Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 15, číslo 7-8/2013 **18. srpen**

7-8/2013

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1320 registrovaných odběratelů)

Obsah :

A. Reino Häyhänen – sovietsky špión

Jozef Kollár, jmkollar@math.sk
KMaDG, SvF STU v Bratislave

1 Úvod

Reino Häyhänen, alias Eugene Maki, alias Victor alebo Vic bol sovietsky agent pôsobiaci v rokoch 1952 až 1957 v USA. Za to, že neupadol do zabudnutia ako množstvo iných vďačí trom faktom:

- bol to on, kto zradil úspešného sovietskeho agenta Rudolfa Abela a pričinil sa o jeho odsúdenie,
- s trochou zjednodušenia sa dá o ňom povedať, že vo všetkých aspektoch svojho agentského pôsobenia v USA zlyhal,
- v súvislosti s ním je známa šifra VIC.

Niektoré informácie o ňom boli známe už od prvého zverejnenia knihy [1] koncom 60-tych rokov. V kapitole o sovietskej kryptografii sa tam, okrem iného, píše aj o šifre VIC a v súvislosti s ňou o Häyhänenovi, ktorý ju používal. Ale podrobnosti jeho prípadu boli zverejnené až v 90-tych rokoch, po odtajnení materiálov CIA ([4] a [2]).

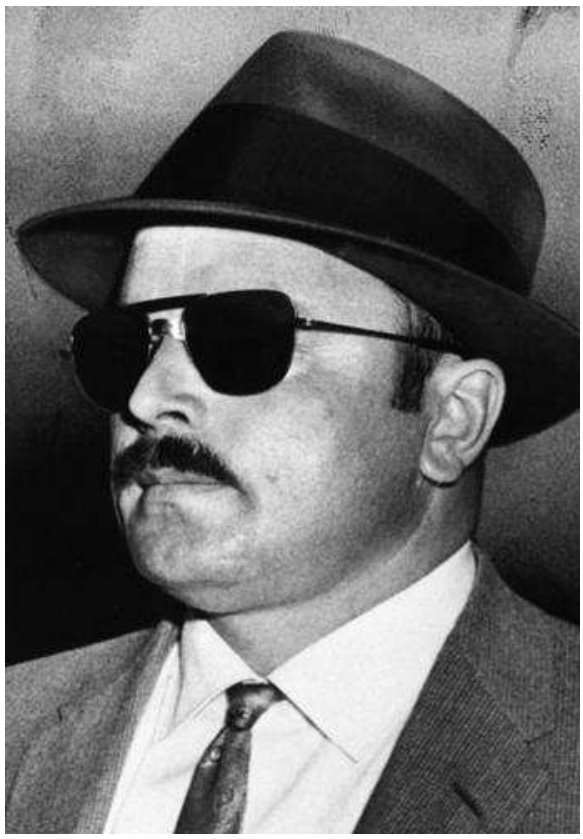
V tomto článku si prerozprávame Häyhänenov životný príbeh. Väčšina informácií bude prevzatá z [4][1], ale čiastočne aj z ďalších zdrojov uvedených v závere článku, ako aj z rôznych webových zdrojov. Webové zdroje, s výnimkou Wikipédie a použitých fotografií, som v použitej literatúre neuvádzal, pretože kvalita informácií v nich obsiahnutých, je veľmi rôznorodá a často obsahujú aj nepresné, alebo úplne chybné informácie. Z webových zdrojov som použil preto len fakty obsiahnuté v niekoľkých rôznych zdrojoch a tie sa väčšinou nachádzajú aj v spomenutom článku a na Wikipédii.

V pokračovaní na budúce by sme potom uviedli podrobný popis šifry VIC, pretože je to z kryptografického hľadiska veľmi zaujímavá ručná šifra.

2 Reino Häyhänen

Reino Häyhänen sa narodil 14. mája 1920 ako syn sedliakov v Leningradskej oblasti, kde sa hovorilo po fínsky. Jeho rodný jazyk bola teda fínština a aj základnú a strednú školu absolvoval po fínsky. V roku 1939, po absolvovaní učiteľského ústavu, ktorý skončil s vyznamenaním, začal pracovať ako učiteľ matematiky a fyziky. Avšak už po dvoch mesiacoch ho zverbovala bezpečnostná služba NKVD. To bolo tesne pred vypuknutím zimnej (fínskej) vojny. Tejto vojny sa Häyhänen zúčastnil ako tlmočník. Aj po skončení zimnej vojny zostal pracovať pre NKVD a osvedčil sa ako expert na otázky fínskej „inteligencie“, v kruhoch ktorej vyhľadával antisovietske živly. V máji roku 1943 bol prijatý do komunistickej strany.

[1] Z prevažnej časti sa jedná o skrátené „prerozprávanie“ uvedeného článku.



Obr. 1: Reino Häyhänen (* 14. 5. 1920) počas procesu s Abelom [8]

V roku 1948 stál plukovník Korotkov, šéf tajných zahraničných spravodajských operácií, pred problémom ako vyriešiť nedostatok použiteľných agentov v USA. Rudolf Abel, spoľahlivý agent pracujúci v USA, bol už takmer v „dôchodkovom“ veku a zatiaľ ako jediná jeho potenciálna náhrada bol agent s prezývkou „Big Shot“[2]. Tento agent sa na svoj post dostal ako politický protežant a bol na požadovanú činnosť nevhodný. Neskôr bol kvôli tomu aj stiahnutý späť. Preto plukovník Korotkov hľadal ďalších kandidátov, ktorí by po viacročnej príprave boli schopní nahradiť Abela a pokračovať v jeho práci. Jedným z kandidátov bol aj 28 ročný operatívny pracovník štátnej bezpečnosti v Karelo-Fínskej SSR, poručík Reino Häyhänen. Jeho kádrový profil sa plukovníkovi Korotkovovi pozdával. Jediným negatívom údajne bolo, že Häyhänen bol ženatý a mal adoptovaného syna. Korotkov však predpokladal, že v prípade zahraničného pôsobenia zvládne aj dlhodobé odlúčenie od rodiny. Häyhänen bol teda zverbovaný a absolvoval počiatočný výcvik v Estónsku, v Talline. Spočiatku sa domnieval, že ho potrebujú ako agenta pre Fínsko, vzhľadom na jeho znalosť fínštiny. Naviac mu sľúbili, že na svoje nové pôsobisko bude môcť vziať aj svoju manželku a syna. Až neskôr mu došlo, že tieto sľuby zrejme nie sú reálne a potom, čo mu bolo doporučené učiť sa anglicky, zistil, že jeho cieľovou krajinou asi nebude Fínsko. V Talline Häyhänen strávil polovicu svojho času učením sa za automechanika a zvládaním fototechniky.

