Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 15, číslo 11-12/2013 **15. prosinec**

11-12/2013

Připravil: Mgr. Pavel Vondruška

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

Obsah :

		str.
A.	**Ukládání hesel bezpečně (J.Vrána)**	**2 - 3**
B.	**Nomenklátory 17. a 18. století (J.Mírka, P.Vondruška)**	**4 - 6**
C.	**Letošní soutěž v luštění skončila – výsledky (P.Vondruška)**	**7 - 8**
D.	**Analýza Rabenhauptovho zašifrovaného dopisu (E.Antal, P.Zajac)**	**9 – 17**
E.	**PF 2013 (P.Vondruška)**	**18**
F.	**O čem jsme psali za posledních 12 měsíců**	**19 – 20**
G.	**Závěrečné informace**	**21**

Příloha k článku D: http://web.telecom.cz/depotpv/ASD12/priloha_k_D.zip

A. Ukládání hesel bezpečně

Jakub Vrána, jakub@vrana.cz, http://www.vrana.cz/

Úvodem

V Crypto-Worldu 9-10/2013 vyšel článek „***Ochrání hashování uživatelská hesla?“***, který na otázku z titulku podle mne bohužel zcela neodpověděl. Rozhodl jsem se tedy reagovat tímto svým článkem, kde popíšu, jak uživatelská hesla správně ukládat.

V první řadě musíme vyloučit nesmyslná řešení jako ukládání hesel v čistém textu nebo jejich šifrování. Jsou špatná proto, že heslo se nesmí dozvědět ani provozovatel aplikace, který má přístup ke všem algoritmům, datům a klíčům. Pro ukládání hesel je potřeba použít hašování a k heslu přiložit náhodnou sůl. Tu přidáváme především proto, aby nebylo poznat, že dvě hesla jsou stejná, ať už hesla dvou uživatelů u stejné služby nebo hesla stejného uživatele u dvou různých služeb. Druhým důvodem je zamezení použití *rainbow tables* – předpočítaných tabulek hašů.

Pomalé hašovací funkce

Víme už tedy, že hesla musíme hašovat a že k nim musíme přiložit náhodnou sůl. Zbývá výběr vhodné hašovací funkce. Běžné hašovací funkce jako MD5, SHA-1 nebo SHA-2 jsou pro ukládání hesel nevhodné především proto, že jsou příliš rychlé. MD5 hesla složeného z osmi malých písmen prolomí oclHashcat na celkem běžné grafické kartě průměrně za **10 sekund** (26^8 / 10.742e9 / 2)! Pokud požadavek na heslo zpřísníme třeba tím, že budeme vyžadovat použití i velkých písmen a čísel, tak řada uživatelů dá velké písmeno na začátek a číslo přidá na konec. Takto zkonstruované heslo útočník prolomí dokonce za 4 sekundy. A to vůbec nemluvíme o použití slovníků nebo hesel získaných z dříve uniknutých databází.

Týrat uživatele požadavky na dlouhá a složitá hesla zkrátka není řešení. Geekům to možná vadit nebude, protože si heslo uloží do klíčenky, ale pro běžné uživatele to bude pohroma končící zapsáním hesla na žlutý papírek přilepený na monitor. Řešením je použít hašovací funkci, která je záměrně pomalá.

Pomalé hašovací funkce vám nabídnu tři: Bcrypt, PBKDF2 a Scrypt. Všechny tři se pro ukládání hesel dají použít, všechny mají parametr umožňující nastavit, kolik iterací hašování se má provést. Ten je vhodné nastavit tak, aby se jedno zadané heslo ověřilo na vašich serverech v rozumném čase, např. do půl sekundy. Vaše uživatele to nijak výrazně neomezí a útočníka to podstatně zpomalí.

Kterou funkci vybrat? Bcrypt je asi nejdostupnější, např. v PHP ji používá funkce password_hash a již dlouhou dobu i funkce crypt . PBKDF2 je nejstandardnější, používá se třeba ve WPA. Scrypt se od ostatních liší tím, že kromě počtu iterací používá i konfigurovatelné množství paměti, což bude představovat značný problém pro útočníka snažícího se paralelně louskat více hesel najednou. *Osobně bych tedy doporučil použít Scrypt.*

Mohlo by vás napadnout i prosté opakované použití rychlé hašovací funkce, třeba miliardkrát. Problém s tímto přístupem je v tom, že můžou vznikat cykly, které velkou množinu vstupů namapují na mnohem menší množinu hašů. Přestože jde spíše o teoretický problém, tak se tomuto řešení proto raději vyhněte.

Co se starými hesly?

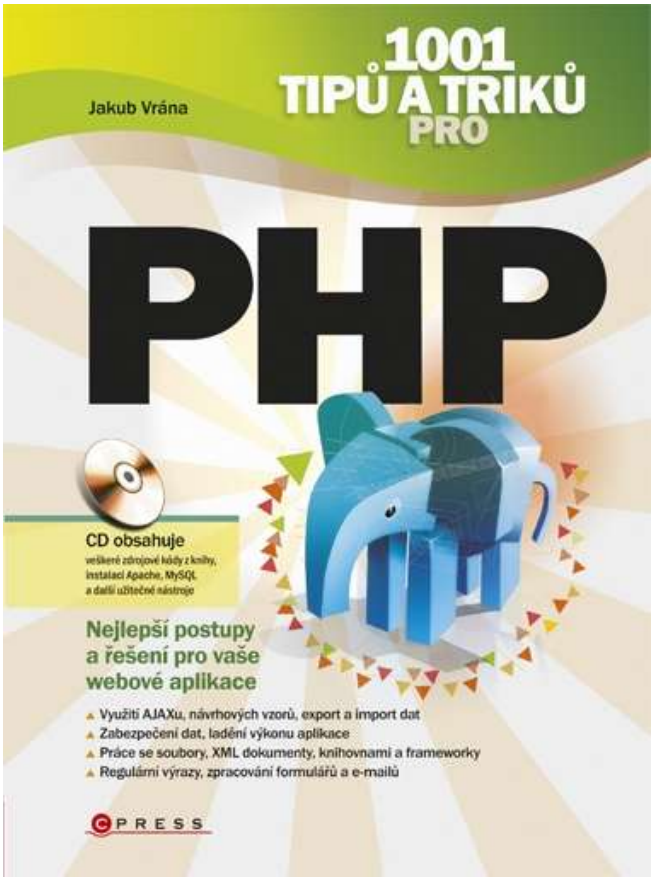
Co dělat v případě, že nevyvíjíte novou aplikaci, ale chcete zabezpečit nějakou stávající, kde máte hesla uložená třeba pomocí MD5?

Mohou vás napadnout tato řešení:

1. Nový algoritmus použít pro nově registrované uživatele a těm stávajícím ho změnit při přihlašování (kdy máte k dispozici heslo v čistém textu).
2. Uživatelům poslat zprávu a požádat je o změnu hesla.
3. Pokusit se prolomit všechna hesla a ta po aplikaci nového algoritmu znovu uložit.

Všechno to jsou hlouposti. Správné řešení je nový algoritmus aplikovat na původní haš, uložené heslo tedy bude např. výsledkem funkce scrypt(cost, salt, md5(password)). Všechny stávající uživatele převedete jednorázově a při ověřování hesla aplikujete danou posloupnost funkcí. Pokud se v budoucnu rozhodnete použít jiný algoritmus, jednoduše ho do posloupnosti přidáte.

Pokud máte důvodné podezření, že databáze s nebezpečně uloženými hesly už unikla, tak všechna stará hesla zneplatněte a uživatelům pošlete jednorázový odkaz pro jejich nové vytvoření.



Nejde jen o hesla

Hesla nejsou jediné tajemství, které musíme chránit. U webových aplikací je skoro stejně hodnotný i session identifikátor, který se používá pro přihlášené uživatele. Ten se na serveru často válí v čistém textu, aniž by se o něj někdo staral. Přitom když ho útočník získá, tak může jménem uživatele provádět většinu akcí. Věnujte mu proto stejnou pozornost jako heslu samotnému. Jen rychlost jeho výpočtu může být mnohem vyšší, protože se ověřuje mnohem častěji a při jeho úniku to přeci jen není tak velká katastrofa jako při úniku hesel – přinejhorším můžeme všechny uživatele odhlásit.

