Crypto-World

Informační sešit GCUCMP
ISSN 1801-2140

Ročník 15, číslo 5-6/2013 **15. červen**

5-6/2013

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1315 registrovaných odběratelů)

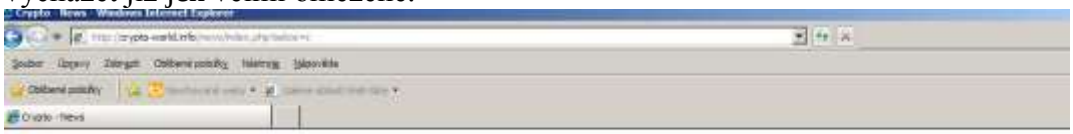
Obsah : str.

A. Konec aktualit v Crypto-News a Bezpečnostních střípků

Jaroslav Pinkava, Crypto-World, jaroslav.pinkava@gmail.com

Dne 22. dubna 2013 vyšlo poslední pokračování Bezpečnostních střípků (dále BS). Ze zdravotních důvodů nemohu v této práci pokračovat.

Děkuji všem čtenářům, a také tvůrcům webu Crypto-World, kde v rámci Crypto-News se objevovaly v sekci NEWS průběžně prakticky denně nové zprávy, a redakci Rootu, která umožnila vydávání jejich přehledu v podobě BS. Nyní budou denní zprávy na Crypto – News vycházet již jen velmi omezeně.



Za dobu téměř osmi let, v průběhu kterých BS vycházely, se objevilo zhruba 400 jejich pokračování (včetně dvou let, kdy vycházely na Intervalu pod názvem Svět bezpečnosti) a na webu Crypto-World bylo v sekci Crypto-News publikováno více než 22 500 zpráv. Podle těchto aktuálních informací zveřejněných na webu se následně v článcích BS objevovala celá řada okruhů problematik, ve stručnosti to byly následující okruhy: přehledy, konference, obecná a firemní bezpečnost, legislativa, politika, sociální sítě, software, malware, špionážní malware, viry, hackeři a jiní útočníci, Anonymous, hardware, bezdrát, VoIP, RFID, mobilní zařízení, mobilní malware, spam, forenzní analýza, elektronické bankovnictví, autentizace, hesla, ID, phishing, elektronický podpis, biometrie, normy a normativní dokumenty, kryptografie a různé.

Práce na vyhledávání zpráv nebylo málo, také každodenní péče o novinky na Crypto-News zabrala nemálo času. Ta činnost mě ale bavila a věřím, že čtenářům přinášela užitečné informace.

Jaroslav Pinkava

Za sekci kryptografie a redakci Crypto-Worldu si dovoluji touto cestou našemu kolegovi a jednomu ze zakladatelů a dlohodobému přispěvateli Jardovi Pinkavovi poděkovat za ty stovky hodin, které pro e-zin a hlavně pro sekci News věnoval.

Děkuji Jardo a pevné zdraví!

Pavel Vondruška

B. Tajomstvo šifrovacieho stroja G. W. Leibniza

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

Motto:
Cryptolysis, ars solvendi aenigmata cryptographica, est summun specimen humanae penetrabililatis. [“Kryptológia, ako umenie lúštenia kryptografických záhad, je najvyššou ukážkou ľudského umu."]

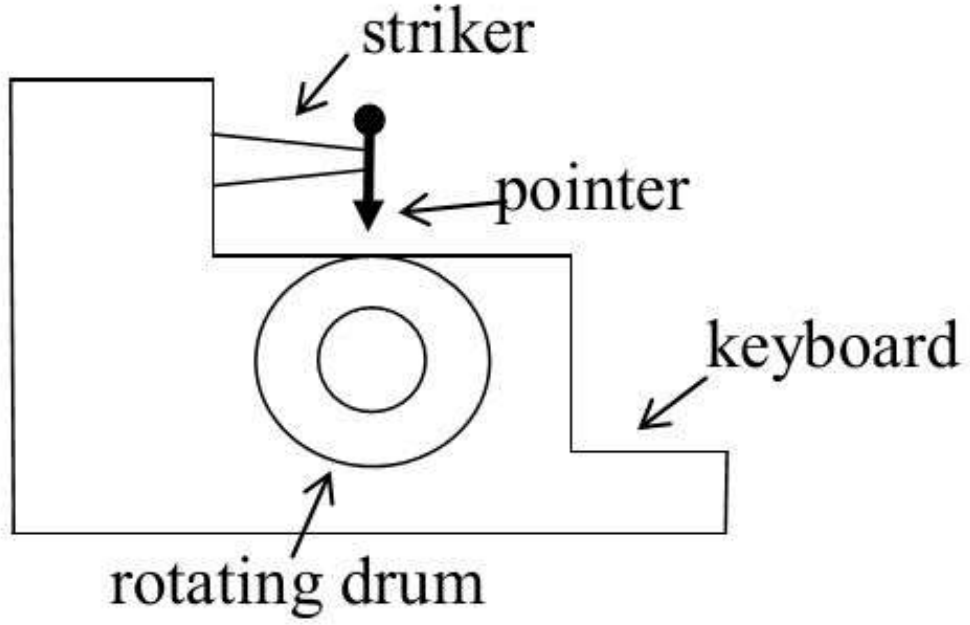
Popredný filozof, matematik a najväčší polyhistor svojej doby G. W. Leibniz kryptoanalytikovi Johnovi Wallisovi, r. 1698

Ak si prelistujete akúkoľvek knižku, v ktorej sa píše o matematických termínoch a symboloch, zistíte, že medzi najčastejšie sa vyskytujúcimi tvorcami pojmov a znakov patrí meno G. W. Leibniz. Tento mimoriadne nadaný všestranný učenec zaviedol napr. symboly pre delenie ":", násobenie ".", diferenciál dx, integrál ∫ a celý rad ďalších. Prednedávnom (nález poznámok síce už v r. 2001, avšak vo forme prezentácie až v priebehu rokov 2010 až 2012) bolo v jeho súbornom diele, ktoré obsahuje 90 objemných zväzkov, pričom vydaných tlačou bolo zatiaľ "len" 50, nájdené pozoruhodné výsledky, ktoré prinášajú ďalší kamienok do mozaiky poznatkov o ranomoderných šifrovacích metódach.

Obr. 1: Gottfried Wilhelm Leibniz (1646-1716)

Presnejšie v Leibnizových zápiskoch a poznámkach (nachádzajúcich sa v 40. zväzku a 4. sérii súborného diela), zo 70. rokov 17. storočia. Schémy a popis neznámeho šifrovacieho stroja našiel Nicholas Rescher, mimoriadny profesor histórie vedy na Univerzite v Pittsburgu a popredný odborník na život a dielo tohto všestranného génia a ktorý je autorom,