Začiatkom roku 1949 bol Häyhänen povolaný do Moskvy, kde výcvik pokračoval pridelením a učením sa legendy, pod ktorou bude v zahraničí pôsobiť a overením si jeho

[2]Túto dehonestujúcu prezývku mu podľa [4] dal práve Abel.

jazykových schopností. Korotkov mal preňho pripravené dve možné identity. Prvou bol pas 12 ročného chlapca z USA, ktorý prišiel do Sovietskeho zväzu so svojími rodičmi v roku 1925. Táto krycia identita nebola ideálna, pretože dotyčný chlapec by bol v tom čase o 7 rokov starší než Häyhänen. Druhá možná identita bola z tohto hľadiska lepšia. Bol ňou Eugen Maki, narodený v Idahu, ktorý prišiel so svojími rodičmi do Estónska v roku 1927 a v súčasnosti pracoval ako šofér a automechanik v KFSSR. Eugen Maki bol len o rok starší než Häyhänen. Okrem toho Maki nemal v USA žiadnych príbuzných, s ktorými by v budúcnosti mohli byť problémy. Korotkov dal Häyhänenovi skonfiškovaný Makiho rodný list, pomocou ktorého mal po nejakom čase získať na americkom konzuláte pas. Na ďalší výcvik bol Häyhänen, teraz už ako Maki, presunutý do Valgy ležiacej v Estónsku na Lotyšských hraniciach, kde oficiálne pracoval ako automechanik. Ohľadne jeho rodiny mu boli dané len vyhýbavé odpovede a bolo mu doporučené, aby žena a syn zostali aj naďalej v Talline s tým, že sa môžu stretávať cez víkendy. V máji bol Maki povýšený na kapitána a očakával, že čoskoro sa začne jeho misia v zahraničí. Zároveň si uvedomil, že jeho krytie nie je dostatočné. Ak by sa uchádzal o ameriký pas ako Eugen Maki, žijúci dlhší čas v Estónsku, tak by sa dostal do pozornosti amerických úradov a bolo by podozrivé, že neovláda estónštinu. Jeho znalosť fínštiny by mu bola zbytočná. Major Abramov ale prišiel s vysvetlením, že keď v roku 1943 sovietske vojská oslobodzovali Estónsko, mnohí estónci utekali do Fínska. Medzi nimi mal údajne byť aj Maki, ktorý odvtedy žil a pracoval vo Fínsku. Maki teda ukončil svoje pôsobenie vo Valge a vrátil sa na čas do Moskvy po nové inštrukcie. Bolo rozhodnuté, že bude presunutý do Fínska a jeho žena a syn majú zostať naďalej v Talline. Ani jeden z nich totiž neovládal fínštinu a tým by obmedzovali jeho mobilitu. Alexa, jeho žena, to už nevydržala, a preto ju Häyhänen odviezol aj so synom do Tambova neďaleko Moskvy, ku jej rodine.

Vo Fínsku sa mal Maki naučiť žiť pod cudzou identitou, stýkať sa s riadiacim dôstojníkom a miestnymi agentami a používať mŕtve schránky a iné komunikačné kanály. Do Fínska bol Maki prepašovaný v kufri diplomatického auta patriaceho veľvyslanectvu v Helsinkách. V aute bol ako pasažier aj Makiho riadiaci dôstojník Vorobjev, ktorý pracoval vo Fínsku pod oficiálnym krytím ako korešpondent novín Práca. Maki strávil nejaký čas za polárnym kruhom v Laponsku a neskôr pracoval v oceliarňach v Tampere ako pomocný robotník. V lete a na jeseň roku 1950 už začínal byť Maki netrpezlivý a nevedel sa dočkať svojej misie v USA. Pri kontrolovaní svojej legendy si všimol, že na jeho, Makiho, rodnom liste je poznámka o neplatnosti v prípade modifikácie. Pritom bolo proti svetlu evidentné, že jeho rodný list bol upravovaný. V Moskve z neho odstraňovali pečiatku, ktorú tam dostal skutočný Maki pri žiadosti o ruský pas. Maki preto z vlastnej iniciatívy napísal list úradom v Idahu, uviedol, že stratil svoj rodný list a požiadal o vystavenie kópie, ktorú skutočne v januári 1951 dostal. O tomto svojom kroku Maki neinformoval vopred Moskvu.