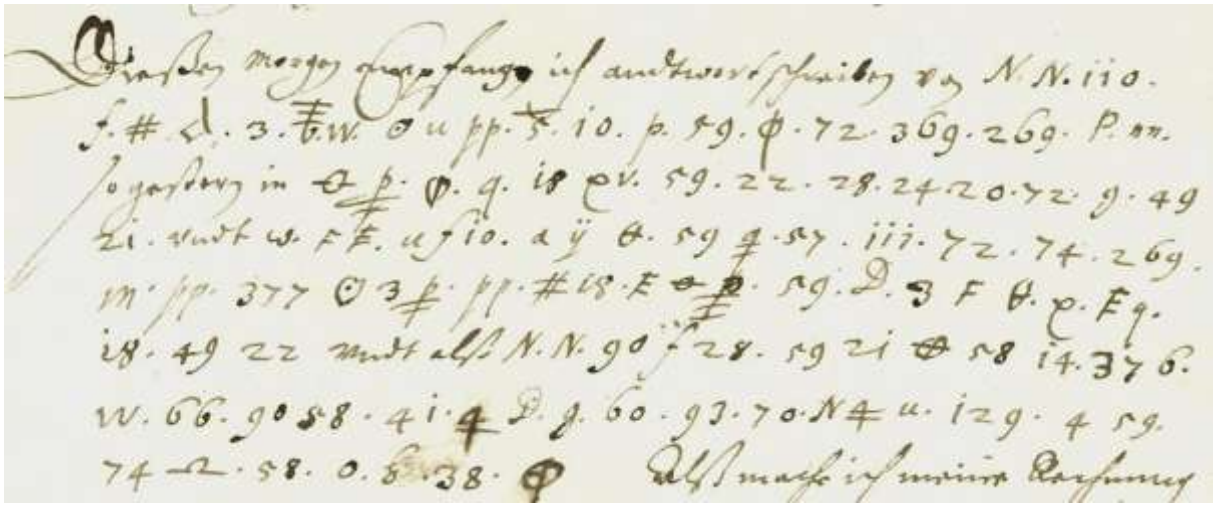
Přijďte si o tomto tématu popovídat 18. 12. 2013 na školení Bezpečnost PHP aplikací .

B. Nomenklátory 17. a 18. století

Jakub Mírka, SOA Plzeň, mirka@soaplzen.cz

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

Vzhledem k tomu, že do 1. 11. 2013 se nepodařilo nikomu vyluštit Rabenhauptovu šifru http://soutez2013.crypto-world.info/dopisy/obr1.jpg, kterou jsme předložili v rámci letošní podzimní soutěže v luštění http://soutez2013.crypto-world.info/, rozhodli jsme se vyslyšet prosbu a nápad jednoho ze soutěžících a poskytnout do posledních týdnů soutěže malou „nápovědu“. Jak naznačují uvozovky, nejednalo se o nápovědu v pravém slova smyslu, ale spíše o komparativní materiál odkazující na dobové nomeklátory, který podle nás mohl soutežícím pomoci udělat si představu, jak přibližně mohla Rabenhauptova šifra vypadat (předpokládáme, že jde o nomenklátor).



Obr. 1. Ukázka ze šifrovaného dopisu Karla Rabenhaupta ze Suché zaslaného Lantkraběnce Amálii Alžbětě v červnu (či červenci) 1646.

Tento materiál jsme pak rozeslali všem soutežícím a uveřejnili na stránce soutěže.
Domníváme se však, že shromážděný materiál by mohl zaujmout i ostatní čtenáře a může se hodit i jako vhodný materiál pro studium konstrukcí nomenklátorů, a proto jsme jej zařadili po skončení soutěže jako samostaný článek do našeho e-zinu.

Dále odkazované snímky dobových nomenklátorů pocházejí z archivního fondu Rodinný archiv Windischgrätzů ze Státního oblastního archivu v Plzni. Nomenklátory náležející do tohoto souboru sice pocházejí většinou až ze druhé poloviny 17. století nebo z první poloviny 18. století, ale jejich konstrukce je z kryptologického hlediska poměrně zajímavá, a tak jsme se domnívali, že by i tak mohly pomoci luštitelům v hledání řešení.

Kromě snímků byly zveřejněny i rekonstrukce několika dalších nomenklátorů, učiněné na základě srovnání otevřeného a šifrovaného textu. Tyto rekonstruované nomenklátory sloužily původně k pracovním účelům a z důvodu časové zaneprázdněnosti již nebyly před uveřejněním přepsány „na čisto“. Věříme ale, že i přesto se v nich lze snadno vyznat a mohou být vhodným zdrojem informací k tomu, jak tehdejší nomenklátory byly sestavovány. Oproti snímkům pořízeným z fondu Rodinný archiv Windischgrätzů mají však tu výhodu, že pocházejí z převážné části z doby třicetileté války stejně jako Rabenhauptův dopis.

Odkazy na shromážděné nomenklátory a jejich popisky:

1) Nomenklátor pro šifrování německy psané diplomatické korespondence blíže neurčených osob ze 2. poloviny 17. století. Obsahuje klíč pro homofonní substituci, bigramy a kódy. *SOA v Plzni, Rodinný archiv Windischgrätzů*, inv. č. 1403, karton 164.
http://soutez2013.crypto-world.info/nomenklator/1.jpg

2) Generální šifra (nomenklátor) císařských ministrů pro německy psanou korespondenci ze 2. poloviny 17. století. Obsahuje klíč pro homofonní substituci, kódy, klamače a pravidla pro psaní opakujících se písmen a dvojhlásek. *SOA v Plzni, Rodinný archiv Windischgrätzů*, inv. č. 1403, karton 164.
http://soutez2013.crypto-world.info/nomenklator/2.jpg

3) Nomenklátor pro šifrování německy psané diplomatické korespondence blíže neurčených osob patrně ze 2. poloviny 17. století. Obsahuje klíč pro homofonní substituci, kódy a klamače. *SOA v Plzni, Rodinný archiv Windischgrätzů*, inv. č. 1403, karton 164.
http://soutez2013.crypto-world.info/nomenklator/3.jpg

4) Nomenklátor pro šifrování francouzsky psané diplomatické korespondence blíže neurčených osob patrně ze 2. poloviny 17. století. Obsahuje klíč pro homofonní substituci, bigramy a kódy. *SOA v Plzni, Rodinný archiv Windischgrätzů*, inv. č. 1403, karton 164.
http://soutez2013.crypto-world.info/nomenklator/4.jpg

5) Nomenklátor pro šifrování italsky psané diplomatické korespondence blíže neurčených osob ze 2. poloviny 17. století. Obsahuje klíč pro mírně homofonní substituci, klamače, bigramy a kódy. *SOA v Plzni, Rodinný archiv Windischgrätzů*, inv. č. 1403, karton 164.
http://soutez2013.crypto-world.info/nomenklator/5.jpg

6) Nomenklátor pro šifrování italsky psané korespondence s kardinálem Cienfuegem z 1. poloviny 18. století. Obsahuje klíč pro mírně homofonní substituci, bigramy, kódy a klamače. *SOA v Plzni, Rodinný archiv Windischgrätzů*, inv. č. 1403, karton 164.
http://soutez2013.crypto-world.info/nomenklator/6.jpg

7) Rekonstrukce nomenklátoru pro německy psanou šifrovanou korespondenci dvorské komory. Rekonstruováno na základě korespondence z roku 1673 uložené v archivním fondu Rodinný archiv Windischgrätzů ve Státním oblastním archivu v Plzni. Nomenklátor obsahuje klíč pro jednoduchou substituci, bigramy a kódy (zjištěna jen nepatrná část).
http://soutez2013.crypto-world.info/nomenklator/7.jpg

8) Rekonstrukce klíče pro homofonní substituci užívanou v korespondenci Johanna Karla ze Schönburgu a Maxmiliána z Trauttmansdorffu. Rekonstruováno na základě korespondence z roku 1637 uložené v archivním fondu Rodinný archiv Trauttmansdorffů ve Státním oblastním archivu v Plzni.
http://soutez2013.crypto-world.info/nomenklator/8.jpg

9) Rekonstrukce nomenklátoru pro německy psanou šifrovanou korespondenci Ferdinanda Zikmunda Kurtze von Senftenau a Maxmiliána z Trauttmansdorffu. Rekonstruováno na základě korespondence z let 1638-1639 uložené v archivním fondu Rodinný archiv Trauttmansdorffů ve Státním oblastním archivu v Plzni. Nomenklátor obsahuje klíč pro homofonní substituci, bigramy a klamače. Neobsahuje žádné kódy.
http://soutez2013.crypto-world.info/nomenklator/9.jpg

10) Rekonstrukce nomenklátoru pro německy psanou šifrovanou korespondenci Ferdinanda Zikmunda Kurtze von Senftenau a Maxmiliána z Trauttmansdorffu. Rekonstruováno na základě korespondence z roku 1646 uložené v archivním fondu Rodinný archiv Trauttmansdorffů ve Státním oblastním archivu v Plzni. Nomenklátor obsahuje klíč pro homofonní substituci a kódy (zjištěna jen nepatrná část).
http://soutez2013.crypto-world.info/nomenklator/10.jpg