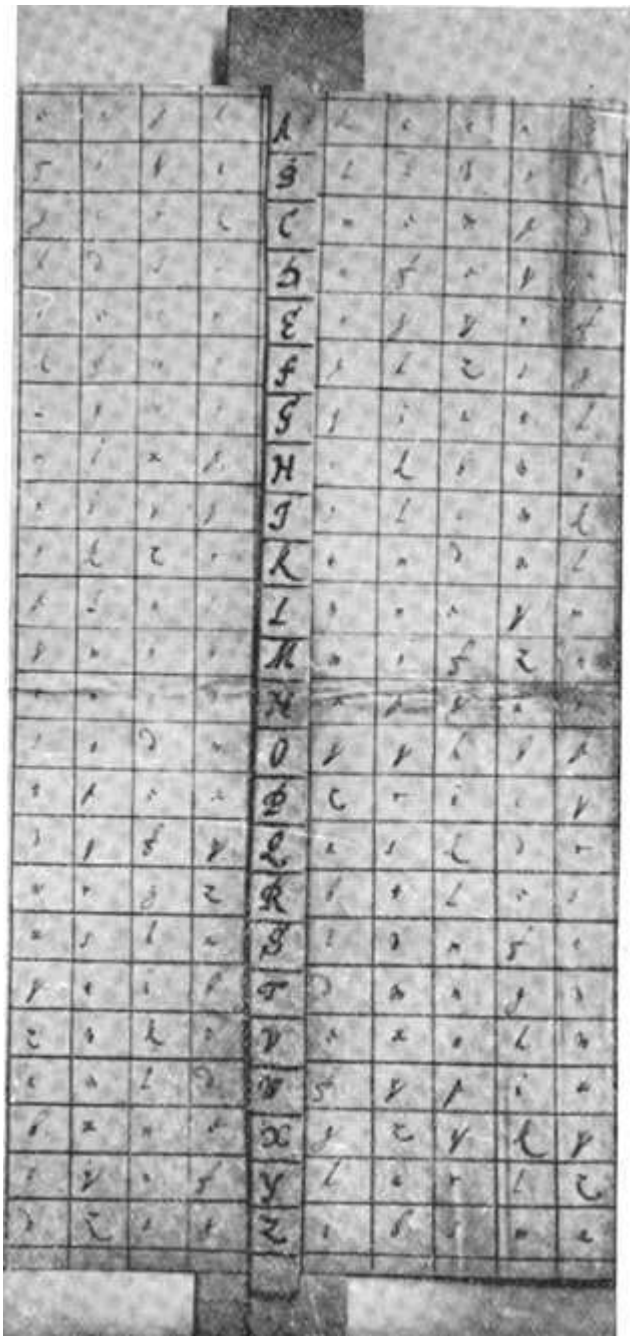
spoluautorom resp. vydavateľom viac než 100 kníh z oblasti filozofie a histórie vedy. Leibniz prišiel so svojimi návrhmi na zostrojenie tohto stroja za vojvodom v Hannoveri v r. 1679 a neskôr v r. 1688 ho ponúkol ríšsko-nemeckému cisárovi Leopoldovi I., ktorý ho však sucho odbil. Podľa prof. Reschera dôvodom jeho chladného odmietnutia bolo, že monarcha a jeho dvorania " *prechovávali až prílišnú a samozrejme neoprávnenú dôveru v bezpečnosť svojich šifrovacích metód*". Výsledkom bolo, že Leibniz svoje memorandum nikdy nepublikoval a tak šifrovací stroj zostal len „na papieri". Anglický kráľ Juraj I., po tom čo sa na začiatku 18. storočia dozvedel o úmysloch svojej ženy utiecť s Leibnizom nechal ju zavrieť do domáceho väzenia a nariadil aby boli všetky jeho spisy—ktorých bolo viac než 200,000—skonfiškované. Našťastie sa však zachovali aj vďaka ich neustálemu vydávaniu nemeckými historikmi. Samozrejme zostrojenie takého stroja si vyžadovalo úzku spoluprácu: s inžinierom Richardom Kotlerom, odborníkom na Leibnizove počítacie stroje Klausom Badurom a Wolfgangom Rottstedtedom, nemeckým strojníkom špecializujúcim sa na historické vynálezy. Jednou z jeho základných súčastí bol tzv. "**Staffelwalze**" – krokovací valec.



Obr. 2: Jednoduchá schéma Leibnizovho šifrovacieho stroja na princípe klavíra[10]

Je to jednoduchý ozubený mechanizmus, v ktorom sa valec otáča rovnomerne a pomocou krokovacích výstupkov prenáša nepravidelný pohyb na s ním spojené ozubené koliesko. Týmto sa tvoria meniace sa hodnoty posuvu v šifrovanom texte a čo samozrejme v konečnom dôsledku viac skomplikuje jeho rozlúštenie.

Samozrejme v tej dobe už existovali rôzne pomôcky vyrobené z pergamenu, tvrdého kartónu, sa šifrovalo systémom viacerých abecied rýchlejšie a ľahšie. Medzi také patril známy Albertiho šifrovací disk ako aj posuvné prúžky.

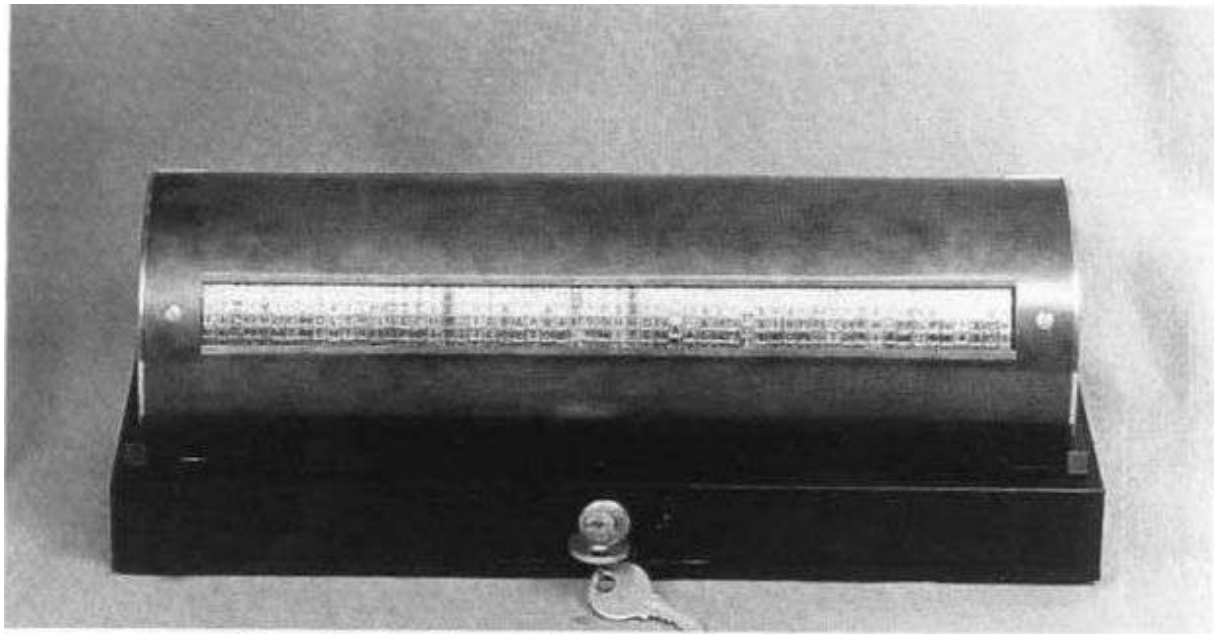


Obr. 3 Šifrovanie pomocou „posuvnej karty“, ktorá sa používala za čias neskoršieho panovania kráľovnej Alžbety I. (okolo r. 1600) [15]

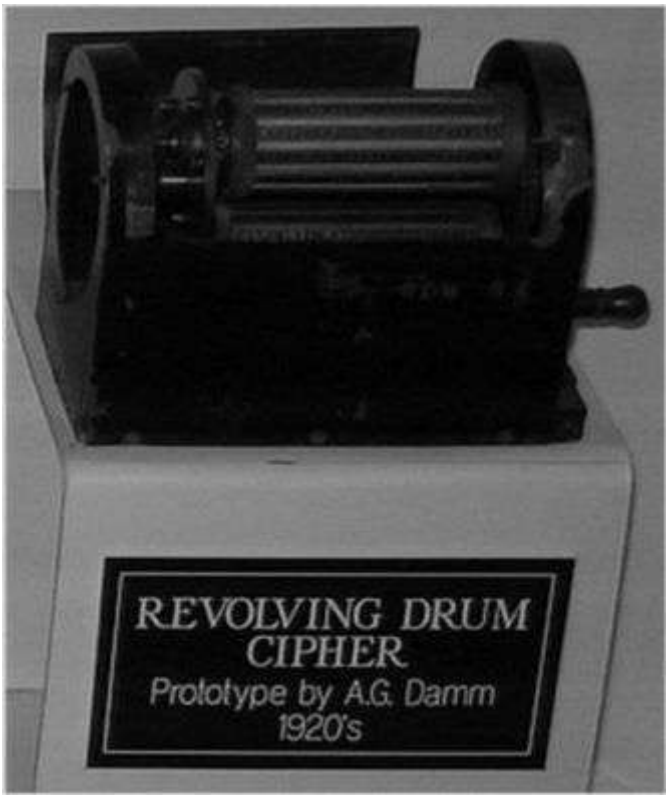
Použitie posuvných prúžkov z dreva uľahčujúcich polyalfabetické šifrovanie sa dá vysledovať už na dvore anglickej kráľovnej Alžbety I. (okolo r. 1600) alebo ho nájdeme graficky znázornené pod názvom **Ars steganographica** v pojednaní jezuitu Athanasia Kirchera ***Polygraphia nova et universalis ex Combinatica arte detecta*** (vydaného v Ríme kníhtlačiarom Varesiom v roku 1663). To nóvum, čo prinášala realizácia Leibnizovho stroja bol vlastne spôsob ako zmechanizovať tento postup.