V septembri 1950 nastal v Makiho osude zlom. Zoznámil sa s Hannou Kurikka, mladou, veselou, ale nie moc vzdelanou blondínkou pochybnej povesti a okamžite sa do nej zamiloval. Hanna bola opakom Häyhänenovej manželky Alexy a s najväčšou pravdepodobnosťou to bol práve vzťah k nej, ktorý neskôr viedol k Makiho zrade. Moskva o tomto vzťahu nebola informovaná. Počas roku 1951 Hanna stále intenzívnešie naliehala na Makiho aby sa vzali. V júli 1951 Maki, na pokyn Moskvy, požiadal o americký pas a v novembri sa oženil s Hannou, opäť bez vedomia Moskvy. Americký pas konečne dostal v júli 1952. Následne bol povolaný späť do Moskvy na trojtýždňový, intenzívny,

záverečný tréning. Hanne Maki povedal, že ide služobne do Francúzska a Talianska a hranice opäť prekročil v kufri diplomatického auta. V Moskve sa učil šifrovať, dešifrovať správy a vyrábať mikrobodky. Bola mu pridelená šifra, neskôr známa ako VIC a mal sľúbené, že po čase dostane v USA jednorazové tabuľky[3]. Takisto sa zoznámil so svojím kontaktným dôstojníkom Svirinom, ktorý oficiálne pôsobil v New Yorku pri sovietskej misii v OSN. So Svirinom sa, pokiaľ to nebude nevyhnutné, nemal stretávať osobne, ale mal ho kontaktovať len prostredníctvom mŕtvych schránok. Po príchode do New Yorku mal navštevovať fínske kluby a zohnať si bývanie. Pre začiatok mu bola daná veľká voľnosť a jeho úlohou bolo len nájsť si bývanie, prácu a zabezpečiť sa tak, aby neskôr mohol budovať sieť agentov. Predbežne mal len informovať Moskvu o svojich krokoch. Po skončení posledného výcviku v Moskve bol povýšený na majora a znovu v kufri auta prepašovaný do Fínska. Hanne sľúbil, že ju dostane do USA hneď ako sa tam sám usadí a 10. októbra 1952 sa odplavil cez Štokholm a Londýn do New Yorku, kam dorazil 21. októbra. Ubytoval sa v lacnom hoteli v Harleme, spoznával mesto a zisťoval si umiestnenia určených mŕtvych schránok. Jemu určené mŕtve schránky boli dutina v múre na Jerome Avenue, lavička v Riverside parku a dutina pod pouličnou lampou vo Fort Tryon parku. To či a kde je umiestnený odkaz si agenti mali navzájom signalizovať kriedovými značkami na železnom zábradlí Macomb Dam mosta.

Maki spoznával aj New Yorský nočný život a neustále myslel na Hannu. Stal sa členom fínskeho klubu a našiel si bývanie u fínskej rodiny v Brooklyne. Prostredníctvom Svirina oznámil domov svoj príchod a poslal dar pre svoju ženu Alexu. V novembri zašifroval a poslal do Moskvy prvú správu, v ktorej žiadal $5 000 na rozbehnutie podnikania. Okrem toho sa v tejto správe pýtal na meno chemikálie potrebnej pri príprave mikrobodiek, to či dostal nejakú osobnú poštu atď. Správa bola odfotená na mikrofilme a umiestnená v dutej fínskej 50 markka minci. Túto nechal v mŕtvej schránke v Riverside parku a onedlho na to podobným spôsobom obdržal odpoveď, ktorá bola ukrytá v dutej americkej 5 centovej minci (*nickel*). Jednalo sa o veľmi známu správu, ktorú náhodou našiel chlapec predávajúci noviny a odovzdal ju polícii. Následne sa ňou zaoberala FBI a neúspešne sa ju pokúšala rozlúštiť. Šifra, ktorou bola správa zašifrovaná je známa pod menom VIC. Až omnoho neskôr, po Häyhänenovom prebehnutí, sa pomocou jeho informácií o šifre VIC a prezradení použitých hesiel, podarilo správu prečítať. Správa obsahovala len gratuláciu k jeho úspešnému príchodu do USA, informáciu o tom, že mu posielajú $3 000 na rozbehnutie podnikania a príkaz, že sa má ohľadne tohto podnikania najskôr poradiť s Moskvou a potom odpovede na jeho otázky a informáciu o tom, že dar jeho žene bol doručený.

V tomto čase už Maki pil viac než by sa patrilo a stal sa z neho alkoholik. V podstate[4] neustále myslel na Hannu a to ako ju čo najskôr dostať do USA. Každopádne ako sovietsky agent už toho pre svojich nadriadených v Moskve veľa nespravil, aj keď ich vodil za nos ešte zopár rokov. Aj spôsob akým sa FBI dostala k jeho zašifrovanej správe je charakteristický. Po dešifrovaní a prečítaní správy Maki opäť mikrofilm vložil do dutej mince a tú si dal do vrecka. Potom zrejme išiel utlmovať svoj žiaľ za Hannou pomocou vodky a ani on sám nevie čo sa stalo s mincou. Buď ju náhodou stratil, alebo ňou omylom zaplatil za noviny. Každopádne ju našiel už spomenutý chlapec predávajúci noviny, keď sa mu rozsypali drobné, jedna minca sa pritom rozpolila a vypadol z nej mikrofilm.

[3]One-Time-Pad, OTP

[4]Podľa Häyhänenových výpovedí a informácií z [4].

Peniaze, ktoré Makimu poslali z Moskvy na rozbehnutie podnikania z väčšej časti prepil a na pôvodne zamýšlaný prenájom garáže mu už nezostalo dosť. Vo februári 1953 konečne prišla za ním do USA Hanna, ktorá dostala víza ako manželka amerického občana. Maki každý druhý mesiac posielal do Moskvy správy, ktoré boli zväčša vymyslené a zavádzajúce. Už počas svojho pôsobenia vo Fínsku si totiž uvedomil, že si môže vybrať medzi agentskou kariérou a Hannou a on si vybral... Tieto informácie o Häyhänenovom agentskom pôsobení v USA pochádzajú z jeho vlastných výpovedí. Už v článku [4], z ktorého je toto prevzaté, vyslovuje autor pochybnosti o tom, že by sa Moskva tak dlho nechala zavádzať agentom, ktorý nedosahuje žiadne výsledky. Tieto pochybnosti sú samozrejme oprávnené. Na druhej strane Moskva v tom čase prejavila dosť veľkú neschopnosť vo výbere svojich agentov, čoho príkladom je aj už spomínaný agent „Big Shot". Preto sa nedá celkom vylúčiť, že ich Häyhänen skutočne mohol zavádzať.

