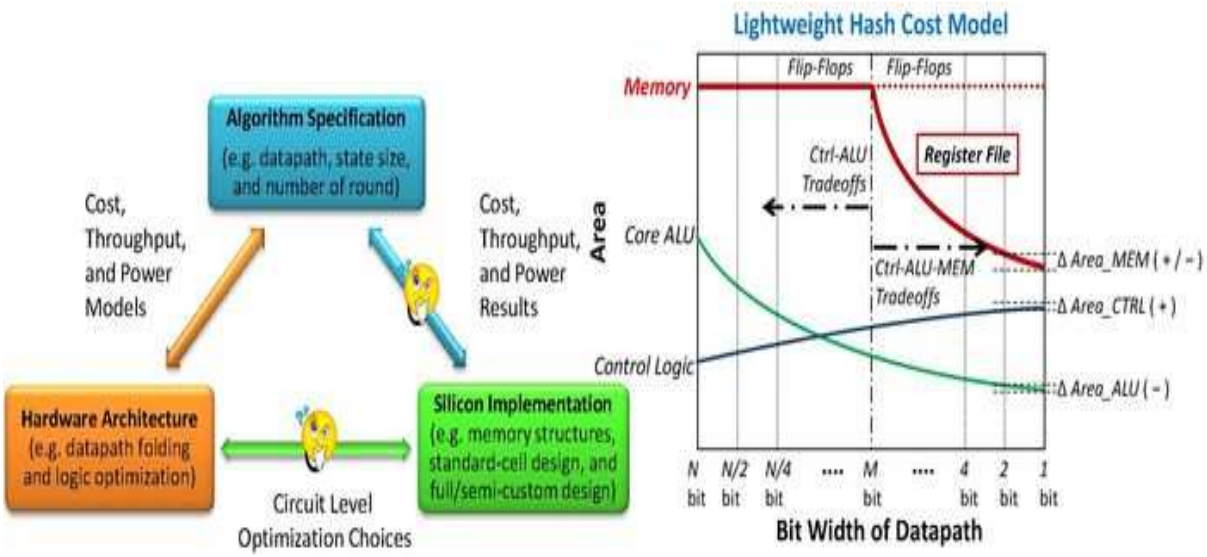
Pro příklad uveďme definici nízkorizikové blokové šifry. Je to bloková šifra, která nemusí být tak bezpečná jako AES, ale musí být mnohem rychlejší. Je určena do prostředí softwaru pro 64bitové procesory osobních počítačů. Aby byla systémově kompatibilní s AES (ale zase neměla zbytečné parametry), požaduje se jedna délka bloku a jedna délka klíče – obojí 128 bitů. I když klíč je definován jako 128bitový, aby bylo možné provést systémovou náhradu AES za LR-AES (Low Risc AES), není nutné, aby byly všechny bity klíče „platné“ nebo „vyplněné“. A to proto, že požadovaná bezpečnost je 2^80, nikoli 2^128. Další omezení se týká počtu otevřených textů, které je možné zašifrovat/dešifrovat během platnosti jednoho klíče a možností útočníka. Aby mělo smysl LR-AES používat místo AES, musí mít nějaký podstatný přínos, čímž je na mysli rychlost. Shrneme-li tedy nízkoriziková omezení, máme:

Definice podmínek:

- Délka bloku 128 bitů
- Délka klíče 128 bitů
- LR-AES je určena do prostředí 64bitových procesorů pro „velké počítače“ (stolní počítače, notebooky, netbooky)
- Jedním klíčem je možné zašifrovat pouze jeden Pentabyte (1000 TB) dat, tj. 2^50 B / 16B = 2^46 bloků dat
- Útočník může znát nebo volit dohromady maximálně 2^46 bloků dat
- Útočník má k dispozici pouze tolik operací na jeho technice, které odpovídají 2^64 průběhům blokové šifry (přitom je lhostejné, zda se mění otevřený text nebo klíč nebo obojí)
- LR-AES musí být nejméně o 100-200% rychlejší než AES

Závěrem jen příslib, že velmi brzo přineseme i konkrétní návrh LR-AES.