Týmto ukazuje prechodovú fázu od kryptografickej pomôcky (ako napr. šifrovací disk) k mechanickému stroju. Rescherov objav tejto sučasti v Leibnizových spisoch a poznámkach sa

ukázal mimoriadne dôležitým vodítkom k úspešnej rekonštrukcii tohto na svoju dobu celkom zložitého mechanizmu. Doposiaľ sa za prvý šifrovací stroj považoval vynález starého otca švédskeho baróna Fredrika Gripenstiernu, Christofera Polhema, tzv. **Chiffre-Maskin**, skonštruovaný v druhej polovici 18. storočia, tiež objavený len pomerne nedávno (70.roky 20. storočia)[2].



Obr. 4: Rekonštrukcia Gripenstiernovho šifrovacieho stroja



Obr. 5: Dammov šifrovací stroj – „Otočný valec“

Ešte neskôr sa podobný kryptografický princíp objavil až v 20. rokoch 20. storočia v mechanicky mierne odlišnej konštrukcii šifrovacieho stroja vynálezcu A. G. Damma[4], na princípe otočného valca.

Život a dielo

Gottfried Wilhelm Leibniz sa narodil v rodine profesora etiky v Lipsku 1. júla 1646 a údajne bol slovanského pôvodu, keďže jeho predkovia vraj mali priezvisko Ľubenec. Po smrti otca (1652) študoval spisy z jeho knižnice. Naučil sa veľmi dobre po latinsky a grécky, ako desaťročný čítal antických klasikov a ako 13-ročný vytvoril denne 300 hexametrov. Po skončení štúdia na gymnáziu (1661) chodil na univerzite v Lipsku a Jene na prednášky práva, filozofie a matematiky. Stal sa magistrom filozofie a doktorom práv. Nezvolil si však život kabinetného vedca, dal sa do služieb práva a politiky. Päť rokov písal v Mohuči filozofické úvahy, pripravoval právne úpravy. V roku 1672 odišiel s diplomatickým poslaním do Paríža. Svoje prvé matematické dielo vypracoval v roku 1666 pod názvom ***Ars combinatoria*** - "*Kombinatorické umenie*". Z jeho myšlienky, že "*je nedôstojné pre nadaného človeka, aby ako otrok strácal hodiny života pri výpočtoch, ktoré by určite bolo možné zveriť ľubovoľnej osobe, pokiaľ by na to použila stroj*", vyplynula snaha skonštruovať lepší počítací stroj ako Pascalov z roku 1641. Leibniz zostavil stroj, ktorý nielen sčitoval, ale aj násobil a delil. Predviedol ho roku 1673 v Paríži. V Londýne mal s ním technické problémy, ale aj tak získal členstvo v Kráľovskej spoločnosti. Neskôr počítací stroj vylepšoval a dosiahol, že sa na ňom dalo umocňovať a hľadať druhú i tretiu odmocninu. Tak sa stal predchodcom počítačovej éry.

Zoznámenie sa s významnými vedcami - Huygensom, Boyleom, Mariottom, Newtonom - a štúdium prác Galileiho, Pascala, Fermata a Vieta (všimol si aj jeho úspechy pri lúštení tajnej korešpondencie katolíckej Ligy, [1, s.116-8]) ho orientovalo na prácu pre vedu, a malo veľký vplyv na duchovný rozvoj. Do vlasti sa vrátil až roku 1676. Tam vstúpil do služieb hannoverského vojvodu Johanna Friedricha von Braunschweig - Lunneburga ako dvorný radca a knihovník. Po jeho smrti sa však jeho postavenie badateľne zhoršilo. Nový vojvoda Ernst August nemal porozumenie pre Leibniznove plány a určil mu jednoznačne úlohu pracovať na genealógii rodu. V tejto súvislosti podnikol v rokoch 1687-1690 cestu do Viedne, Ríma a Neapola. Počas nej mu ponúkli miesto správcu knižnice vo Vatikáne, ale lákavú ponuku musel ako nekatolík odmietnuť.

Leibniz a kryptografia

Údaje o Leibnizových kontaktoch so šiframi a kódmi známe z kryptologickej literatúry sa doposiaľ obmedzovali na jednotlivé menšie poznámky v jeho listoch. Ako "osobnú" šifru používal v listoch adresovaných svojim vedeckým kolegom a rivalom jednoduchú zámenu s heslom šifrovej abecedy LABYRINTHUS.

```
OT: A B C D E F G H I L M N O P Q R S T U X Y Z
ŠT: l a b y r i n t h u s c d e f g h o p q x z
```

Obr. 4: Jednoduchá zámena s kľúčovým slovom LABYRINTHUS

V diplomatickej a právnej korešpondencii však používal zložitejšie šifrovanie typické pre vtedajšiu dobu – **nomenklátor.** Známa je taktiež jeho korešpondencia s významným matematikom prednewtonovskej éry - **Johnom Wallisom**[1, s.169], ktorý bol taktiež mimoriadne výnimočným lúštiteľom pre Cromwella ako aj neskôr pre anglickú korunu. Vyjadril v nej obavy z toho, aby umenie lúštiť, v ktorom Wallis preukázal neoceniteľné služby nielen Anglicku ale aj vďaka neúnavnému Leibnizovmu sprostredkovaniu hannoverskému vojvodstvu nezomrelo spolu so svojím majstrom. Preto navrhol poslať mu mladšieho učňa, ktorého by mohol zasvätiť do tohto záhadného umenia. V roku 1700 dokonca navrhol dvoch nádejných kandidátov G. C. Bauermeistera a C. L. Cibrovia. Keďže Wallis na neustále Leibnizovo naliehanie vždy poslal iba vylúštené listy (hlavne z tajnej korešpondencie francúzskeho kráľa Ľudovíta XVI.) a všeobecné vodítka k ich vyriešeniu a namietal, že pravidlá na odhaľovanie významu tajných správ sa nedajú exaktne sformulovať, sú skôr učenými odhadmi a ovocím trpezlivosti a vytrvalosti, tento jeho ambiciózny projekt stroskotal. Paradoxne neskôr však Wallis podobné argumenty použil pri značne prehnaných finančných požiadavkách, ktoré požadoval od anglického kráľa pre zaškolenie svojho vnuka **Williama Blencowa** [1, op.cit.]. Aj vďaka novým zisteniam prof. Reschera vieme, že okrem toho bol v listovom kontakte aj s pracovníkmi tzv. čiernych kabinetov najvýznamnejších panovníckych dvorov - **Antoine Rossignolom** (1600-1682) [1, s.157-161] a najmä doposiaľ neznámym abbém **Giuseppem Spedazzim**, pracujúcim v **Geheime-Kabinetz Kanzlei** vo Viedni [1, s.163], ktorý bol mimo iného aj skvelým hudobným skladateľom.

Leibniz bol taktiež fascinovaný myšlienkou vytvoriť univerzálny jazyk, všeobecný myšlienkový algoritmus, ktorým by získaval správnu odpoveď na každú otázku. Vždy si všímal funkčné závislosti, systematicky sa zamýšľal nad vlastnosťami matematických funkcií. Odhalil, že konečné možno vyjadriť ako nekonečný súčet nekonečne malých. V rokoch 1673 až 1676 objavil diferenciálny a integrálny počet. Výsledky však publikoval až v diele ***Nova methodus pro maximis et minimis*** – "*Nová metóda o najväčších a najmenších veličinách*" (1684) a neskôr ***De geometria recondita et analysi indivisibilium atque infinitorum*** - "*O skrytej geometrii a analýze nedeliteľných a nekonečných veličín*" (1686). Jeho terminológia a symbolika sa ujala. Ďalší učenci rozvinuli celú teóriu a jej aplikácie.