Na jar 1953 bol Maki nútený osobne sa stretnúť so Svirinom. Postup akým sa mali stretnúť je popísaný v [4] a veľmi pripomína americké agentské filmy[5]. Takže pred Moskvou Maki predstieral budovanie agentúrnej siete a Hanne zasa naznačoval, že zdrojom jeho príjmov (zo zamestnania, v ktorom pôvodne pracoval, ho totiž medzičasom vyhodili) je obchod s drogami[6]. Na jeseň toho istého roku sa druhý a posledný raz osobne stretol so Svirinom, zrejme kvôli kontrole zo strany Moskvy. Svirin mu ako komunikačný kanál s Moskvou pridelil nového kuriéra. Bol ním fínsky námorník s prezývkou Asko, ktorý sa plavil do New Yorku 3-4 krát ročne. Maki sa s ním mal stretávať v istom kine v Brooklyne. Asko už predtým pracoval ako kuriér pre iného sovietskeho agenta, ale boli s tým problémy, pretože Asko hovoril len po fínsky. S Makim žiadne podobné problémy nehrozili. Začiatkom roku 1954 dostal Maki prostredníctvom Aska úlohu z Moskvy. Išlo o nadviazanie kontaktu s agentom, ktorý stratil kontakt na svojho riadiaceho dôstojníka. Maki mal podozrenie, že k tomuto došlo práve vďaka Askovým obmedzeným jazykovým schopnostiam.

Na jar roku 1954 došlo ku prvému kontaktu Makiho s Abelom. Plukovník Rudolf Ivanovič Abel, vlastným menom Viliam Henrichovič Fišer, sa narodil v roku 1903 vo Veľkej Británii. Jeho rodičia boli ruskí emigranti, pôvodom etnickí nemci a presvedčení komunisti. Z Ruska utiekli pred cárskou políciou. Fišer sa v roku 1920 vrátil do Sovietskeho zväzu, slúžil v armáde a neskôr pracoval v spravodajských službách. Od roku 1948 pracoval ako tajný agent v USA a úspešne budoval agentúrnu sieť. V čase Makiho pôsobenia v USA sa blížil ku 60-tke a tešil sa na ukončenie svojho pôsobenia v USA a skorý návrat domov k manželke a dcére. Agent „Big Shot", ktorého mu z Moskvy poslali bol preňho veľkým sklamaním, a preto vkladal nádeje do nového agenta. S Makim sa stretol po prvý raz na 1. mája 1954 v kine na Long Islande. Krycie meno Makiho bolo Vic (Victor) a krycie meno Abela bolo Mark. Abel sa mal s Makim pravidelne stretávať, zabezpečiť jeho ďalší výcvik, dohliadať naňho a vyplácať mu plat majora. S Makim sa dohodol na stretnutiach minimálne raz týždenne.

Abelov počiatočný dojem z Makiho bol dobrý. Považoval ho len za neskúseného a príliš opatrného, čomu prisudzoval to, že Maki zatiaľ nezískal žiadnych ďalších agentov. Maki sa Abelovi sťažoval, že z Moskvy nedostal dosť peňazí na rozbehnutie podnikania. Abel mu prisľúbil, že ak sa zdokonalí vo fototechnike, tak mu pomôže so zriadením vlastného fotoateliéru[7]. Dovtedy ho používal ako svojho pomocníka a šoféra, s úmyslom

[5]Zrejme nie všetko si v Holywoode vymýšlajú.

[6]Skutočne originálna výhovorka, ale v 50-tych rokoch sa zrejme drogy nebrali tak vážne ako dnes.

[7]Fotografovanie bolo Abelovým koníčkom a ako svoje krytie využíval práve fotoateliér.

Obr. 2: Rudolf Ivanovič Abel (* 11. 7. 1903 – † 15. 11. 1971) [7]

preveriť si jeho schopnosti. Toto sa dialo v rokoch 1954 a 1955. Jednou z prvých Makiho úloh bolo napr. sledovanie istého agenta, ktorému Moskva nedôverovala. Ďalšou úlohou pre Makiho bolo pátranie po agentovi s krycím menom Quebec. Bol to bývalý zamestnanec americkej armády. Nejaký čas pôsobil na ambasáde v ZSSR a tam bol prinútený k spolupráci pomocou kompromitujúcich materiálov. Po návrate do USA sa ale stiahol a prerušil kontakty s Moskvou. Pôvodne dostal za úlohu pátranie po Quebecovi Abel a mal ho prinútiť k opätovnej spolupráci. Abel tým nebol nadšený a už z princípu nepovažoval za dobrý základ spolupráce vydieranie kompromitujúcimi materiálmi. Keďže ale Moskva trvala na nájdení Quebeca, presunul Abel túto úlohu na Makiho. Maki dostal od Abela tri týždne voľna na cestu na západ a pátranie po Quebecovi. Okrem toho mal po ceste v oblasti Chicaga a Detroidu zistiť informácie o (pravdepodobne) vojenských zariadeniach. Maki sa vrátil krátko pre Vianocami v podstate bez akýchkoľvek výsledkov. Akurát pomocou telefonátu Quebecovej rodine zistil jeho údajnú adresu v Arizone. V tom čase už Abel zastával názor, že Maki je kompetentný len v prípade, že dostane konkrétnu úlohu a jasné inštrukcie, ale že je neschopný, pokiaľ sa veci nechajú na jeho úsudok a iniciatívu. Naviac Abel vedel o Makiho probléme s alkoholom a zrejme sa nejako dozvedel aj o Hanne. Preto mu už od roku 1955 prideloval len jednoduché úlohy. Počas roku 1955 sa Abel chystal na plánovanú cestu do Moskvy. Tam mal svojím nadriadeným podať správu o Makim. Mienil im povedať, že Maki sa hodí za asistenta, ale nie ako jeho náhrada v USA a chcel žiadať aby rýchlo našli ďalšieho kandidáta na túto funkciu, pretože nechcel predlžovať svoj pobyt v USA.