11) Rekonstrukce nomenklátoru pro latinsky psanou šifrovanou korespondenci Františka Pavla de Lisola, Johanna Tasselta a Maxmiliána z Trauttmansdorffu. Rekonstruováno na základě korespondence z léta roku 1645 uložené v archivním fondu Rodinný archiv Trauttmansdorffů ve Státním oblastním archivu v Plzni. Nomenklátor obsahuje klíč pro homofonní substituci, dvojhlásky, klamače a kódy (zjištěna jen nepatrná část).
http://soutez2013.crypto-world.info/nomenklator/11.jpg

12) Rekonstrukce nomenklátoru pro latinsky psanou šifrovanou korespondenci Františka Pavla de Lisola a Maxmiliána z Trauttmansdorffu. Rekonstruováno na základě korespondence z prosince roku 1645 uložené v archivním fondu Rodinný archiv Trauttmansdorffů ve Státním oblastním archivu v Plzni. Nomenklátor obsahuje klíč pro homofonní substituci, klamače a kódy (jednotlivé kódy nezjištěny až na pravděpodobný kód pro slovo „rex“, tj. král).
http://soutez2013.crypto-world.info/nomenklator/12.jpg

13) Konečně uvádíme odkaz na knihu Aloyse Meistera *Die Geheimschrift im Dienste der päpstlichen Kurie von ihren Anfängen bis zum Ende des XVI. Jahrhunderts*.

https://archive.org/details/diegeheimschrif00meisgoog

Tato kniha obsahuje celou řadu klíčů a nomenklátorů papežské kurie především ze 16. století, které sloužily především pro italskou a latinskou korespondenci. Ovšem i tyto nomenklátory by mohly být luštitelům užitečné, neboť papežská kurie užívala již v 16. století šifrovací metody, s nimiž se setkáváme u šifrovaných dopisů různé provenience ještě v 17. století.

C. Letošní soutěž v luštění skončila – výsledky

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

Vážení soutěžící, děkujeme za váš zájem a účast v letošní soutěži v luštění, kterou jsme vyhlásili Crypto - Worldu 07-08/2013 a pro jejíž podporu byla vytvořena doprovodná stránka http://soutez2013.crypto-world.info/ .

Stručná statistika letošní soutěže:
Celkem soutěžících: 40
Počet soutěžících, kteří vyřešili prvé dvě úlohy: 17

Přehled předložených úloh:
1. úloha (2 body) (17 řešitelů)
2. úloha (2 body) (18 řešitelů)
3. úloha (96 body) (0 řešitelů)

1. úloha - Vstupní test 1 (1/1)

Jako první úloha, kterou jsme označili jako vstupní test 1, byl zveřejněn tento dopis: http://soutez2013.crypto-world.info/dopisy/obr3.jpg
V doprovodném článku J.Mírky šlo dohledat, že jde o francouzsky psaný dopis Alexandra de Bournonville Maxmiliánovi z Trauttmansdorffu, v němž mu oznamuje, že u Arnsbergu byly zachyceny dva dopisy Karla Rabenhaupta ze Suché, jejichž opisy mu zasílá. 21. července 1646. *SOA v Plzni, pracoviště Klášter, Rodinný archiv Trauttmansdorffů, inv. č. 125.*
Jméno pisatele Alexandre de Bournonville se v článku vyskytuje na několika místech. Nebylo třeba nic luštit. Stačilo vložit správné jméno pisatele dopisu.
Správná ospověď proto byla: ALEXANDRE

2. úloha - Vstupní test 2 (1/2)

Jako druhá úloha, kterou jsme označili vstupní test 2, byl zveřejněn tento dopis: http://soutez2013.crypto-world.info/dopisy/obr2.jpg
Tentokráte šlo o opis nešifrovaného dopisu Karla Rabenhaupta ze Suché zaslaného lantkraběnce Amálii Alžbětě 13. července 1646. *SOA v Plzni, pracoviště Klášter, Rodinný archiv Trauttmansdorffů, inv. č. 125.*
Dopis je zmíněn v doprovodném článku k souteži.
Opět nebylo třeba nic luštit. I zde opět stačilo vložit správné jméno pisatele dopisu.
Správná ospověď: RABENHAUPT

3. úloha - Soutežní úkol (1/3)

Jako třetí a hlavní úloha soutěže byl předložen opis šifrovaného dopisu Karla Rabenhaupta ze Suché zaslaného Lantkraběnce Amálii Alžbětě v červnu (či červenci) 1646. *SOA v Plzni, pracoviště Klášter, Rodinný archiv Trauttmansdorffů, inv. č. 125.* http://soutez2013.crypto-world.info/dopisy/obr1.jpg
Tento dopis byl zachycen katolickou stranou, a tak k adresátce nikdy nedoputoval a nemohl být příjemcem dešifrován. Rabenhauptovi protivníci se jej sice pokoušeli rozluštit nebo zjistit klíč jiným způsobem, ale s největší pravděpodobností se jim to nikdy nepodařilo, a tak odhalení tajemství tohoto dopisu čekalo na účastníky naší soutěže.
Správná ospověď: nevyřešeno

Bohužel se ukázalo, že vyluštit předloženou třetí úlohu bylo příliš těžkým oříškem a nikomu ze soutěžících se jí vyřešit ve vyhlášeném termínu do 3.12. nepodařilo. **Tajemství obsahu dopisu tak zůstalo prozatím stále neodhaleno.**

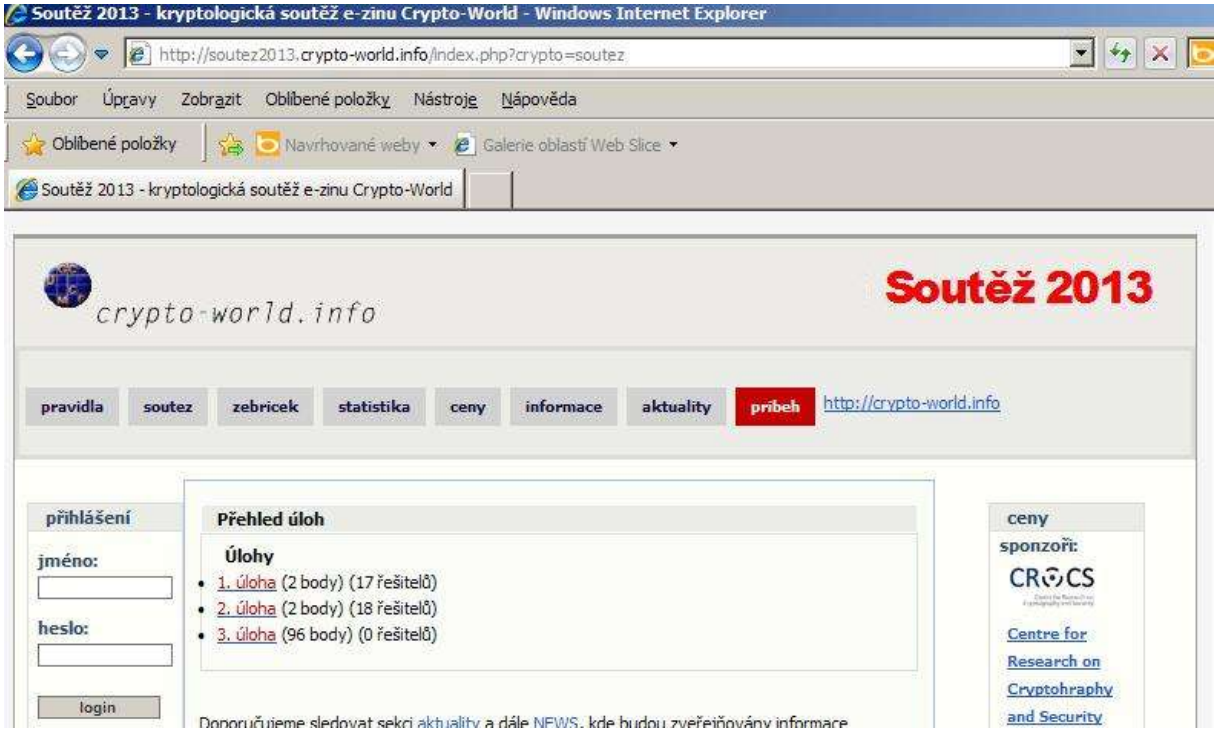
Vyhlašovatelé souteže proto oznámili, že připíší soutěžícím pomocné body na základě zaslaných analýz třetí úlohy. Provedené rozbory a své pokusy o vyluštění zaslali po tomto oznámení tři soutěžící.
Redkace jim na základě kvality těchto rozborů přidělila pomocné body.