Narušitelia listového tajomstva

Existencia praxe otvárania, falšovania pečatí, kopírovania a lúštenia šifrovanej korešpondencie hlavnými európskymi mocnosťami ako bolo Francúzsko, Anglicko, Španielsko a sv. rímska ríša národa nemeckého je dostatočne známa. Možno však prekvapí fakt, že aj hannoverský vojvoda Georg Wilhelm z Braunschweig-Lünebergu využíval na získavanie informácií o plánoch cudzích diplomatov svoj vlastný menší, ale o to efektívnejší čierny kabinet. Strategická poloha tohto vojvodstva spočívala v prevažnej miere na skutočnosti, že všetka pošta pochádzajúca z Francúzska, ktorej cieľom boli škandinávske krajiny, východné Nemecko a Poľsko mala prechádzať cez toto teritórium. O jej vybavovanie, kontrolu a transport sa starali zamestnanci kniežat z Thurn a Taxisu, ktorí vlastnili monopol pre doručovanie poštových zásielok na väčšine územia Svätej rímskej ríše s výnimkou severu: Hamburg, Brandenburg-Prusko a vojvodstvá v Celle a Hannoveri. Slúžni rodiny Thurn a Taxis prijímali všetku poštu z Francúzska už v Španielskej časti Holandska, kde mali taktiež monopol. Pošta bola následné prevážaná cez Brusel, Kolín a Frankfurt do Norimbergu, kde bola rozdelená na dve časti: jedna bola určená pre severnú Európu a ďalšia pre Prahu a krajiny nachádzajúce sa ďalej za ňou. V Norimbergu bola všetka pošta otváraná a kopírovaná

cisárskymi úradníkmi pri plnej spolupráci kniežaťa z Thurnu a Taxisu. Čierny kabinet v Norimbergu bol založený na začiatku tzv. **Deväťročnej vojny** (vojna prebiehala v rokoch 1688 až 1697 medzi „pomazanými“ vládcami Holandska, Anglicka, ríšsko-nemeckého cisára Leopolda I. a radou menších či väčších ríšskych kniežat na jednej a francúzskeho kráľa "Slnko" Ľudovíta XVI. na druhej strane, zápasu o rovnováhu politicko-mocenských síl v Európe) a slúžil na monitorovanie francúzskej diplomatickej aktivity v Nemecku a východnej Európe.

V Celle boli tieto listy skopírované podruhýkrát z poverenia samotného vojvodu Georga Wilhelma a posunuté ďalej Britom.

Vojvoda mal v Celle prinajmenšom k dispozícii dvoch kryptoanalytikov, ktorí vedeli ako nakladať so zachyteným francúzskymi zašifrovanými listami. Boli to **Ludwig Ernst Neubourg** (zomrel v roku 1713) a **Johann Philip Schlemm** (1672 - 1733). Schlemm mal za manželku dcéru Johanna Albrechta Zachariaeho, hannoverského štátneho tajomníka, ktorý už na tomto poli zjavne mal nejakú skúsenosť. Do tohto umenia zasvätil obidvoch: Neubourga aj Schlemma a zrejme bol jedným z mála vzácnych ľudí, ktorí mali okamžitý vhľad do zložitých zákutí kryptológie. Môže tu zákonite vyvstať otázka, ako je možné, že sa v takom malom kniežatstve našlo zrazu v pravom momente dostatok schopných lúštiteľov. Práve tu treba poukázať na osobnosť Wilhelma Leibniza, ktorý vlastnil, podobne ako Wallis, silnú analytickú mysleľ so záujmom o jazyk a obzvlášť jeho gramatiku. Leibniz sa sám osobne síce nepovažoval za veľkého kryptoanalytika, ale mohol napomôcť rozvinúť analytickú bázu pre ľudí, ktorí boli evidentne, čo sa týka umenia lúštiť zložité nomenklátory oveľa nadanejší ako on.

Nešťastné opomenutie

Myšlienka šifrovacieho stroja, zrejme uzkostlivo strážená Leibnizom, však mohla preniknúť na stránky histórie čiernych kabinetov vďaka náhodnému stretnutiu Mohlo k tomu dôjsť pri prvej návšteve zo začiatku augusta roku 1716 bývalého kniežaťa, teraz už kráľa Juraja I., ktorý si zvolil za svoju prvú zahraničnú cestu návrat do Hannoveru, keďže ho postihla nemoc odišiel aj do Bad Pyrmontu, aby sa tu podrobil liečebnej kúre. Leibniz z Hannoveru tam odišiel 4. augusta a práve vtedy dorazil do Hannoveru, aby ho navštívil **Johann Ludwig Zollmann** (tajný radca v Zeitzi a Leibnizov častý korešpondent). Jeho syn **Philip Heinrich** nakoniec prišiel o deň neskôr za ním. Zollmann mladší, ako mimoriadne schopný rýchlo postupoval v spoločenskom rebríčku na dvore Hannoverského vojvodu, dokonca sa mal zaúčať do tajomstiev perlustrácie v Hannoverskom čiernom kabinete (Leibnizovi ho ako nadaného lúštiteľa do čierneho kabinetu odporučil jeho otec), nasledoval Juraja Ľudovíta do Británie po jeho nástupe na trón a presťahoval sa v roku 1714 do Londýna, kde ho barón Bothmer menoval za opatrovateľa a ochrancu jedného zo svojich synov. Tu mal vstúpiť aj do služieb anglického **Tajného úradu** – angl. ***The Secret Office*** a mal sa stať jedným z popredných londýnskych kryptografov. V roku 1723 bol menovaný zahraničným tajomníkom pri Royal Society, vďačil za to “svojmu ovládaniu mnohých jazykov”. V roku 1727 sa stal členom Royal Society. Pôvodne sa jeho meno písalo Zollmann, ale počas pobytu v Anglicku to druhé n vypustil. Zomrel v roku 1748. Zollmannovci boli ubytovaní v rovnakom dome na Schmiedestrasse, kde mal od roku 1698 žiť taktiež aj Leibniz, hlavným cieľom ich návštevy bolo zabezpečiť informácie o najnovšej, vylepšenej verzii Leibnizovho počítacieho stroja. Zmena plánov však zmarila príležitosť plodnej výmeny myšlienok medzi Leibnizom a

Zollmanovými ohľadne sľubného potenciálu jeho veľkého vynálezu, čo by malo nesporný význam najmä pre uľahčenie množstva mravenčej práce úradníkov v kniežacích tajných kabinetoch.

Ako jeden z najvzdelanejších učencov svojej doby Leibniz klasifikoval prvky ľudského myslenia. Prispel k základom modernej matematickej logiky, ma podiel na objave teórie determinantov. Zaoberal sa históriou, teológiou, filozofiou, jazykovedou, diplomaciou. Bol autorom niekoľkých technických vynálezov (napr. pumpy na odsávanie vody zo šachiet či oceľových pásov, čo je dnes neoddeliteľná súčasť moderného tanku). Dal podnet na vytvorenie akadémií vied v Prusku i v Rusku. V roku 1700 sa stal prvým predsedom Akadémie vied v Berlíne (*Sozietät der Wissenschaften*). V rokoch 1712-1714 zotrval Leibniz vo Viedni u princa Eugena Savojského (veľkého vojvodcu a jedného zo statočných obrancov Viedne proti Turkom), zúčastnil sa aj rokovania o tzv. **Utrechtskom mieri**. V závere jeho životnej púte ho však postretli nešťastné okolnosti. V roku 1714 umrela náhle anglická kráľovná Anna a za nového anglického kráľa bol zvolený Georg Ludwig Hannoverský, ktorý nielenže Leibnizovi nedovolil prísť do Londýna, ale ani v Hannoveri si nenašiel preň chvíľku času. Zomrel opustený a bez toho, aby si ho na hannoverskom dvore vôbec niekto všimol, dňa 14. novembra 1716. Je to smutné, ale mnohé Leibnizove matematické myšlienky boli realizované až v 20. storočí a možno, že niektoré ešte len na realizáciu čakajú. Na uskutočnenie čakajú aj jeho sny o znášanlivosti, porozumení a láske medzi ľuďmi a medzi národmi. Dá sa len na záver zaželať ľudstvu, aby raz na svete naozaj zavládla tá povestná leibnizovská harmónia a mier.