Abel plánoval opustiť USA najneskôr koncom júna 1955. Predtým dal Makimu zaria-

denie a peniaze na zriadenie sľúbeného fotoateliéru. Tesne pred odchodom dostal Abel z Moskvy príkaz, doručiť $5 000 Helene Sobellovej. Bola to manželka Mortona Sobella, ktorý bol odsúdený na 30 rokov za špionáž pre ZSSR. Nebola to jednoduchá úloha, pretože Helena Sobellová bola sledovaná. Abel peniaze dal do dvoch plechoviek a spolu s Makim bol tieto plechovky schovať v Bear Mountain parku. Maki dostal za úlohu kontaktovať Helenu Sobellovú a dať jej podrobné informácie o umiestnení peňazí. Abel aj vymyslel spôsob ako má nepriamo kontaktovať Helenu Sobellovú a dal Makimu jasné príkazy. Potom odcestoval cez Mexiko, Paríž a Viedeň do Moskvy. V Moskve podal Abel správu o nedokončených akciách, podarilo sa mu presvedčiť svojich nadriadených aby nechali na pokoji Quebeca a nesnažili sa ho nútiť ku spolupraci, ale jeho správa o Makim nepola prijatá s pochopením. U nadriadených Abel nebol príliš obľúbený pre svoju priamočiarosť a jeho hodnotenie Makiho pripisovali jeho skostnatelosti a profesionálnej žiarlivosti. Napokon sa dohodli na takom kompromisnom riešení, že Abel po návrate do New Yorku bude Makiho nejaký čas tajne sledovať. Ešte počas Abelovho pobytu v Moskve prišla správa od Makiho, že peniaze Helene Sobellovej boli doručené.

V roku 1956, po svojom návrate do New Yorku, nechal Abel sledovať Makiho. Jeho agenti rýchlo zistili, že si prenajal priestory na fotoateliér a zriadil účet v banke, ale nepodnikol žiadne ďalšie kroky. Okrem toho zistili, že žije s Hannou ako s manželkou a takmer vždy keď niekam ide, ho Hanna sprevádza. V susedstve mali zlú povesť, boli považovaní za pijanov a kolovaly chýry, že Maki je zapletený aj v obchode s drogami. Naviac Maki nebol členom žiadneho fínskeho klubu ako mal prikázané a nevykazol ani žiadnu inú agentskú činnosť. Abel o týchto zisteniach podal v apríli 1956 správu do Moskvy. Medzitým sa Helena Sobellová pýtala Moskvy, kde je jej sľúbených $5 000. Toto ešte viac utvrdilo Abela v jeho podozreniach voči Makimu. Z Moskvy dostal pokyn vyšetriť ako vlastne Maki doručil peniaze. Abelovi agenti zistili, že Maki si v inkriminovanom čase kúpil dom. Abel navrhol Moskve poslať Helene Sobellovej nových $5 000 a Makiho povolať do Moskvy, aby tam vysvetlil kde získal peniaze na kúpu domu. Moskva už bola opatrnejšia, ale ešte stále neverila obvineniam voči Makimu. Svirin, ktorý sa plánoval v októbri vrátiť do Moskvy mal tieto obvinenia opäť preveriť. Zatiaľ mal Abel kontaktovať Makiho a pokračovať s ním v spolupráci ako predtým.

V októbri Svirin napokon svojou správou presvedčil Moskvu o pravdivosti obvinení voči Makimu. V Moskve sa rozhodli Makiho sťiahnuť. Abel by ho bol najradšej poslal domov čo najskôr a rovnakou trasou cez Mexiko akú používal aj on. To bola najbezpečnejšia trasa, pretože nevyžadovala pas. Maki zrejme tušil problémy a svoj odchod pod rôznymi zámienkami odkladal. Abel, v snahe zmierniť Makiho podozrenia, mu povedal, že obdržal z Moskvy správu o jeho plánovanom povýšení na podplukovníka. Napokon 24. apríla 1957 Maki odplával loďou Liberté. 30. apríla loď zakotvila v Le Havre a Maki/Häyhänen odcestoval do Paríža. Tam sa 2. mája podľa inštrukcií telefonicky hlásil na sovietskom obchodnom zastupiteľstve. 3. mája sa stretol na stanici metra s agentom, od ktorého dostal ďalšie pokyny. Mal odcestovať vlakom do Mníchova a odtiaľ lietadlom do západného Berlína. Následne mal prejsť do východného Berlína a tam mal telefonicky kontaktovať istého (fiktívneho) pána Wojcheka. Naposledy sovietski agenti videli Häyhänena večer 3. mája v Paríži, kde podľa dohody prešiel ulicou Victora Huga a nemal vo vrecku noviny, čo bolo dohodnuté znamenie, že všetko je v poriadku a bude podľa dohody pokračovať v ceste do Berlína. Ale 5. aj 6. mája márne čakal pán Wojchek v Berlíne na telefonát. Dôstojníci KGB v Európe pátrali po Häyhänenovi, ale kým zistili čo sa stalo, bol už mimo ich dosah.

Häyhänen namiesto toho, aby odišiel podľa pokynov do Mníchova a odtiaľ do Berlína, kontaktoval 6. mája americké veľvyslanectvo. Pracovníkovi spravodajskej služby porozprával svoj príbeh a žiadal, aby ho urýchlene dostali späť do USA k jeho žene. Američania po prvotnom šoku a overení si základných údajov, ho 9. mája posadili do lietadla a dopravili späť do USA. Maki/Häyhänen poznal svojho šéfa len pod krycím menom Mark a nevedel kde v Brooklyne býva, ani kde je jeho fotoateliér. Z rozhovorov s Abelom ale vedel o jeho fotoateliéri dosť podrobností na to, aby ho američania podľa nich boli schopní identifikovať a začali ho sledovať. Po tom čo Moskva varovala Abela, že jeho bývalý pomocník zmizol v Paríži, zmizol aj Abel alias Emil Goldfus. Namiesto neho sa istý Martin Collins presúval z hotela do hotela a chystal sa opustiť krajinu. Pred odchodom sa ale rozhodol odstrániť nejaké kompromitujúce materiály, nachádzajúce sa v jeho fotoateliéri, čo sa mu stalo osudným. Ráno 21. júna 1957 zatkli Abela/Goldfusa/Collinsa v hoteli. Pri vyšetrovaní neprehovoril. Počas súdu proti nemu vypovedal Häyhänen/Maki. Odsúdený bol na 45 rokov za špionáž a trest si odpykával v Atlantskej federálnej väznici v Giorgi. V čase písania článku [4] bol Abel stále vo väzení. Zo svojho trestu si ale odsedel len 4 roky, pretože 10. februára 1962 ho Moskva vymenila za zajatého pilota špionážneho lietadla U-2, Garyho Powersa.