Na základě tohoto vyhodnocení bylo stanoveno následující konečné pořadí letošní soutěže:

1	**jugin**	50	14.12 (06:27)
2	**MD5Mir**	6	14.12 (06:27)
3	**RABENHAUPT**	5	14.12 (06:27

4 - 17 místo obsadili soutežící kteří získali 4 body, jejich celkový přehled viz.:
http://soutez2013.crypto-world.info/index.php?crypto=zebricek

Celkový vítěz letošní soutěže, který byl přihlášen pod pseudonymem **jugin**, získal tablet GOCLEVER TAB R76.2 včetně pouzdra s klávesnicí, který věnoval hlavní sponzor soutěže firma DIGNITA, s.r.o.
S rozborem zašifrovaného dopisu, včetně některých velmi zajímavých a inspirativních pracovních hypotéz, který za podpory svého kolegy připravil a zaslal, se můžete seznámit v následujícím článku ***Analýza Rabenhauptovho zašifrovaného dopisu.***



Děkuji všem účastníkům soutěže, omlouvám se, za tak těžký úkol, ale doufám, že vám možnost odhalit tajemství obsahu dosud nedešifrovaného/nevyluštěného dopisu přinesla příjemné a vzrušující chvíle při jeho řešení.

D. Analýza Rabenhauptovho zašifrovaného dopisu

Eugen Antal & Pavol Zajac, ÚIM FEI, STU v Bratislave, (<meno.priezvisko>@stuba.sk)

(Výskum podporovaný grantom VEGA 1/0173/13 a APVV-0586-11)

V tomto príspevku sa zaoberáme lúštením šifrovaného dopisu Karla Rabenhaupta zo Suchej zverejnenej ako súťaž v časopise Crypto-World [1]. Jedná sa o korešpondenciu Karla Rabenhaupta s regentkou Hesensko-Kaselska Amáliou Alžbetou, v armáde ktorej Rabenhaupt slúžil ako dôstojník. Dopis je neurčito datovaný do obdobia jún alebo júl 1646. V čase vzniku Rabenhaupt vojensky operoval v oblasti Porýnia [1, 4]. V tomto čase prebiehala tzv. Hesenská vojna, ktorá bola súčasťou záverečnej fázy 30-ročnej vojny.

Obr. 1. Pôsobenie K. Rabenhaupta v roku 1646 (prevzaté z [3], upravené)

Šifru sa nám zatiaľ vylúštiť nepodarilo, ale v tomto príspevku by sme chceli prezentovať niektoré pozorovania, ktoré by mohli prispieť k ďalšiemu pokroku v oblasti lúštenia. Okrem autorov prispeli k pokroku v oblasti Z. Šedová, M. Sýs a mnohým ďalší kolegovia, ktorým ďakujeme za poskytnutú pomoc a zaujímavé nápady pri lúštení. Na celkové vylúštenie dopisu sa chceme pokúsiť využiť lúštenie softvérové, ku ktorému by sme ale potrebovali podrobný

slovník s historickým jazykom používaným dobovo, plus slovník potenciálne sa vyskytujúcich ťahákových slov (geografické názvy, mená a pod.)

Niekoľko poznámok k homofónnej šifre

V zadaní súťaže [1] bola zverejnená domnienka, že list bol šifrovaný homofónnou substitúciou pomocou typického dobového nomenklátora. Sumarizujme si typický princíp nomenklátorovej homofónnej šifry: Jednotlivé znaky otvoreného textu sa môžu šifrovať priamo jedným znakom (alebo skupinou znakov) viacerými spôsobmi (napr. "d" sa môže šifrovať ako "w", "26", alebo Θ). Tieto znaky označujeme ako *homofóny*. Navyše nomenklátory často obsahovali *klamače,* t.j. symboly alebo skupiny symbolov, ktoré nemali význam pre legitímneho čitateľa, ale mali za úlohu pomýliť lúštiteľa správy. Ďalším prvkom nomenklátorov sú substitúcie skupín znakov špecifikovanou skupinou symbolov (zväčša číselnou), napr. "de" sa šifruje ako "53". Tieto budeme označovať ako *bigramy*, aj keď vo všeobecnosti môže symbol šifrovať aj dlhšie skupiny hlások. Finálne, súčasťou nomenklátora môže byť kódová kniha, kde sa skupinou symbolov (*kód*) nahradí celé slovo alebo fráza, napr. "Cisár Svätej Ríše Rímskej Národa Nemeckého" bude jednoducho "KK".

V prípade správneho použitia homofónnej šifry lúštiteľ prakticky nemá šancu ju rozlúštiť. Správne navrhnutý nomenklátor by mal obsahovať toľko homofónnych variant jedného písmena, aby sa vyrovnala štatistika symbolov v zašifrovanom texte. Napr. ak "a" je dvakrát tak časté ako "m", tak "a" by malo byť šifrované dvakrát takým počtom homofónov ako "m". Navyše homofóny by mali byť vyberané náhodne. V tomto prípade potom v zašifrovanom texte dostaneme prakticky rovnomerné rozdelenie symbolov, ktoré pri dostatočnom počte homofónov ku dĺžke textu vedie na možnosť považovať za správu prakticky akýkoľvek text požadovanej dĺžky.

Pri používaní homofónnej šifry sa však často vyskytujú viaceré závažné chyby. V prípade známej Zodiacovej šifry [5] napr. pomohlo správu rozlúštiť nedostatočný počet homofónov a fakt, že homofóny neboli priraďované náhodne ale cyklicky [5, 6]. Príklad cyklického opakovania homofónov v Zodiacovej šifre *Z408* je znázornené na obrázku 3.

```
1 2 3 4 5 4 6 7 2 8 9 10 11 12 13 11 7 14 15 16 17 18
19 20 21 1 22 3 23 24 25 26 19 17 27 28 19 29 6 30 8 31
26 32 33 34 35 19 36 37 38 39 40 4 1 2 7 3 9 10 41 6 2
42 10 43 26 44 8 29 45 27 5 28 46 47 48 12 20 22 15 14
17 49 19 23 16 26 18 36 1 24 30 38 21 26 13 31 37 50 39
40 10 34 33 25 19 44 43 9 49 26 18 7 32 35 39 2 7 45 46
4 3 2 7 23 13 26 44 22 27 6 29 10 10 8 51 5 24 26 12 30
38 14 26 25 31 37 45 27 47 1 52 7 3 36 10 16 54 11 21
48 34 40 17 44 6 22 8 20 5 51 12 9 15 14 30 37 16 33 45
38 43 29 10 21 22 30 1 36 10 53 32 19 47 48 46 17 4 23
13 28 35 41 3 37 27 49 10 6 33 2 45 38 34 15 44 24 22
11 18 47 30 25 28 8 37 1 31 45 27 43 34 41 38 5 40 3 50
6 12 8 41 1 52 7 15 14 48 16 15 32 33 9 3 29 11 39 47
43 42 6 17 21 31 36 50 18 2 2 30 27 34 8 38 39 51 44 4
1 2 2 5 42 41 3 52 7 15 12 17 13 26 14 26 53 20 52 49
51 16 23 1 41 1 7 2 9 32 37 10 6 51 16 53 46 19 26 53
29 39 26 14 15 5 17 18 19 24 44 53 32 19 41 1 2 52 45
33 53 22 25 20 7 13 41 50 13 41 36 46 48 31 45 25 11 26
53 17 46 52 52 21 17 37 3 9 10 13 35 20 2 18 51 5 23 28
32 33 26 53 49 28 30 16 47 7 3 35 14 21 15 44 13 47 1
14 30 21 26 44 22 27 38 11 19 30 8
```

Obr. 3. Príklad cyklovej štruktúry šifry Z408 (prevzaté z [5])

Tieto cykly umožňujú identifikovať, ktoré homofóny predstavujú ten istý znak, čím odstránime "homofonizáciu" a priblížime sa ku klasickej substitučnej šifre. Ďalšou chybou je použitie rovnakého množstva homofónov pre každú hlásku. V tomto prípade si tabuľku homofónov môžeme predstaviť ako niekoľko riadkov abeced (viď. napr. obrázok 3, a nomenklátory 1,3 a 4 z [7]).