Obr. 6: Rekonštrukcia Leibnizovho šifrovacieho stroja

Prof. Rescher podrobne zaznamenal príbeh G.W. Leibniza a jeho vlastnej rekonštrukcie šifrovacieho stroja v brožúrke s názvom ***Leibniz and cryptography***, ktorá bola k dispozícii na slávnostnej prednáške spojenej s recepciou, konajúcej sa dňa 14. decembra 2012 v priestoroch Hillmanovej knižnice Univerzity v Pittsburgu. Pre prípadných záujemcov si ho prakticky vyskúšať, existuje aj softvérová realizácia algoritmu šifrovacieho stroja v programovacom jazyku Python 2.0.

Literatúra:

1. David Kahn, *The Codebreakers*, Scribner, 1996, 1200pp., **ISBN** 0-684-83130-9,

2. Bengt Beckman. *Codebreakers: Arne Beurling and the Swedish crypto program during World War II*. Translated by Kjell-Ove Widman. Providence, RI: American Mathematical Society, 2002, **ISBN** 0-8218-2889-4, 259pp.

3. Struik, Dirk Jan, *Dějiny matematiky*, 1. vyd. Orbis, 1963. Edice: Malá moderní encyklopedie ; sv. 43, 250s., s. 113-116,

4. "YRBFYR OTHN: Pitt Professor Resurrects History's First Sophisticated Wartime Coding Machine", 11.04.2013, http://www.news.pitt.edu/ciphermachine,

5. Jerry Proc, Revolving Drum Cipher, 11.04.2013 - http://jproc.ca/crypto/revolving_drum_cipher.html

6. "Leibniz's Reconstructed Cipher Machine on Display at University of Pittsburgh", German Missions in the United States, 11.04.2013, http://www.germany.info/Vertretung/usa/en/__pr/GKs/NEWY/2012/12/19__Leibniz.html

7. Project: Leibniz Encryption, 11.04.2013, http://anastasllc.com/blog/index.php/2012/09/26/project-leibniz-encryption/

8. Nicholas Rescher, **LEIBNIZ AND CRYPTOGRAPHY**: *An Account on the Occasion of the Initial Exhibition of the Reconstruction of Leibniz's Cipher Machine*, 11.04.2013, http://www.pitt.edu/~rescher/Leibniz%20Machine.htm

9. Wikipédia, Heslo: Gottfried W. Leibniz, 11.04.2013, http://en.wikipedia.org/wiki/Gottfried_Wilhelm_Leibniz

10. Rescher, Nicholas (2011) *LEIBNIZ'S MACHINA DECIPHRATORIA*. http://philsci-archive.pitt.edu/8499/

11. Zmek, Bořek, *Tajné poštovní lóže,* časopis **Genealogické a heraldické listy**, č. 5, roč. 1970, s.7-9

12. Oakley, S. P., „*Interception of posts in Celle, 1694-1700*", in Hatton and Bromley, eds., *William III. and Luis XIV.*, pp. 95-116,

13. Scherhaufer, Albin Franz, „*Der Kaiserliche Dechiffriersekretär Johann Joseph von Neuff (1677-1734)*", In Wiener Geschichtsblätter, Roč. 17 (1962), s. 46-51

14. Stix, Franz, *Zur Geschichte und Oragnisation der Wiener Geheimen Ziffernkanzlei*, in: MIÖG 51 (1937), S. 131-160,

15. Schooling, J. Holt, *Secret in Cipher*, II. From late Elizabethan Days to Mid-Stuart Times, The Pall Mall Magazine, Vol VIII, No. 33, p. 249

C. Kaspersky Lab odhalila novou kyberšpionážní operaci NetTraveler

Moskva, 4. června 2013 – Analytici Kaspersky Lab zveřejnili zprávu o nové kampani kybernetické špionáže NetTraveler (Cestovatel po síti). Skupina škodlivých programů infikovala 350 obětí, mezi nimi významné vládní a veřejné instituce ve 40 zemích po celém světě. Jedná se jak o vládní úřady a ambasády, tak i o ropný průmysl, výzkumná centra, zbrojní firmy i aktivistické organizace. Cílem útoků bylo sledování činnosti obětí a také krádež dat.

Dle zprávy Kaspersky Lab probíhal útok už od roku 2004. Nejvíce aktivity pak analytici zaznamenali v letech 2010 až 2013. Naposledy se útočníci zaměřili na oblasti výzkumu vesmíru, nanotechnologií, energetiky (včetně jaderné), laserů, medicíny a komunikace.

Oběti útočníci napadli pomocí sofistikovaných phishingových e-mailů se škodlivými přílohami – soubory Microsoft Office obsahujícími vysoce zneužitelné zranitelnosti (CVE-2012-0158 a CVE-2010-3333). Přestože Microsoft už dávno vydal jejich záplaty, stále jsou účinnými prostředky cílených útoků.

Dle názvů škodlivých příloh lze odhadnout, jak významné byly cíle útočníků:

- Army Cyber Security Policy 2013.doc (armádní plán kybernetické bezpečnosti)
- Report - Asia Defense Spending Boom.doc (růst výdajů na obranu v Asii)
- Activity Details.doc (detaily činnosti)
- His Holiness the Dalai Lama's visit to Switzerland day 4 (návštěva jeho svátosti Dalajlámy ve Švýcarsku, den čtvrtý)
- Freedom of Speech.doc (svoboda slova)

Na C&C servery NetTraveleru bylo dle vyšetřování analytiků Kaspersky Lab nahráno více než 22 gigabytů odcizených dat. Mezi nimi byly systémové údaje, záznamy psaní na klávesnici či PDF, excelové a wordové dokumenty a soubory. NetTraveler byl také schopen do počítačů nainstalovat backdoor ve formě malwaru, který kradl citlivé informace, například detaily nastavení aplikací.

Ačkoli nebyla prokázána jakákoliv spojitost, NetTraveler si vybral k útoku několik významných obětí, které se staly cílem útoku také kybernetické špionážní kampaně Red October, o níž informovala společnost Kaspersky Lab už v lednu.

Kompletní analýzu Kaspersky Lab s detaily útoku NetTraveler naleznete zde.

Produkty Kaspersky Lab identifikovaly a neutralizovaly škodlivé programy toolkitu NetTraveler s označením ***Trojan-Spy.Win32.TravNet*** *a* ***Downloader.Win32.NetTraveler****, a několik zranitelností souborů Microsoft Office používané při phishingu této kampaně, zejména* ***Exploit.MSWord.CVE-2010-333*** *a* ***Exploit.Win32.CVE-2012-0158****.*

Pro další informace prosím kontaktujte:
Michal Malysa
PR Consultant
Grayling
Tel.: 224 251 555
Mobil: 775 708 086
michal.malysa@grayling.com

D. Reakcia na článok „Andreas Figl – rakúsky dôstojník a kryptológ“

Jozef Krajčovič, kryptosvet@gmail.com, http://katkryptolog.blogspot.sk

Zo značným záujmom a zvýšenou pozornosťou som si prečítal článok uverejnený v e-zine C-W 3-4/2013 a po jeho zbežnom prelúskaní som si aj osobne povzdychol, ako pekne, pútavo a hlavne pregnantne na mňa reagoval "kolega" pán Kollár. A rozviedol moju krátku a nepresnú poznámku o "nájomnej práci" A. Figla pre nacistické Nemecko. Nebudem sa s ním vôbec hádať, že som o jeho nedobrovoľnom "angažmá" pre III. Rišu a napojení na Wilhelma Höttla z RSHA, nenapísal viacej vysvetľujúcich riadkov. Mal som na to svojské dôvody z hľadiska, ktoré môže a domnievam sa, že aj musí pochopiť naozajstný nadšenec pre všetko súvisiace s bezpečnosťou informácií a fascinujúcimi tajomstvami šifier a kódov. Predpokladal (teraz už viem, že mylne) som totiž, že snáď každý odborný čitateľ C-W je s osudmi Andreasa Figla oboznámený aj z populárno-historického popisu pána V. P. Borovičku, ktorý sa dá nájsť vo forme menšieho odstavca v jeho knihe ***Přísně tajné šifry*** [5]. Ale aspoň sa môžem utešovať z nesporného faktu, že mojím pričinením vznikol pekný článok o jeho "zakázanom" strojopise ***Systeme des Dechiffrierens***.