Podobne ako Abela, prezradil Häyhänen američanom aj Svirina, ktorého poznal pod krycím menom Michail. Ten však už koncom roku 1956 odcestoval do Moskvy.

Literatúra

[1] Kahn David: The Codebreakers (str. 668-671)
Scribner, 1996

[2] Kahn David: Number One from Moscow
CIA Historical Review Program – odtajnené 1993

[3] Kahn Jeffrey: The Case of Colonel Abel
Journal of National Security, Law & Policy, June 2010

[4] Rocafort W. W.: Colonel Abel's Assistant
CIA Studies in Intelligence, Vol. 3, Issue: Fall, 1959 – odtajnené 1994

[5] Wikipedia: Rudolf Abel
`http://en.wikipedia.org/wiki/Vilyam_Genrikhovich_Fisher`

[6] Wikipedia: Reino Häyhänen
`http://en.wikipedia.org/wiki/Reino_Häyhänen`

[7] Fotografia: Rudolf Abel
`http://www.sueddeutsche.de/politik/spionage-im-kalten-krieg-im-dienst-des-gegners-1.972117-6`

[8] Fotografia: Reino Häyhänen
`http://madamepickwickartblog.com/2013/01/the-secret-agent-bumblers/`

B. Dosud nevyluštěný dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché z doby třicetileté války. (Soutěž o ceny)

Jakub MÍRKA, SOA Plzeň, mirka@soaplzen.cz

Když jsem se s Pavlem Vondruškou na podzim minulého roku domlouval na publikování svého článku o šifrované korespondenci uložené ve Státním oblastním archivu v Plzni,[1] slíbil jsem mu, že v budoucnu na stránkách Crypto-Worldu uveřejním též některé dosud nedešifrované ani nevyluštěné raně novověké šifrované dopisy, na něž jsem narazil při pátrání po šifrách v našem nebo v některých jiných archivech.

Jak jsem uvedl již ve výše zmíněném článku, v našich archivech převládají spíše dopisy, které částečně či úplně dešifrovali již jejich adresáti. Přesto se však mezi nimi najdou i takové, které dosud dešifrovány nebyly. Z nich jsem vyloučil ty, které jsou šifrovány pomocí jednoduché substituce a které by luštitelsky zdatní čtenáři Crypto-Worldu jistě hravě rozlouskli, a ty, jež jsou evidentně šifrovány převážně pomocí kódů, jejichž luštění je naopak obvykle extrémně náročné a bez znalosti dobových reálií téměř nemožné. Nakonec mi zbyl malý vzorek několika šifer, které se zdály být vhodné pro luštitelskou soutěž. Mezi nimi jsem se bez většího rozmýšlení rozhodl pro dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché hesensko-kasselské adresovaný lantkraběnce Amálii Alžbětě z roku 1646, který je součástí písemné pozůstalosti Maxmiliána z Trauttmansdorffu v archivním fondu Rodinný archiv Trauttmansdorffů, uloženém na pracovišti Klášter u Nepomuka Státního oblastního archivu v Plzni.[2] Tento dopis, který jsem vybral především s ohledem na osobu jeho pisatele, byl zachycen katolickou stranou, a tak k adresátce nikdy nedoputoval a nemohl být 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 čeká právě na čtenáře Crypto-Worldu. Jeho reprodukci najdete na obrázku č. 1.

Ještě před začátkem soutěže musím poctivě říct, že v současné době nejsem schopen zodpovědně stanovit obtížnost této šifry. Na základě letmého průzkumu počtu a podoby znaků jsem dospěl k závěru, že pravděpodobně půjde o homofonní substituční šifru. Vzhledem k výskytu trojciferných číslic v šifrové abecedě se také domnívám, že šifra bude obsahovat i kódy. Nelze vyloučit ani užití bigramů. Zde však upozorňuji na to, že oba tyto závěry jsou pouhými neověřenými domněnkami. Ze své vlastní zkušenosti považuji takový typ šifer za velmi obtížně luštitelný, zvláště když se dochoval tak krátký text, jako je tomu v tomto případě. Potíže pravděpodobně bude činit i to, že Rabenhauptovy dopisy jsou psány němčinou, která se v mnoha okolnostech liší od současné pravopisné podoby. O to netrpělivěji budu očekávat výsledky soutěže, od níž si slibuji, že nám ukáže, nakolik tyto šifry byly bezpečné nebo spíše nakolik jsou bezpečné z hlediska dnešních znalostí. Já osobně se

---

[1] MÍRKA Jakub. Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni, část I. Crypto-World, sešit 11–12/2012, s. 12–28; *totéž, část II.*,Crypto-World, sešit 1–2/2013, s. 2–12; *totéž, část III.*, Crypto-World, sešit 3–4, s. 2–14.

[2] SOA v Plzni, pracoviště Klášter, Rodinný archiv Trauttmansdorffů, inv. č. 125.

domnívám, že jejich luštění bude velmi obtížné i za pomoci moderní výpočetní techniky a že počet úspěšných luštitelů nebude nijak vysoký. Upozorňuji tedy, že zapojení do luštitelské soutěže je pouze na vlastní nebezpečí a úspěch nelze zaručit ani u těch nejzdatnějších kryptoanalytiků z řad čtenářů Crypto-Worldu. Mohu se ale mýlit a počet řešitelů nakonec může být alespoň z mého pohledu nečekaně vysoký.