Obr. 3. Časť klúča pre homofónnu substitúciu (prevzaté z [7], nomenklátor č. 3, upravené)

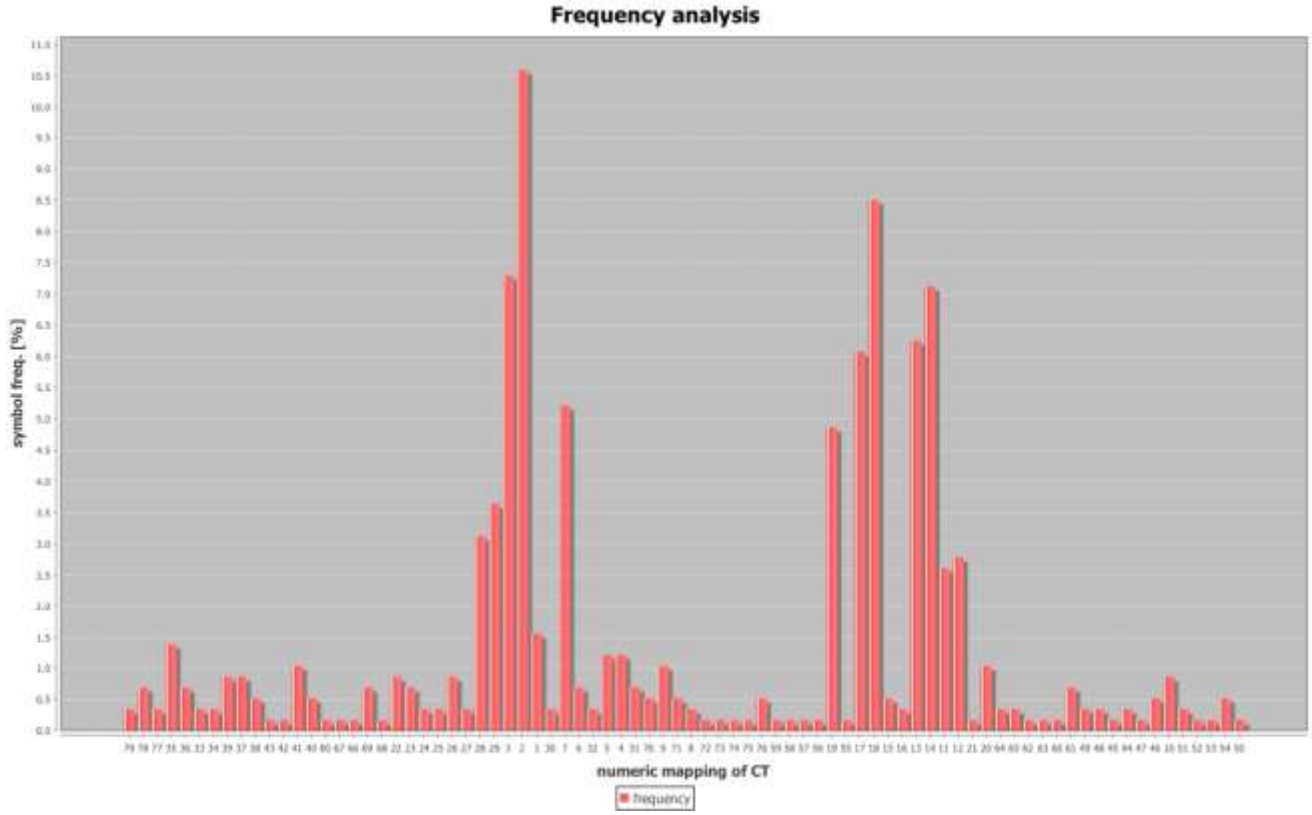
Štatistika otvoreného textu sa potom "kopíruje" do štatistík jednotlivých abeced. Pri dostatočne dlhom zašifrovanom texte nám tieto štatistiky umožňujú stotožniť niektoré najčastejšie homofóny (a dokonca stotožniť ich priamo so znakom otvoreného textu).

Pri lúštení homofónnej šifry sa snažíme jednak o stotožnenie homofónov navzájom, a jednak o ich stotožnenie s príslušným znakom otvorenej abecedy podobne ako pri obyčajnej substitúcii. Na základe štatistickej analýzy sa snažíme priradiť najčastejšie písmená alebo skupiny písmen. S výhodou sa dajú využiť špeciálne vzory ("abab"), alebo potenciálne otvorené slová a frázy, ktoré sa dajú v texte uhádnuť.

Pri ručnom aj počítačovom lúštení je dôležité mať kvalitný slovník, ktorý podrobne popisuje jazyk otvoreného textu, vrátane jeho štatistických vlastností a významných slov. Preto aj okolnosti vzniku dopisu a jeho potenciálny obsah je dôležitý pre kryptoanalytika z hľadiska prípravy slovníka. Pri použití nomenklátora je pravdepodobné, že niektoré dôležité slová/mená budú zašifrované kódovým slovom. V prípade dynamickej vojnovej situácie však pri príprave nomenklátora nemuseli byť k dispozícii napr. mená jednotlivých veliteľov, alebo všetky geografické údaje. Pre väčšiu šancu na vylúštenie dopisu by bolo dobré presne zmapovať pôsobenie a pohyby vojsk v čase a priestore, kde bol dopis napísaný.

Analýza individuálnych symbolov

V zašifrovanom texte sa nachádza **576** symbolov – **80** unikátnych. Z nich najčastejší je symbol "**.**", potom nasledujú číslice, a napokon ostatné symboly majú pomerne rovnomernú štatistiku a malý počet výskytov. Histogram symbolov okrem bodky (bodky predstavujú zhruba 30% textu) je znázornený na obrázku 4. Symboly sú kódované pomocou čísiel od 1 po 80. V prílohách je k dispozícii priame mapovanie na pôvodnom obrázku šifrovaného dopisu, ako aj mapovanie jednotlivých symbolov.



Obr. 4. Frekvencia symbolov zašifrovaného textu

Vzhľadom na uvedené štatistiky je oprávnená domnienka, že sa používal systém podobný ako v dopise Johanna Karla von Schönburg Maxmiliáno z Trauttmansdorffu [2] - (Obrázok 15). Bodka pravdepodobne slúži ako oddeľovač skupín číslic predstavujúcich jedno číslo kódujúce jeden údaj (homofón, klamač, bigram, kód). Zlúčením skupín číslic dostávame prepis, ktorý má už relatívne vyrovnané štatistiky:

Durchleuchtige, Hochgeborne Fürstin, Gnädige Frau
Dießen Morgen empfang ich Andtwortschreiben von 1 . 1 . N110 .
4 . 5 6 . N3 . 8 . 9 . 10 11 69 12 . N5 . N10 . 12 . N59 . 15 . N72 . N369 . N269 . 21 . 22 22 .
so gestern in 45 42 . 72 . 20 . N18 37 43 . N59 . N22 . N28 . N24 . N20 . N72 . N9 . N49
N21 . undt 80 . 36 35 . 11 4 N10 . 26 44 41 . N59 46 . N57 . N111 . N72 . N74 . N269 .
23 . 69 12 . N377 10 N3 71 . 69 12 . 5 N18 . 35 68 78 . N59 . 39 . N3 36 41 . 37 . 35 20 .
N18 . N49 N22 undt alß 1 . 1 . N90 4 N28 . N59 N21 47 N58 N14 . N376 .
9 . N66 . N90 N58 . N41 . 48 39 . 27 . N60 . N93 . N70 . 1 48 11 . N129 . N4 N59 .
N74 31 . N58 . N0 . N38 . 49 alß mache ich meine Rechnung
N396 . 12 . 34 . N10 . N5 50 . N4 11 . N70 . N24 . N5 35 . N42 . N115 . N100 . N72 N106
N129 . N3 36 15 . N939 . N6 . 11 44 63 79 79 . 26 N5 . 54 54 . N3 78 . N59 4 . 62
N10 51 51 . N10 . N5 . N12 . 23 . 22 22 . 40 N6 . N38 . N22 . 34 N57 31 . N24 . N18 . 26
N90 . N14 27 . 11 46 . undt negst Gottes Hülff 40 N6 . N59 . N22 . N369
9 . 39 . N11 5 N4 . N59 . N22 . 38 38 . 41 61 37 . 11 64 10 . N34 . N68 20 . 78 24 24
N11 . 39 . 38 . N123 . N107 . N138 . N83 . N21 N376 undt weil[e]n ich gute
Hoffnung habe, daß die alliirten in ihren Vortheil lenger
alß andere werden können stehen pleiben, undt vielleicht
was geshehen solle, Eh 10 11 73 22 . 1 1 . 54 41 . 11 6 36 8 . 23 . N100 .
N110 . N70 . N9 . N5 49 . N90 53 . 11 N5 . 12 N37 N115 . 31 . 20 . 4 N100 41 . N59 . 6 . N24
35 5 N6 64 40 19 . N369 . 9 . 12 12 . N277 . So hette Eu[uer]Fürst[lichen] Gn[aden]
underthenig zu bitten, die schleunige verordnung zu thuen
das 23 . N360 . 12 12 . 10 20 . 1 . 55 . N975 . 6 . 11 . 9 . 33 33 N90 . 74 . 11 N5
N100 . N60 . 4 75 . N59 76 . N58 . 65 56 5 N106 auch die . 41 11 46 5 35 19 .
N59 . 57 . N57 N1011 . 61 61 . N10 . N913 9 . 26 . 17 17 . N119 . 12 . 59 71 . N5 . 11 .
60 N58 65 N28 . N83 N129 . N20 . N24 . N18 . N12 N59 . N22 . 26 . 61 37 . 35 58 5
N6 . 66 . vielleicht möchte 69 12 . N93 . N70 39 5 N129 31 . N3 . 71 N20 . N77 .