Po počiatočných uznanlivých prejavoch úcty som sa však odhodlal aj napriek týmto značným pozitívam poukázať na niektoré problematické zákutia, ktoré sa tak ako v každom subjektívne ladenom diele nachádzajú aj v ňom.

Zareagujem postupne na tie pasáže v článku, v ktorých pán Kollár podľa môjho názoru zašiel mimo rámec historickej skutočnosti, ktorú uvediem podľa viacerých prameňov. Na začiatku je to pozn. pod čiarou, v článku [1] uvedená na strane 17, citujem: "*Amt VIE = úrad VIE, bol zahraničnou spravodajskou službou R.S.H.A. pre Európu. Nebolo to spravodajstvo nacistickej strany ako sa nepresne uvádza v článku [6], ale v našej terminológii by sme to mohli nazvať spravodajstvom štátnej bezpečnosti.*"

Podľa [2] v hesle o **SD** (***S**icherheits**d**ienst des Reichsfuhrers der SS*, Bezpečnostnej službe ríšskeho vodcu SS) na str. 311-312 sa uvádza, že „*po už po r. 1932, kedy bol menovaný do jej čela známy "kat" českého národa R. Heidrich, ktorý sa stal v roku 1934 de facto vedúcim Gestapa, došlo v týchto štátnobezpečnostných zložkách k uvedeniu stavu typickému pre nacizmus - a to je stieranie hraníc medzi štátnymi a stranickými inštitúciami. Ďalej sa tu tvrdí, že ešte na začiatku mesiaca, kedy malo dôjsť aj k známej "noci dlhých nožov", ktorá sa uskutočnila dňa 30. júna 1934, bola dekrétom SD vyhlásená za jedinú spravodajskú organizáciu NSDAP. Neskôr, konkrétne v novembri 1938, došlo k prijatiu dekrétu, ktorým sa z nej stala jediná stranícka aj štátna spravodajská služba. V septembri 1939 bola včlenená do aj mnou v článku uvádzaného úradu RSHA, kde SD Inland tvoril Úrad III a SD Ausland Úrad VI*“. Preto **Amt VIe**, tj. **Úrad VIe** môže byť podľa vyššie uvedených faktov z histórie tejto nacistickej organizácie podľa mojej mienky nazvaný aj "spravodajstvo nacistickej strany", bez ujmy na presnosť a úplnosť.

Mám však aj ďalšie rukolapné skutočnosti, ktoré ma utvrdzujú o správnosti mojej formulácie. O funkcii úradu v rámci RSHA, oddelenia Amt VI-E, sa dá čo to dozvedieť, aj keď sa bližšie prizriete na text z nemeckej wikipédie, heslo SD [3]:

Hneď prvý odstavec je veľavravný:
"*Der Sicherheitsdienst des Reichsführers-SS (Abkürzung SD[1]) war ein Teil des nationalsozialistischen Machtapparates in der Zeit des Nationalsozialismus im Deutschen Reich und während des Krieges im besetzten Europa. Er wurde 1931* ***als Geheimdienst der NSDAP*** *(zvýraznil J.K.) bzw. der ihr zugehörigen SS gegründet und unterstand ab 1939 dem Reichssicherheitshauptamt (RSHA).*"

Uvedený citát spolu s popisom ďalšieho vývoja tejto tajnej služby jasne dokladuje, že na rozdiel od skutočne relatívne ideologicky "neutrálnej" zahraničnej tajnej služby, Abwehru, ktorého bol šéfom admirál Canaris, a ktorý dokonca mal napojenie na vnútornú protinacistickú opozíciu vo vojenských a civilných kruhoch, je myslím zrejmé, že môj čiastočne skrátený popis je formálne korektný. Môže sa síce nepriamo namietať, že v každej zložke štátnobezpečnostného aparátu III. ríše bol viac menej otvorene prítomný vplyv nacistickej strany na ich chod a riadenie, ale tento nie je doložený napr. takými nespochybniteľnými skutočnosťami, ako je to práve v prípade **SD**, a jej zložky **Ausland-SD**, tj. v oddelení ozn. **Amt VI-E** ich úplným mocenským ovládnutím fanatickými nacistickými pohlavármi typu R. Heidricha, E. Kaltenbrunnera a napokon aj bezprostredným vplyvom ríšskeho vodcu SS Heinricha Himmlera.

Ak sa ešte pristavím pri pánovi Borovičkovi a jeho knihe *Prísne tajné šifry* [5], (mám obidve vydania, české a slovenské v osobnej knižnici) on tam v tomto prípade dôsledne vychádza z kapitálneho diela vari snáď najznámejšieho kryptologického historika Davida Kahna[4], ktorá o tejto nešťastnej "službe" A. Figla pre RSHA podáva ucelené informácie vychádzajúce z vtedy dostupných prameňov, ktoré však nezmenili žiadne "nové" odhalenia. Takže v tomto ohľade sa aj na "detektívkára a popularizátora" V. P. Borovičku aspoň čo sa týka relevantného odstavca možno spoľahnúť.

Pán Borovička samozrejme vo svojej knihe rovnako píše nepresnosti a nepravdy, napr. čo sa týka formálneho popisu polyalfabetickej substitúcie aj iných tématických okruhov spojených s "imperialistickými" západnými tajnými službami, pretože vtedajší komunistický režim jednoducho vďaka cenzúre nedovoľoval, aby určité fakty o NSA a pod. boli zverejňované v pozitívnom, ba ani "neutrálnom" tóne. Práve v [4], na strane 449 a nasl. spomína zatknutie A. Figla Gestapom v r. 1938 a následné všimnutie si jeho neutešenej existencie Wilhelmom Höttlom, dôstojníkom novovzniknutého RSHA.

No a na záver sľubený citátik z českého vydania knihy [5], ktorý sa nachádza na str. 57-58:
"*... Šlo o velmi komplikovaný systém, takzvané diagrafické šifry (moja pozn. v skutočnosti bigramové), a vrchní velení SS se k němu dostalo shodou mnoha okolností. Hned po anšlusu Rakouska v březnu 1938 se tehdejší pracovník abwehru a pozdější šéf sicherheitsdienstu a nakonec také abwehru Walter Schellenberg dostal do archívu rakouské výzvědné služby a našel zde úplnou kódovou (pozn. šifrovaciu) dokumentaci. Na svou dobu byla velice progresívní a berlínští odborníci okamžite prohlásili, že převezmou některé prvky do nově připravovaného systému. Nebylo to tak snadné. K vypracování zásad provozu bylo zapotřebí velkých zkušeností a teoretických znalostí. Esesáci je neměli. Měl je však jejich vězeň.*
Když převzali nacisté v Rakousku moc, zatkli a zavřeli vynikajícího teoretika a šifrovacího experta, rakouského generála (pozn. aj podľa pána Borovičku!) Andrease Figla. Teď si na něho vzpoměli a dali ho přivézt z věznice. Není vyloučeno, že právě on byl autorem, nebo alespoň jedním z autorů, onoho pozoruhodného šifrovacího systému. Není známo, zda a jakým způsobem ho přinutili, nebo jestli sám kapituloval, ale Figl souhlasil s návrhem,

nastěhoval se do kanceláře ve Wannsee u Berlína a založil zde šifrovací odbor SS a SD (Geheimfernmeldewesen des SD und SS). Zde pak vznikla složitá šifra, ktorou měli Rejewski a Zygalski rozluštit. ..."