Doprovodný obrázek k pojmu ***Lightweight Cryptography - Lightweight Hash***



The Technology Dependence of Cost Analysis of LightweightHash Designs,

převzato z http://filebox.vt.edu/users/xuguo/homepage/newproject.html

D. Společná novela zákona o elektronickém podpisu (účinná od 1.7.2012)

Pavel Vondruška, Crypto-World,
pavel.vondruska@crypto-world.info

D1. Zákon o elektronickém podpisu 227/2000 Sb.

Zákon o elektronickém podpisu 227/2000 Sb. se stal nedílnou součástí našeho právního řádu. Postupně byly všechny typy podpisů, které zde tento zákon zavádí, akceptovány do nejrůznějších oblastí a právní praxe. Akceptace byla zajištěna novelou řady zákonů. Mimo těch, které jsou (byly) uvedeny přímo v zákoně je podpis v současné době zmíněn v celé řadě dalších zákonů. Mezi nejvýznamnější pak bezesporu patří Zákon 499/2004 Sb. o archivnictví a spisové služeb a Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

V řadě právních předpisů byl pojem elektronického podpisu citován a odkazován ne zcela přesně a často nejasně např. jen odkazem na Zákon č.227/2000 Sb. (např. takto: může být podepsáno resp. opatřeno podle zvláštního právního předpisu). Toto v praxi vedlo k nejasnostem při aplikaci těchto předpisů.

V průběhu let 2000-2012 byl zákon několikráte novelizován. Z větších novel zde připomeneme tu nejrozsáhlejší z 26. července 2004. Tato novela zákona o elektronickém podpisu (č. 440/2004 Sb.) nově zavedla pojem „kvalifikované časové razítko“, které prokazuje existenci elektronického dokumentu v čase. Další novinkou byla v evropském kontextu ojedinělé rozdělení pojmu podpis fyzické osoby a podpis technického zařízení, které provádí označení automaticky na základě vůle vlastníka tohoto zařízení – tedy zavedení tzv. „elektronické značky“. Pro ty se stejně jako pro zaručený elektronický podpis se používá technologie digitálních podpisů. Rozdíl mezi nimi spočívá v tom, že elektronickou značkou může označovat data i právnická osoba nebo organizační složka státu a používat k tomu automatizované postupy.

Větší novelou byla i novela zákona o elektronickém podpisu (č. 101/2010 Sb.), která nabyla účinnosti 15. dubna 2010. Tento předpis (v reakci na rozhodnutí 2009/767/ES) nařizuje Ministerstvu vnitra novou povinnost a to vést a zveřejňovat

seznam důvěryhodných certifikačních služeb a stanoví orgánům veřejné moci povinnost uznávat kvalifikované certifikáty vydané v ostatních členských státech EU.

V rychlém sledu pak následovaly drobné novely, které byly provedeny zákonem č. 281/2009 Sb. (s účinností od 1. ledna 2011) a zákonem č. 424/2010 Sb. (část změn s účinností od 30 prosince 2010 a část s účinností od 1. ledna 2012).

Zákon č. 227/2000 Sb., o elektronickém podpisu - s přehledným barevným vyznačením těchto posledních změn si lze stáhnout z webu Ministerstva vnitra:

http://www.mvcr.cz/soubor/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx

D2. „Společná“ novela (zákon č. 499/2004 Sb., zákon č. 227/2000 Sb. a další.)

Celkem v tichosti a bez velkého zájmu médií proběhla letos na jaře rozsáhlá (co do počtu změn) a však co do obsahu nikoliv příliš zásadní tzv. “společná“ novela, která mění jak zákon č. 227/2000 Sb., o elektronickém podpisu, tak i zákon č. 499/2004 Sb., o archivnictví a spisové službě. A spolu s nimi opravuje (spíše než nějak zásadně mění) celou řadu dalších právních předpisů.