37 . 35 N5 . 20 76 11 12 N77 . N93 . N238 . N120 . N57 . N74 . 12 76 N6 . N12 . 67
N42 . 78 N57 . 30 30 . 12 12 . 77 77 N5 . N57 . N106 32 . 32 . N103 4 . N129 15 . N18
N110 . N125 . N70 . N72 . N6 . N369 . 1 . 25 25 . N260 . Eu[uer] Fürst[lichen] Gn[aden]
hirmit [Gedelicher] Obhuet empfehlend verpleib

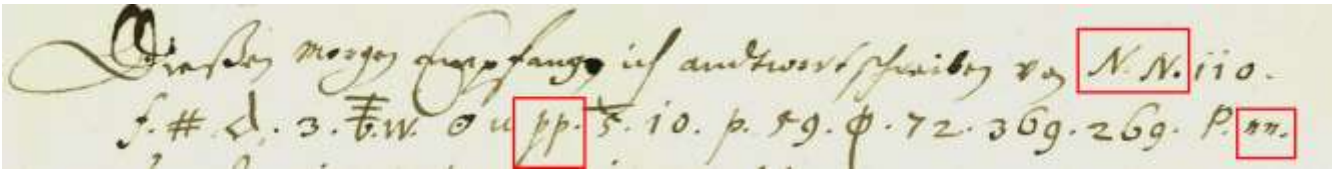
V ďalšom texte budeme súhrne označovať individuálne *znaky* (písmená latinskej abecedy v zašifrovanom texte), *glyfy* (iné individuálne znaky v zašifrovanom texte), *čísla* (skupiny číslic oddelené bodkami alebo zjavnými medzerami) ako *symboly*. Znaky a glyfy sú v prepise označené kódovým číslom podľa pôvodného mapovania, číselné symboly zo zašifrovaného textu sú kódované pomocou prefixu **N**, t.j. N129 znamená postupnosť číslic 129 v pôvodnom dopise.

Najpočetnejšie glyfy, čísla a písmená sú uvedené v nasledujúcej tabuľke:

Číslo	**Počet**	**Písmeno**	**Počet**	**Glyf (mapovanie)**	**Počet**
N59	13	*p*	16	*5*	7
N5	8	*u*	15	*20*	6
N6	7	*N*	9	*41*	6
N57	7	*E*	8	*10*	5

V prílohách je k dispozícii kompletná tabuľka početnosti symbolov (rozdelené na glyfy, čísla a písmená) zašifrovanej ako aj početnosti znakov nešifrovanej časti dopisu.

Niektoré symboly sa vyskytujú v pároch (viď. obr. 5). Vzhľadom na špecifickú polohu prvého páru (v preklade dopis začína zhruba vetou: "*Toto ráno som prijal [písomnú] odpoveď od ...*") máme hypotézu, že tieto dvojice sú označením osôb, resp. iné kódy.



Obr. 5. Začiatok šifrovaného dopisu (prevzaté z [1], upravené)

V [8] je uvedené, že Rabenhaupt velil Hesenským vojakom v oblasti Rýna na základe spojenectva Amálie Alžbety s Wolfgangom Wilhelmom z Pfalz-Neuburgu. Preto by "N.N." mohli označovať iniciálky (W.W.) práve Wolfganga Wilhelma. Tieto isté "iniciálky" sa nachádzajú v texte ešte dvakrát a na oboch miestach sú v kontexte otvoreného textu opäť na vhodnej pozícii, aby predstavovali osobu.

Odhad metódy šifrovania

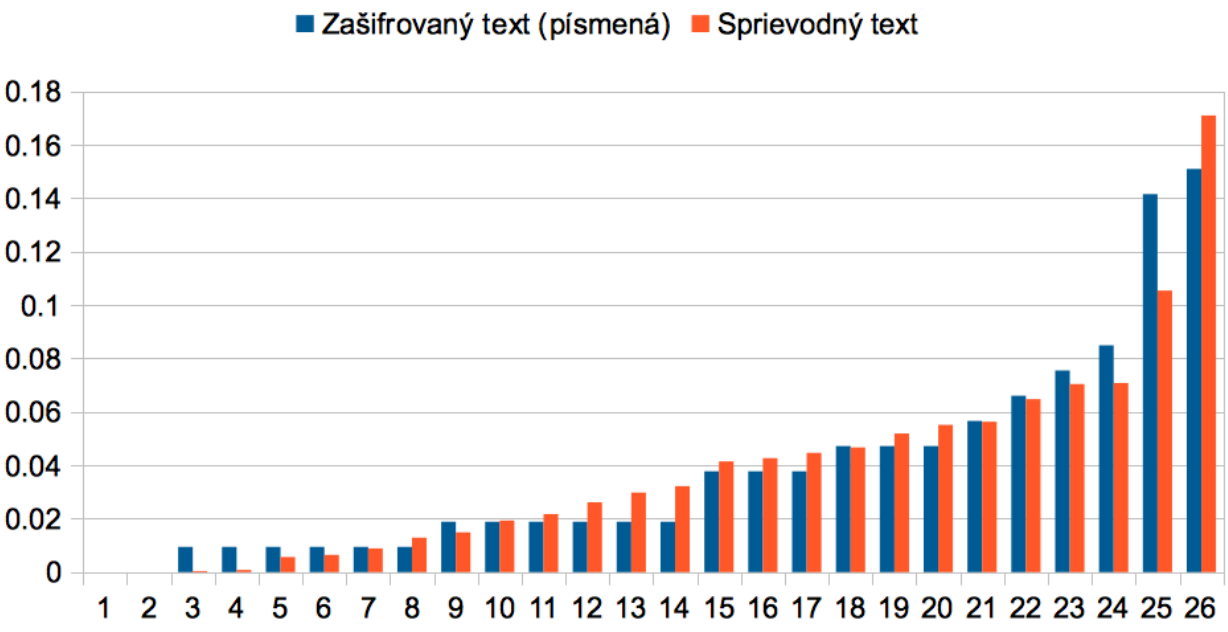
Vzhľadom na veľký počet individuálnych symbolov sa zdá byť pomerne vierohodná hypotéza, že sa používal komplexný nomenklátor s potenciálnou homofónnou časťou, možnosťou šifrovania bigramov aj s kódovou časťou a prípadnými klamačmi. Homofonizácia však nie je úplne dokonalá vzhľadom na veľký počet výskytov niektorých znakov.

Ako prvú pracovnú hypotézu sme si zvolili nomenklátor obsahujúci skupiny bigramov v tvare (spoluhláska, samohláska), t.j. "da", "de", "di", "do", "du" šifrované číslami. Počet čísel v zašifrovanom texte zhruba kopíruje počet očakávaných dvojíc. V príkladoch nomenklátorov boli často čísla prideľované v skupinách zaradom (napr. 25, 26, 27, 28, 29). Pri analýze štatistík však táto hypotéza nevyhovuje, lebo nie je možné rozdeliť čísla vyskytujúce sa v zašifrovanom texte na vhodné pätice tak, aby vznikli súvislé úseky a všetky čísla boli pokryté. Navyše, niektoré čísla majú extrémne vysoké počty výskytov vzhľadom na typické štatistiky bigramov otvoreného textu. Pravdepodobnejšia je preto možnosť, že časť čísel šifruje aj homofóny, a iba niektoré sú bigramy, alebo kódy.

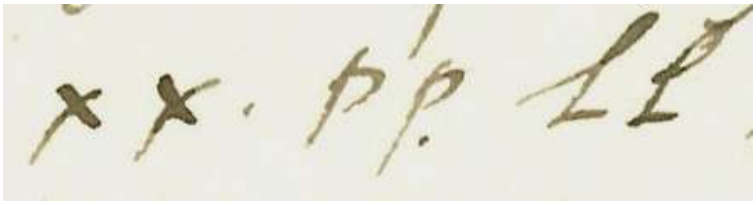
Vzhľadom na nerovnomerné štatistiky predpokladajme ďalej, že sa používa homofónna substitúcia s nesprávnou konštrukciou tabuľky. T.j. každému znaku otvoreného textu zodpovedá presne rovnaký počet homofónov bez ohľadu na jeho frekvenciu v otvorenom texte.

Vytvorili sme si štatistiky otvoreného textu na základe nezašifrovanej časti listu a listu sprievodného. Jedným z dôležitých charakteristík využívaných pri analýze zašifrovaných textov je tzv. index koincidencie (IC). Jedná sa o štatistiku vyjadrujúcu pravdepodobnosť, že pri náhodne zvolených textoch sa nám zhodnú znaky na tom istom mieste medzi dvoma textami. Pri náhodnom texte s 26-znakovou abecedou je táto pravdepodobnosť blízka 3,7 %. Naopak, pre reálny jazyk je táto pravdepodobnosť výrazne vyššia. Pre otvorený text Rabenhauptových dopisov je táto hodnota až 7,5 %. Je zrejmé, že substitučná šifra zachová IC, keďže sa zachovajú pravdepodobnosti výskytu jednotlivých znakov. Podobne, ak si správne zvolíme skupinu znakov z jedného riadku tabuľky homofónov, a máme dostatočný počet znakov zašifrovaného textu, dostaneme IC blízky IC otvoreného textu. Naopak, ak zvolíme nesprávnu skupinu (napr. symboly použité ako bigramy), IC bude pravdepodobne značne odlišný (nižší).