Ještě více než počet úspěšných luštitelů nás ale bude zajímat samotný způsob řešení. Jeho zaslání je tedy také podmínkou úspěšného řešení. Přitom je třeba dodat, že v případě, že by skutečně šlo o homofonní substituční šifru doplněnou o kódy, ke splnění úkolu samozřejmě postačí, když se luštiteli podaří odhalit převodní tabulku pro homofonní substituci či v rámci možností její převážnou část, nikoli už jednotlivé kódy, které by si většinou mohl pouze domýšlet.

KAREL RABENHAUPT ZE SUCHÉ

Dříve než se budeme zabývat samotným šifrovaným dopisem, považuji za užitečné čtenáře blíže seznámit alespoň ve stručnosti s osobou jeho odesilatele. Ačkoli Karel Rabenhaupt ze Suché pocházel z Čech, jeho jméno je u nás dnes téměř neznámé. Jinak je tomu ovšem v Nizozemí a především v Groningenu, kde je po něm pojmenována ulice (podobně jako v některých dalších městech v severní části Nizozemí), kavárna, střelecký spolek, kapela dechové hudby, klub deskových her ad. V Groningenu také v minulosti stály Rabenhauptovy kasárny, které vyhořely roku 1945, a centrum města zdobí jeho pamětní deska a busta. Nizozemský badatel Wilken Engelbrecht označil Karla Rabenhaupta ve Sborníku příspěvků IV. setkání genealogů a heraldiků za zdaleka nejdůležitějšího Čecha pro jeho vlast. Abychom pochopili, proč tomu tak je, bude třeba se krátce seznámit s jeho životními osudy. To nám také alespoň zčásti pomůže zasadit předložený šifrovaný dopis do širších historických souvislostí.[3]

Karel Rabenhaupt[4] ze Suché se narodil dne 8. ledna 1604[5] v Třemošnici poblíž Čáslavi jako jeden z minimálně pěti synů Zikmunda Rabenhaupta (Robmhápa) ze Suché a Kateřiny, rozené Žehušické z Nestajova.[6] O jeho mládí toho příliš

---

[3] Níže uvedená pasáž článku o Rabenhauptově životě je převážně převzata z uvedeného článku Wilkena Engelbrechta. ENGELBRECHT, Wilken. Flüchtling im fremden Lande. Weissenberger Exulanten in niederländischen Quellen. In. *Sborník příspěvků IV. setkání genealogů a heraldiků. Ostrava 14.–15. 10. 1989*. Ostrava 1992, s. 13–18. Na některých místech je doplněna o informace z dalších zdrojů. BÍLEK, Tomáš V. *Dějiny konfiskací v Čechách po r. 1618*. Praha 1882, s. 461–462; POTEN, Bernhard von. Karl Freiherr Rabenhaupt von Suche oder Sucha. In. *Algemeine Deutsche Biographie. Siebenundzwanzigster Band*. Leipzig 1888, s. 85–87 (dostupné z http://www.deutsche-biographie.de/index.html); *Ottův slovník naučný. XXI. díl*. Praha 1904, s. 864–865; http://www.30jaehrigerkrieg.de/rabenhaupt-karl-freiherr-rabenhaupt-von-sucha-3/ (internetové stránky Bernarda Warlicha k třicetileté válce – stav k 7. 8. 2013). Uvedené práce obsahují odkazy na další související prameny a literaturu.

[4] Česká podoba jména obvykle zní „Robmháp ze Suché“. V článku jméno ponechávám v německém tvaru především z toho důvodu, že tohoto tvaru po většinu svého života v cizině používal sám Karel Rabenhaupt a pod ním je také obvykle uváděn, a též z toho důvodu, že samotný tvar Robmháp vznikl až počeštěním původně německého jména Rabebhaupt (tj. havraní hlava), které se odráží i ve znaku rodu.

[5] Někdy se též uvádí 3. ledna 1604 nebo 6. ledna 1602. Přikláním se k dataci uvedené Wilkenem Engelbrechtem s odvoláním na informaci Františka Chocholatého. ENGELBRECHT, Wilken. Flüchtling im fremden Lande. Weissenberger Exulanten in niederländischen Quellen. In. *Sborník příspěvků IV. setkání genealogů a heraldiků. Ostrava 14.–15. 10. 1989*. Ostrava 1992, s. 17 (pozn. č. 44).

[6] Údaj opět převzat z výše citovaného článku Wilkena Engelbrechta. Tamtéž, s. 14. Jindy je uváděno, že Kateřina byla rozená Chuchelská z Nestajova. Viz např. http://patricus.info/Rodokmeny/Rabenhaupt.txt (stav

nevíme. Byl vychován ve víře pod obojí a roku 1620 se podílel na obraně Budyšína proti armádě saského kurfiřta Jana Jiřího. Po porážce stavovských vojsk na Bílé hoře odešel kvůli své víře z vlasti a roku 1622 přišel prakticky bez prostředků s Petrem Arnoštem II. Mansfeldem do Nizozemí, kde byl představen princi Mořici Oranžskému. Ten ho přijal do své tělesné gardy a umožnil mu studovat pevnostní stavitelství na univerzitě v Leidenu. Ve druhé polovině dvacátých let 17. století bojoval v nizozemském vojsku. Roku 1627 se vyznamenal při obléhání Groenlo a byl povýšen do hodnosti poručíka.