Plné název této novely:

Zákon, kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů, a další související zákony

Citace: 167/2012 Sb., Částka: 60/2012 Sb.,

Rozeslána dne: 30. května 2012

Datum přijetí: 25. dubna 2012,

Datum účinnosti od: **1. července 2012**

http://www.sbirka.cz/POSL4TYD/NOVE/12-167.htm

Udělejme si stručnou inventuru toho, co všechno se díky uvedené novele k uvedenému datu změní a to zejména s ohledem na p„elektronické podpisy a značky“:

1) mění se definice tzv. uznávaného podpisu:

„zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby“

Definice je rozšířena o požadavek na jednoznačnou identifikaci podepisující osoby. A také zpřesňuje povinnost jeho používání ve veřejné správě i ve vztahu k veřejné správě. A dále upřesňuje uznávání zahraničních kvalifikovaných certifikátů

2) dále dochází k důsledné opravě ve všech ostatních zákonech, které dosud umožňovaly používat „pouze“ zaručený elektronický podpis a klade se zde nyní povinnost používat pouze uznávaný podpis. Konkrétně jde o změnu níže uvedených paragrafů v následujících zákonech:

Občanský soudní řád (§47, §174), Rejstřík trestů (§11 a následující), Katastrální zákon (§344), Zákon O návykových látkách (§28-31),Zákon O posuzování vlivů na životní prostředí (§6), Zákon o zbraních (§42), O služebním poměru příslušníků bezpečnostních sborů (§175), Správní řád (§19, §37,§69), Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, Zákon o elektronických komunikacích (§25,33,75), Občanský soudní řád (§174), Zákon o střetu zájmů (§12), Insolvenční zákon (§97), Zákon O výzkumu na lidských embryonálních kmenových buňkách a souvisejících činnostech (§5), Zákon O stabilizaci veřejných rozpočtů (čl. LXXII-IV §17), Zákon o zdravotních službách (§55), Zákon o specifických zdravotních službách (§44)

Důsledkem toho je, že prakticky jiný než uznávaný podpis nyní není po této společné novel v českých právních předpisech zmíněn. Buď je tedy (pokud není forma v právním předpisu stanovena) možno použít jakoukoliv formu elektronického podpisu nebo je potřeba použít uznávaný podpis, protože ostatní formy, které byly doposud zmiňovány, byly touto formou důsledně nahrazeny. Konkrétně jde tedy zejména o náhradu zaručeného elektronického podpisu a zaručeného elektronického

podpisu založeného na kvalifikovaném certifikátu. Za zajímavost jistě stojí i to, že se stále v českém právním řádu (na rozdíl od běžné praxe v EU) neobjevil požadavek na použití *kvalifikovaného podpisu* tedy zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu vytvářený bezpečným podpisovým prostředkem. Dále se mění se terminologie a místo *opatřit podpisem nebo značkou* se celkem důsledně (a podle mne méně přesně) zavádí *podepsat* (příklad*: "opatřený zaručeným elektronickým podpisem nebo elektronickou značkou" se nahrazuje slovy "podepsaný uznávaným elektronickým podpisem nebo označený uznávanou elektronickou značkou"*.)

3) mění se definice pojmu „datová zpráva“, neboli toho, co je podepisováno, nově se zcela logicky připouští i to, že se může jednat o data v podobě souboru

4) mění se požadavky a pravidla na uchovávání informací o vydaných a zneplatněných kvalifikovaných certifikátech

5) změn je samozřejmě mnohem více, např. za významné lze dále považovat pokus zareagovat na Rozhodnutí Komise 2011/130/ES z února 2011, které zavádí tzv. referenční formáty podpisů PAdES-BES a EPES, jde-li o PDF dokumenty a připouští i používání dosavadních klasických formátů (PKCS#7) za podmínky poskytnutí informací o tom, jak lze jejich platnost ověřit.