Po malom experimentovaní môžeme zistiť, že písmená v zašifrovanom texte majú podobnú štatistiku (IC, rozdelenie frekvencií) ako písmená otvoreného textu zodpovedajúce substitučnej šifre (viď. obr. 6). Teda pravdepodobne jeden riadok tabuľky homofónov predstavujú písmená. Niektoré nezhody štatistík môžu byť spôsobené aj zdvojením niektorých znakov (už spomenuté "NN", extrémny príklad je na obrázku 7).

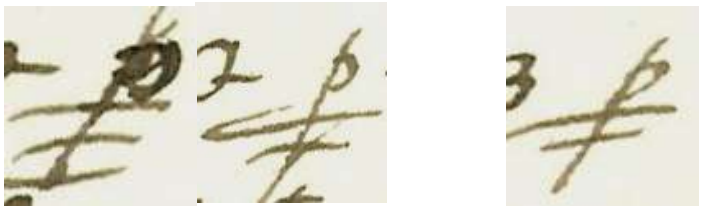


Obr. 6. Frekvencia výskytov písmen v sprievodnom dopise a zašifrovanej časti Rabenhauptovho listu (iba v rámci skupiny písmen)



Obr. 7. Zdvojenie písmen

Glyfov je v zašifrovanom počte väčšie množstvo, až 46. IC prvých 26 symbolov je značne odlišný od IC otvoreného textu (iba 3.4 %). Ich počet je však blízky hodnote 2*26 mínus málo časté znaky. Alternatívna hypotéza je, že glyfy predstavujú dva riadky tabuľky homofónov. Hypotézu otestujeme tak, že rozdelíme glyfy podľa početnosti "na preskáčku" do dvoch skupín. T.j. do prvej skupiny dáme najčastejší glyf, do druhej skupiny druhý najčastejší, do prvej skupiny tretí najčastejší atď. Jednotlivé skupiny majú IC mierne vyššie (cez 4 %), ale stále je značný rozdiel v štatistike týchto skupín a štatistike OT. Ak vynecháme zo štatistiky glyfy iba s jedným výskytom štatistika sa vylepší. Problém je, že niektoré glyfy majú možno špeciálny význam (rôzne podčiarkované glyfy podobné "p" a "q" – viď. obr. 8), alebo predstavujú klamače. Pravdepodobná je teda hypotéza, že iba vybrané glyfy môžu tvoriť ďalší riadok homofónnej tabuľky, ale aj klamače; prípadne, že niektoré glyfy predstavujú ten istý znak, ale bol pri prepise identifikovaný ako odlišný glyf. Trochu odvážna, aj keď ničím nepodložená hypotéza je, že rôzne varianty podčiarknutého "p" a "q" kódujú číselné údaje napr. "100" vojakov.



Obr. 8. Podčiarkované podobné glyfy

Podobne môžeme analyzovať skupiny čísel. Prvých 26 najčastejších čísel má index koincidencie 3,8 %, čiže príliš málo na to, aby predstavovali riadok tabuľky homofónov. Podobne, pri rozdelení čísel na dvojice dostaneme indexy koincidencie len okolo 4 %, čiže hypotéza dvoch riadkov homofónov, ktoré sú číslami je nepravdepodobná. Čo je však zaujímavé: ak zoberieme prvých 26 čísel numericky (1-26), tak IC ich rozdelenia je zhruba 7%, čo zodpovedá štatistike korpusu. Je teda značne pravdepodobné, že jeden riadok tabuľky homofónov tvoria práve čísla (prvé v poradí). Odlišnosti v štatistike a odlišnosti v histogramoch nás vedú k hypotéze, že riadok s číslami je posledný riadok tabuľky homofónov, a že homofóny sa preferenčne vyberali zhora (t.j. ak sa znak vyskytne len raz, tak na číslený prepis nedôjde). To vedie tiež k možnej hypotéze, že sa používal cyklický výber homofónov.

Niektoré zaujímavé štatistiky šifrovaného dopisu

Po analýze čísiel (číselných symbolov) šifrovaného dopisu je možné nájsť niekoľko zaujímavých pozorovaní:

- Najpočetnejšie číslo "N59" sa nachádza 4x v spojení s (tiež početným) číslom "N22", čo znamená 2/3 výskytu čísla "N22".
- Číslo "N90" sa nachádza v spojení so zdvojenými symbolmi s kódmi "1" a "33" (Otázka je, či môže byť význam "1 1" totožný s významom "33 33" ?).
- Podobne ako v predošlom prípade číslo "N10" sa nachádza v spojení so zdvojenými kódmi "51 51" a "61 61" ("51" = "61" ?), alternatívne "plukovník 51" a "plukovník 61".
- Vzor "N59" "symbol" "N57" sa nachádza s mapovaním "57" a "46" (Otázka je, či môže byť význam mapovania "46" totožný s významom mapovania "57", alebo či je možné použiť tento vzor pri hladaní možných slov?).
- Šifrovaný dopis obsahuje dlhšie číselné úseky ("*N110.N125.N70.N72.N6.N369*", "N59.*N22.N28.N24.N20.N72.N9.N49", "N57.N111.N72.N74.N269"* ...)

Ďalšou zaujímavosťou šifrovaného dopisu je cyklickosť niektorých symbolov. Pomocou aplikácie z [5] sme otestovali:

- Cyklické opakovanie číselných symbolov, kde možnú skupinu homofónov môžu tvoriť skupiny (vo formáte ["skupina"] – "postupnosť v dopise"):
  - [N20, N12] - N20, N12, N20, N12, N20, N12
  - [N90, N100] - N90, N90, N100, N90, N100, N90, N100, N90, N100
  - [N3, N18] - N3, N18, N3, N18, N3, N18, N3, N3, N18, N18, N3, N18
  - [N70, N129] - N70, N129, N70, N129, N70, N129, N70, N129, N129, N70 , v prípade, že do skupiny pridáme číslo N106, sa cyklickosť ešte "zachová", ale už nie je taká pravidelná ako v predošlom prípade.
  - [N28, N21, N74] - N28, N21, N74, N28, N21, N74, N21, N28, N74
- Cyklické opakovanie nečíselných symbolov (vo formáte ["skupina"] – "postupnosť v dopise"):
  - [10, 20] - 10, 20, 10, 20, 10, 20, 10, 20, 10, 20, 20
  - [69, 71] - 69, 69, 71, 69, 71, 69, 71
  - [26, 78, 31] - 26, 78, 31, 26, 78, 31, 26, 78, 31, 26, 26, 31, 78
  - [5, 37] - 5, 37, 5, 37, 5, 37, 5, 5, 5, 37, 5, 37

Pomocou spomenutej aplikácie sme ešte dostali "ďalších kandidátov skupín", v ktorých je možné nájsť cyklickosť, ale s väčším počtom chýb: [20,41,78], [4, 36], [39, 37, 78], [20, 41, 78] a [N6, N57].

Sumarizácia

Je pravdepodobné, že písmená a prvých 26 čísel predstavujú v zašifrovanom texte homofóny (s preferenciou písmen). Navyše tieto homofóny kopírujú štatistické rozdelenie otvoreného textu. Je možné, že tabuľka homofónov obsahuje aj niektoré glyfy, ale nie je možné ich identifikovať štatisticky. Ostatné čísla a glyfy budú pravdepodobne klamače, bigramy a kódové slová. Pri lúštení preto treba vychádzať z písmen a prvých 26 čísel a snažiť sa využiť štatistiky a vhodné slová v úsekoch identifikovaných homofónov.

Niektoré zaujímavé hypotézy:

- Duplikáty majú špeciálny význam, keďže sa vyskytujú príliš často
- Glyfy "podčiarknuté p,q" majú špeciálny význam
- Vzhľadom na špeciálny význam písmena "p" v zašifrovanom texte je možné predpokladať, že najčastejšie nemecké písmeno "e" je šifrované písmenom "u" (mapované kódovým označením 11)
- Ďalšia hypotéza je, že písmeno "n" je homofónne šifrované na číslo "N5", a tiež, že "N57"-"N59" by mohli označovať bigramy s "n" na začiatku ("na", "ne", "ni", "nu"). Tomu nasvedčujú aj rozumné vzdialenosti medzi jednotlivými výskytmi predpokladaného písmena "n" v otvorenom texte.

Cyklovú štruktúru by bolo treba preskúmať podrobnejšie, kedže sa v zašifrovanom texte objavujú často cykly, kde jednotlivé symboly majú takmer rovnaký počet výskytov.