Nakoniec som však veľmi rád, že pán Kollár reagoval na môj článok a bližšie rozobral "zakázané dielo" *Systeme des Dechiffrierens*, ktoré som nemal k dispozícii pri jeho písaní.
Postscriptum: Až neskôr sa ukázalo, a to po dôkladnejšom rešerši v mojom osobnom archíve, že domnienku pána Kollára o hodnosti Andreasa Figla ako generála podporuje aj znenie poznámky pod čiarou, ktorú som si všimol v článku [6], o histórii viedenskej ***Geheime Kabinetz Ziffernkanzlei***. Citujem v pôvodnom znení:

„*Andreas Figl,(pozn. nasleduje názov jeho prvotiny) ... . Figl, österreichischer Geheimdienstmann des Ersten Weltkrieges, wurde 1938 als General (pozn. podčiarkol J.K.) und Chef des österreichischen Dechiffrierdienstes von der Gestapo verhaftet, bald darauf aber - vermutlich auf Görings persönliche Intervention - freigesetzt und in einer Villa am Wannsee als Instruktor des deutschen Geheimdienstes verwendet, wo er seinen Schatz an Erfahrungen an eine ganze Generation von Chiffreuren weitergab.*“

Literatúra:

[1] Kollár, Jozef M., *Andreas Figl – rakúsky dôstojník a kryptológ*, In Crypto-World, 3-4/2013, s. 15 - 23,

[2] Churáň, M. a kol., *Encyklopédie špionáže*, Praha: Libri, 2000, s. 311-312,

[3] Wikipedia, jej nemecká verzia, heslo o tajnej službe SD: http://de.wikipedia.org/wiki/Sicherheitsdienst_des_Reichsf%C3%BChrers-SS, 11.04.2013,

[4] Kahn, David, *The Codebreakers: Story of Secret Writing*, New York, Scribner, 1996, pp. 449-451,

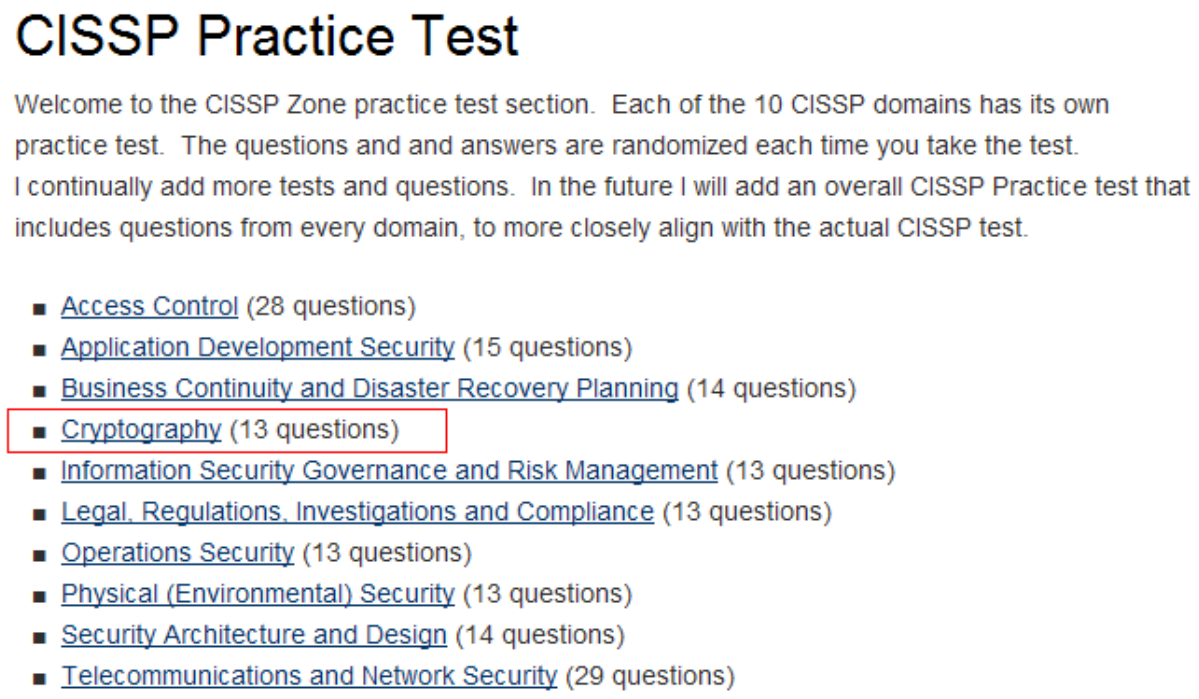
[5] Borovička, V. P. *Přísně tajné šifry*, Praha, Naše vojsko, 1982, 1. vyd., 320s.

[6] Harald Hubatschke, *Die amtliche Organisation der geheimen Briefüberwachung und des diplomatischen Chiffrendienstes in Österreich*. (Von den Anfängen bis etwa 1870), in: Mitteilungen des Instituts für Österreichische Geschichtsforschung 83 (1975), S. 352–413, konkrétne s. 363.

E. Cvičný CISSP test z kryptografie

Pro zajímavost si můžete otestovat své obecné znalosti z kryptografie na jednom z cvičných testů ke zkoušce k CISSP.

CISSP (The Certified Information Systems Security Professional) je jednou z celosvětově uznávaných zkoušek z oblasti informační bezpečnosti. Získaný certifikát prokazuje znalost bezpečnostních témat na úrovni bezpečnostního specialisty. Mezi témata, která je potřeba zvládnout, patří cloud computing, mobilní bezpečnost, vývoj aplikací, řízení rizik, BCM, fyzická bezpečnost, telekomunikace, síťová bezpečnost a také PKI a kryptografie.


CISSP Practice Test

Welcome to the CISSP Zone practice test section. Each of the 10 CISSP domains has its own practice test. The questions and and answers are randomized each time you take the test. I continually add more tests and questions. In the future I will add an overall CISSP Practice test that includes questions from every domain, to more closely align with the actual CISSP test.

- Access Control (28 questions)
- Application Development Security (15 questions)
- Business Continuity and Disaster Recovery Planning (14 questions)
- Cryptography (13 questions)
- Information Security Governance and Risk Management (13 questions)
- Legal, Regulations, Investigations and Compliance (13 questions)
- Operations Security (13 questions)
- Physical (Environmental) Security (13 questions)
- Security Architecture and Design (14 questions)
- Telecommunications and Network Security (29 questions)

Certifikát vydává (ISC)² .
Více infromací ke zkoušce a k získání certifikátu najdete např. zde:
How to Get Your CISSP® Certification https://www.isc2.org/cissp-how-to-certify.aspx .

Zkouška se skládá v anglickém jazyce.

Pro test vašich znalostí z části kryptografie využijte následující volně dostupný test, který je k dispozici na podpůrných stránkách k přípravě na zkoušku CISSP:

Cryptography Practice Test Questions

Question 1
What key length does AES not support?

a) 192-bit
b) 256-bit
c) 512-bit
d) 128-bit

Question 2
Which of the following is a disadvantage of asymmetric cryptology?

a) Does not provide non-repudiation
b) Slower than symmetric cryptology
c) Complex key distribution
d) No potential for centralized key management

Question 3
Which term relates specifically to the art and science of code breaking?

a) Cryptography
b) Cryptanalysis
c) Cryptology
d) Repudiation

Question 4
Public Key Infrastructure uses a "web of trust" to verify identities?

a) False
b) True

Question 5
Which algorithms are no longer recommended for use?

a) DES
b) RSA
c) IPSEC
d) AES

Question 6
The Digital Signature Algorithm implements a modified version of which algorithm that is based on discrete logarithms in a finite field?

a) Merkle-Hellman Knapsack
b) El Gamal
c) AES
d) Twofish

Question 7
What is the attempt to hide data in "plain view"?

a) El Gamal
b) Cryptanalysis
c) Substitution
d) Steganography

Question 8
The Caesar Cipher is an example of what kind of cipher?

a) Substitution
b) Transportation
c) Steganography
d) Vernam

Question 9
The Digital Signature Standard specifies all of the following as valid algorithms for creating digital signatures except:

a) RSA
b) DSA
c) ECDSA
d) AES

Question 10
Which key exchange technique allows parties to exchange secret keys over an insecure medium without exposing the keys?

a) Diffie-Hellman
b) Merkle-Hellman Knapsack
c) MD5
d) Twofish

Question 11
Storing private keys with a third party is referred to as what?

a) Key escrow
b) Key caching
c) Key backup
d) Key banking

Question 12
Digital certificates contain both a public and private key

a) False
b) True

Question 13
Secure hash algorithms provide both confidentiality and integrity?

a) False
b) True

Nyní si zkontrolujte své odpovědi:

CORRECT 1c 2b 3b 4a 5a 6b 7d 8a 9d 10a 11a 12a 13a

Pokud jste dosáhli 100 %, pak upřímně blahopřeji.