6) **ministerstvo vnitra také dostává zmocnění k vydání prováděcí vyhlášky, která má stanovit závazné postupy pro ověřování platnosti elektronických podpisů, značek a certifikátů**

Ministerstvo vnitra povinnost, vydat vyhlášku pro ověření podpisů a certifikátů velmi rychle splnilo a stihlo připravit a vydat vyhlášku tak, aby byl účinná také od onoho „magického data“ 1.7.2012, kterým začíná platit výše popsaná „společná novela“ . Podívejme se na závěr na tuto vyhlášku.

D3. Vyhláška 212/2012 Sb. o postupech při ověření platnosti zaručeného elektronického podpisu

Vyhláška o struktuře údajů, na základě kterých je možné jednoznačně identifikovat podepisující osobu, a postupech pro ověřování platnosti zaručeného elektronického podpisu, elektronické značky, kvalifikovaného certifikátu, kvalifikovaného systémového certifikátu a kvalifikovaného časového razítka (vyhláška o ověřování platnosti zaručeného elektronického podpisu)

Citace: **212/2012 Sb**. Částka: 75/2012 Sb.

Rozeslána dne: **20. června 2012**

Datum přijetí: **13. června 2012,**

Datum účinnosti od: **1. července 2012**

http://www.sbirka.cz/POSL4TYD/NOVE/12-212.htm

Vyhláška definuje závazné postupy při ověřování. Osobně vidím tuto vyhlášku jako velmi přínosnou, protože jsem se setkal v praxi s tím, že se tak důsledně nepostupovalo a bylo obtížné prokazovat, že je to nutné. Lze samozřejmě najít určité nedostatky, které plynou zejména z toho, že vyhláška nestačila zatím zareagovat na již zmíněné referenční formáty podpisů. U těchto formátu si umím představit, že vyhláška někdy v budoucnu rozšíří požadavky na ověření specifických detailů těchto formátů.

E. Call for Papers - Mikulášská kryptobesídka

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

Základní informace

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

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *29. listopadu* a (b) půldne prezentací příspěvků a diskusí v pátek *30. listopadu 2012*. Pro workshop jsou domluveny zvané příspěvky:

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

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.buslab.org.

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a tak, aby přišly nejpozději do *1. října 2012*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2012 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *29. října*. Příspěvek pro sborník workshopu pak musí být dodán do *12. listopadu*.

Důležité termíny

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

Programový výbor

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

Mediální partneři

F. O čem jsme psali v květnu a červnu 2000 – 2011

Crypto-World 5/2000

Crypto-World 6/2000

Příloha : Navajo Code Talkers, revize z 15.6.1945, soubor Dictionary.htm

Crypto-World 5/2001

Příloha : priloha.zip - mystery.mid (viz. článek "Záhadná páska z Prahy")

Crypto-World 6/2001

Crypto-World 5/2002

Crypto-World 6/2002

Crypto-World 5/2003

Crypto-World 6/2003

Crypto-World 5/2004

Crypto-World 6/2004

Crypto-World 5/2005

Crypto-World 6/2005

Crypto-World 5/2006

Crypto-World 6/2006

Crypto-World 5/2007

Crypto-World 6/2007

Příloha: Mikulášská kryptobesídka (6.-7.12.2007)- MKB2007_CallForPapers_cerven.pdf

Crypto-World 5/2008

Příloha: 1) Mikulášská kryptobesídka (4.-5.12.2008): CFP_MKB2008_May.pdf
2) Příloha k článku „Príklad útoku na podpisovaný dokument … “ : priklad.bmp

Crypto-World 6/2008

Crypto-World 5/2009

Příloha: Call for Papers Mikulášská kryptobesídka 2009 - CFP_MKB2009.pdf

Crypto-World 6/2009

Příloha: javascript-priloha.pdf (179 kB), avascript-priloha_1_3.rtf (64 kB)

Crypto-World 5/2010

Crypto-World 6/2010

Crypto-World 5/2011

Crypto-World 6/2011

G. Závěrečné informace

1. Sešit

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

2. Registrace / zrušení registrace

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

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška Jozef Krajčovič 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