Literatúra

1. Jakub MÍRKA: Dosud nevyluštěný dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché z doby třicetileté války. CryptoWorld 7-8, 2013.

2. Jakub MÍRKA: Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni, část I.-III. Crypto-World 11-12/2012, 1-2/2013, 3-4/2013.

3. Prispievatelia Wikipédie: Blaeu 1645 - Iuliacensis et Montensis Ducatus, [online]. Wikipedia, 2007. [cit: 2013-12-07]. Dostupné na internete: http://commons.wikimedia.org/wiki/File:Blaeu_1645_-_Iuliacensis_et_Montensis_Ducatus.jpg .

4. Jakub MÍRKA: Opis nešifrovaného dopisu Karla Rabenhaupta ze Suché zaslaného lantkraběnce Amálii Alžbětě 13. července 1646 . , [online]. Crypto-World , 2013. [cit: 2013-12-07] Dostupné na internete: ‹ http://soutez2013.crypto-world.info/dopisy/obr2.jpg ›.

5. Eugen ANTAL, Juraj VARGA: Zodiac. Mikulášská kryptobesídka 2010 : Sborník příspěvků. Praha, 2.-3.12.2010. Praha: Trusted Network Solutions, 2010, s. 89--90. ISBN 978-80-904257-1-2.

6. John C. KING, Dennis R. BAHLER: An Algorithmic Solution of Sequential Homophonic Ciphers, Cryptologia, 1993, 17:2, 148-165

7. Jakub MÍRKA : Ukázky nomenklátorů [online]. Crypto-World , 2013. [cit: 2013-12-07] Dostupné na internete: ‹ http://soutez2013.crypto-world.info/pribeh/napoveda.pdf >

8. Bernd WARLICH: Rabenhaupt, Karl Freiherr Rabenhaupt von Sucha, [online]. 2012. [cit: 2013-12-08] Dostupné na internete: ‹ http://www.30jaehrigerkrieg.de/rabenhaupt-karl-freiherr-rabenhaupt-von-sucha-3/ >

E. PF 2013

Všem našim čtenářům přeji do roku 2014 pevné zdraví, klid na zajímavou práci, štěstí a úspěch v profesním a osobním životě.

Za redakci e-zinu Crypto-World, za spolupracovníky a za kryptologickou sekci Jednoty českých matematiků a fyziků

Pavel Vondruška

A na závěr roku drobná úloha pro ty, kteří si chtějí během svátků vyřešit jednu homofonní šifru:

16.36.78.64.13 52.9.21.22.80.44.17 49.75.9.50.41.31 9 52.72.82 21.36.17.19.59.69.72.86 75 48.22.11.59 22.00.11.44 23.25.14.63.82 11.27.59.67.9.25.74.43 57.25.31.23.27.68 - 52.45.25.19.12.28 23.9.52.13.88 75.22.21.12.94.28.26.18.9.

„Drobná“ nápověda pro výběr vhodného nomenklátoru ☺ (1646)

F. O čem jsme psali za posledních 12 měsíců

Kompletní obsah všech vyšlých čísel od roku 1999 je dostupný zde
http://crypto-world.info/index2.php?vyber=obsah

Crypto-World 5-6/2012

A.	HERMANN POKORNY - "zaslúžilý umelec" v lúštiteľskom odbore vo víre I. svetovej vojny (J.Krajčovič)	2 - 8
B.	Najstaršia zašifrovaná písomná pamiatka v Čechách (J.Krajčovič)	9 – 10
C.	Nízkoriziková kryptografie (V.Klíma)	11 - 13
D.	Společná novela zákona o elektronickém podpisu (účinná od 1.7.2012) (P.Vondruška)	14 – 18
E.	Call for Papers - Mikulášská kryptobesídka 2012	19
F.	O čem jsme psali v květnu a v červnu 2000 – 2011	20 – 24
G.	Závěrečné informace	25

Crypto-World 9-10/2012

A.	Pointerová šifra a nízkoriziková náhrada AES (V.Klíma)	2 – 8
B.	Kryptografické zabezpečení prodeje lihovin (R.Palovský)	9 – 13
C.	Kryptologické perličky 2 (K.Šklíba)	14 – 20
D.	Záhada kodexu Rohonczi Codex (E. Antal)	21 – 28
E.	Kaspersky Lab uvádí Kaspersky Internet Security 2013	29 - 31
F.	O čem jsme psali v září a říjnu 1999 – 2011	32 – 35
G.	Závěrečné informace	36

Příloha: neoglyfy.pdf , ukázka ze sešitu Batěk A. S.: Neoglyfy I., str. 4 – str. 13
(http://crypto-world.info/casop14/neoglyfy.pdf)

Crypto-World 11-12/2012

A.	SHA-3 a lehká kryptografie (V.Klíma)	2 – 11
B.	Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni , část I. (J.Mírka)	12 – 28
C.	Tip na vánoční dárek - Enigma - bitva o kód (P.Vondruška)	29 – 30
D.	Pracovní příležitost (World Startup Project)	31
E.	O čem jsme psali v listopadu a prosinci 1999 – 2011	32 – 35
F.	Závěrečné informace	36

Příloha: Obrazová příloha k článku B (Mírka, J.) http://crypto-world.info/casop14/cast1.zip

Crypto-World 1-2/2013

A.	Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni, část II. (J.Mírka)	2 -12
B.	Lúštitelia historických šifier - A.V. Maloch a Josef Šusta (J. Krajčovič)	13 - 21
C.	Elektronický podpis v praxi (P.Vondruška, J.Peterka)	22
D.	SOOM.cz - Hacking & Security konference #2 (R.Kümmel)	23
E.	Security and Protection of Information 2013	24 – 25
F.	O čem jsme psali za posledních 12 měsíců	26 - 27
G.	Závěrečné informace	28

Příloha: Obrazová příloha k části II. Mírka, J.: Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni
http://crypto-world.info/casop15/obr2.zip

Crypto-World 3-4/2013

A. Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni, část III. (J.Mírka) 2 -14
B. Andreas Figl – rakúsky dôstojník a kryptológ (J.Kollár) 15 - 23
C. Central European Conference on Cryptology 2013 24
D. call for papers - CYBERSPACE 2013 25 - 26
E. O čem jsme psali za posledních 12 měsíců 27 - 28
F. Závěrečné informace 29

Příloha: Obrazová příloha k části III. Mírka, J.: Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni
http://crypto-world.info/casop15/obr3.zip

Crypto-World 5-6/2013

A. Konec aktualit v Crypto-News a Bezpečnostních střípků (J.Pinkava) 2
B. Tajomstvo šifrovacieho stroja G. W. Leibniza (J.Krajčovič) 3 – 11
C. Kaspersky Lab odhalila novou kyberšpionážní operaci NetTraveler 12
D. Reakcia na článok „Andreas Figl – rakúsky dôstojník a kryptológ“ (J.Krajčovič) 13 – 15
E. Cvičný CISSP test z kryptografie 16 – 18
F. Central European Conference on Cryptology 2013 26.-28. června, Telč 19 – 20
G. Call for Papers Mikulášská kryptobesídka 21
H. O čem jsme psali za posledních 12 měsíců 22
I. Závěrečné informace 23

Crypto-World 7-8/2013

A. Reino Häyhänen – sovietsky špión (J. Kollár) 2 – 9
B. Dosud nevyluštěný dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché z doby třicetileté války. (Soutěž o ceny) (J. Mírka) 10 – 18
C. Soutěž 2013, luštění originálního šifrového dopisu ze 17. století (P.Vondruška) 19 – 21
D. Diskrétní logaritmus a metody jeho výpočtu (J. Pulec) 22 – 26
E. Kaspersky v Praze - Kybernetické zbraně jsou nejhorším vynálezem století 27 – 28
F. Pozvánka k podzimním kurzům Akademie CZ NIC 29 – 31
G. O čem jsme psali za posledních 12 měsíců 32 – 33
H. Závěrečné informace 34

Crypto-World 9-10/2013

A. Sovietska šifra VIC (J.Kollár) 2 – 16
B. Prolamování hash otisků (R.Kümmel) 17 – 24
C. Upoutávka na knihu K.Burdy – Aplikovaná kryptografie 25
D. Soutěž v luštění / Dosud nevyluštěný dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché z doby třicetileté války (J.Mírka, P.Vondruška) 26 – 27
E. O čem jsme psali za posledních 12 měsíců 28 – 29
F. Závěrečné informace 29

Příloha: ukázka z knihy Aplikovaná kryptografie
http://crypto-world.info/casop15/Burda_akryptografie.pdf

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
	Jozef Martin Kollar
	Vlastimil Klíma
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
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/
Jozef Martin Kollar	jmkollar@math.sk ,	
Jozef Krajčovič	kryptosvet@gmail.com ,	http://katkryptolog.blogspot.sk
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška, jr.	pavel@crypto-world.info ,	http://www.pavelvondruska.cz/