F. Central European Conference on Cryptology 2013
26.-28. června, Telč

V posledním červnovém týdnu se uskuteční v bývalé jezuitské koleji v Telči, dnes středisku Masarykovy univerzity, konference MoraviaCrypt, v rámci sérií konferencí ***„Central European Conference on Cryptology“.***

Zvané přednášky představí zajímavé výsledky Rainera Steinwandta (Florida Atlantic University) na téma kryptoanalýzy s kvantovými počítači, Dietera Gollmanna (TU Hamburg) o kompilátorech s nulovým rozšířením znalostí a Clemense Heubergera (TU Graz) na téma efektivní implementace kryptografie (hyper)eliptických křivek.

Konferenci pořádá Fakulta informatiky Masarykovy univerzity, stránky conference lze nalézt na http://www.fi.muni.cz/cecc/ a předběžný program conference uvádíme níže.

Conference program

Tuesday, June 25

Early evening (time TBD) - Registration desk open

Wednesday, June 26

08:30 - 09:15	Registration desk open
09:15 - 09:30	Conference opening
09:30 - 10:30	Invited talk 1 - Rainer Steinwandt
10:30 - 11:00	Coffee break
11:00 - 11:30	Talk 1: Eugen Antal. Lightweight cipher based on FIALKA M-125 design
11:30 - 12:00	Talk 2: Nicolas Courtois. New Combined Differential And Complexity Reduction Attacks on GOST
12:00 - 12:30	Talk 3: Pavol Zajac and Michal Ondros. Rotational cryptanalysis of the simplified GOST
12:30 - 14:00	Lunch
14:00 - 14:30	Talk 4: János Folláth and Tamás Herendi. On construction of sequences with Gaussian distribution
14:30 - 15:00	Talk 5: Laszlo Csirmaz. Probabilistic Infinite Secret Sharing
15:30 - 16:00	Coffee break
16:00 - 16:10	Position I: Anna Grocholewska-Czurylo, Janusz Stoklosa, Krzysztof Bucholc and Krzysztof Chmiel. A New Block Cipher PP-2
16:10 - 16:20	Position II: Arkadiusz Gasecki. Low Data Complexity Differential-Algebraic Attack on Reduced Round DES
16:20 - 16:30	Position III: Piotr Syga, Marek Klonowski, Przemyslaw Kubiak, Miroslaw Kutylowski and Tomasz Struminski. Authentication with a RFID Tag - Fighting Pickpockets
16:30 - 16:40	Position IV: Marek Sys and Petr Svenda. Evolutionary circuit with limited set of functions - an application to eStream candidates
16:40 - 16:50	Position V: Renata Kawa. Nonhierarchical Secret Sharing Schemes

16:50 - 17:00	Position VI: Matus Jokay, Martin Kosdy and Martin Cavoj. Steganographic File System Embedded in Static Images
17:00 - 17:10	Position VII: Éva Csernusné Ádámkó and Attila Pethõ. Security analysis of a Location Stamping protocol for GPS coordinates
17:10 - 17:20	Position VIII: Anna Grocholewska-Czurylo. Statistical analysis of strong S-boxes
17:20 - 17:30	Position IX: Sami Omar and Houssem Sabri. Convolution Product and Fast Hash Functions
17:30 - 18:20	Rump session (or short presentations and then rump session)

19:00 Conference dinner (venue TBA)

Thursday, June 27

08:30 - 09:00	Registration desk open
09:00 - 10:00	Invited talk 2 - Dieter Gollmann
10:00 - 10:30	Talk 6: Pavol Svaba, Van Trung Tran and Pascal Marquardt. MSTg: Cryptographically strong pseudorandom number generator and its realization
10:30 - 11:00	Coffee break
11:00 - 11:30	Talk 7: Gyula O.H. Katona. A combinatorial problem motivated by identification with labels
11:30 - 12:00	Talk 8: Tommi Meskanen, Valtteri Niemi and Noora Nieminen. Classes of Garbling Schemes
12:00 - 12:30	Talk 9: Michal Hojsík and Petr Nižnanský. Algebraic, Fast Algebraic and Higher Order Algebraic Attacks
12:30 - 14:00	Lunch
14:05	Visit to the Telc Chateau (http://www.zamek-telc.eu/en/) and then individual touring of the town and parks, followed by individual discussions, meetings & dinners

Friday, June 28

08:30 - 09:00	Registration desk open
09:00 - 10:00	Invited talk 3 - Clemens Heuberger
10:00 - 10:10	Position X: Ivan Gorbenko, Elena Kachko and Konstantin Pogrebnyak. Parallelized Pollard's Rho Method for Multi-core Processors for Computing Discrete Logarithms
10:10 - 10:20	Position XI: Laszlo Merai. Pseudorandomness of binary sequences derived from linear recursive sequences
10:20 - 10:30	Position XII: Marcel Šebek. Towards Fully-Bideniable Public-Key Encryption
10:30 - 11:00	Coffee break
11:00 - 11:30	Talk 10: Attila Pethõ and Noriko Hirata-Kohno. On a key exchange protocol based on Diophantine equations
11:30 - 12:00	Talk 11: Sangeetha Jose, Preetha Mathew K and Chandrasekaran Pandu Rangan. An Efficient Password Based Blind Signature for Real World Applications(Extended Abstract)
12:00 - 12:30	Talk 12: Przemyslaw Kubiak, Miroslaw Kutylowski and Wojciech Wodo. Protection of Digital Images from Personal Identity Documents
12:30 - 14:00	Lunch

End of the conference

G. Call for Papers
Mikulášská kryptobesídka

28. – 29. listopad 2013, Praha
http://mkb.tns.cz

Základní informace

Mikulášské kryptobesídky už letos bude do jednoho kusu po tuctu. 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 *28. listopadu* a (b) půldne prezentací příspěvků a diskusí v pátek *29. listopadu 2013*. Pro workshop jsou domluveny zvané příspěvky od:

- Riccardo Focardi (Univ. Venezia, Itálie).
- Flaminia Luccio (Univ. Venezia, Itálie).
- David Naccache (ENS, Francie).
- Karsten Nohl (nezávislý výzkumník, SRN).
- Tomáš Rosa (Raiffeisenbank & UK, ČR).

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

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.tns.cz. 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 2013*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2013 – 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 2013
Oznámení o přijetí/odmítnutí:	29. října 2013
Příspěvky pro sborník:	12. listopadu 2013
Konání MKB 2013:	28. – 29. listopadu 2013

Programový výbor

Michal Hojsík, UK, Praha, CZ
Marek Kumpošt, NetSuite & FI MU, Brno, CZ
Vašek Matyáš, FI MU, Brno, CZ – předseda
Zdeněk Říha, FI MU, Brno, CZ
Luděk Smolík, Siegen, DE
Martin Stanek, UK, Bratislava, SK
Pavol Zajac, STU, Bratislava, SK

Mediální partneři

H. 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 7-8/2012

Příloha: dokument, který měl být odeslán pouze do interní skupiny NISTu pro výběr SHA-3
(více informací viz článek V.Klímy)

Crypto-World 9-10/2012

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

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

Crypto-World 1-2/2013

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

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

I. 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/