Později se ve vojenských službách natolik proslavil, že mu prý roku 1633 přijetí do svých služeb nabídl princ Radziwiłł, ale Rabenhaupt vstoupil do služeb hesensko-kasselského lantkraběte Viléma V. Zde snad zpočátku působil jako stavitel pevností, ale již roku 1633 byl uváděn jako velitel Schaarkopfova jízdního pluku. Roku 1637 zemřel lantkrabě Vilém V. a vlády se jako regentka dosud nezletilého syna Viléma VI. ujala lantkraběnka Amálie Alžběta. Roku 1639 se Rabenhaupt oženil s Annou Margaretou von Meerfeld. V té době již byl vlastníkem dvora v městečku Weinheim. Tento dvůr stojí dodnes a stále nese jméno Rabenhaupt´scher Hof. Na Rýně bojoval minimálně od roku 1640 a roku 1641 je uváděn jako vrchní velitel hesenských vojsk na jeho levém břehu. Na obou březích Rýna pak bojoval po většinu čtyřicátých let 17. století. Přitom minimálně od roku 1644 bylo jeho základnou Neuss poblíž Düsseldorfu, odkud podnikal rozličné výpady a odkud o dva roky později zaslal lantkraběnce Amálii Alžbětě šifrovaný dopis, který je předmětem tohoto článku. V září roku 1645 Alexandre de Bournonville zaslal zprávu o boji s Rabenhauptem z polního tábora u Ulmu. Roku 1646, z nějž pochází uvedený šifrovaný dopis, jsou o Rabenhauptovi zprávy již z února, kdy obsazoval četné statky v okolí Jülichu a Bergu. Počátkem března už se prý nacházel na druhém břehu Rýna poblíž Wipperfürthu. Dále víme, že minimálně v červenci se zdržoval v Neuss a že poblíž operovala armáda francouzského maršála vikomta de Turrene.[7] Koncem září již Rabenhaupt obléhal Zons a během října se měl dostat až do Weselu. V dubnu 1647 byl opět v Neuss. Obdobným způsobem pravděpodobně probíhala větší část jeho působení na Rýně ve čtyřicátých letech. Šlo zřejmě o velké množství různých taktických přesunů, obléhání měst a pevností či menších bitev se střídavými úspěchy. Dá se tedy očekávat, že v šifrovaném dopise lantkraběnce Amálii Alžbětě nejspíše popisuje aktuální situaci na bojišti. Nakolik závažná ta sdělení byla, ale budeme moci konstatovat, až pokud se dopis podaří rozluštit.

Po uzavření Vestfálského míru vystoupil Rabenhaupt z armády, rozšířil své majetky ve Wenheimu a koupil statek Fränkisch-Crumbach. Jeho žena zemřela roku 1669. Po její smrti prý dokonce poprvé od svého odchodu navštívil Čechy, v nichž mu bratr Ferdinand, který přestoupil ke katolické víře a který zemřel roku 1659, doživotně odkázal výnosy ze svých statků za předpokladu, že by Karel rovněž konvertoval ke katolictví. To však neučinil. Roku 1670 se oženil Marií Dorotheou von der Recke von der Horst.

Jak uvádí Wilken Engelbrecht, roku 1672 přišla jeho „hvězdná hodina“, za niž mu bude nizozemský lid navždy vděčný. Toho roku začala francouzsko-nizozemská

---

k 7. 8. 2013), kde lze najít i rodokmen Rabenhauptů ze Suché.

[7] SOA v Plzni, pracoviště Klášter, Rodinný archiv Trauttmansdorffů, inv. č. 125 (opis nešifrovaného dopisu z 13. července 1646).

válka a během několika měsíců byla obsazena polovina země. Severní provincie nemohly očekávat žádnou pomoc a musely se spoléhat na své vlastní síly. V té době nabídla nizozemská provincie Groningen Rabenhauptovi vrchní velení, což byla dle sdělení Wilkena Engelbrechta nejvyšší pozice, jakou kdy nějaký cizinec ve svobodném Nizozemí zastával. Rabenhaupt nejen dokázal ubránit Groningen proti desetkrát silnějšímu münsterskému vojsku, ale též obklíčení prorazit a dobít zpět jednu z nejmodernějších a nejsilnějších pevností své doby, Coevorden. Tím prakticky zachránil severní část země a umožnil stavům intenzivněji napřít své síly proti Francii. Za to byl jmenován starostou Groningenu a počátkem roku 1673 správcem kraje Drenthe a pevnosti Coevorden. Když pak byl roku 1673 převelen na jižní frontu, stěžovali si stavy kraje Drenthe, že byly jeho jmenováním do těchto funkcí obejity. Generální stavy jim sice daly za pravdu, ale Rabenhaupt pro ně byl natolik důležitý, že byl ve funkci ponechán. Roku 1673 byl také povýšen do stavu svobodných pánů. Zemřel bezdětný 12. srpna 1675. Jeho přítel, jezuita Jan Michgorius, nad ním pronesl šestihodinovou smuteční řeč a groningenské stavy mu nechaly vystavět honosnou hrobku, která však byla roku 1796 zničena. Roku 1922, tedy 250 let po jeho velkém vítězství, mu však město Groningen nechalo vztyčit pamětní desku. Největším vyznamenáním pro něj ale zřejmě je, že dodnes žije v povědomí nizozemského lidu.

ŠIFROVANÝ DOPIS LANTKRABĚNCE AMÁLII ALŽBĚTĚ

Dne 20. července odeslal císařský vojevůdce Alexandre de Bournonville z města Hammu Maxmiliánovi z Trauttmansdorffu, nejvyššímu hofmistrovi císaře Ferdinanda III., do Münsteru dopis (viz obr. č. 3), k němuž přiložil opisy dvou listů velitele hesenských vojsk Karla Rabenhaupta ze Suché adresovaných hesensko-kasselské lantkraběnce Amálii Alžbětě. Tyto dopisy byly zachyceny u Arnsbergu a jeden z nich byl šifrovaný (šifrovaný dopis viz obr. č. 1, nešifrovaný viz obr. č. 2). Bournonville Trauttmansdorffovi sděloval, že se mu šifrovaný dopis nepodařilo vyluštit a že mu zasílá jeho opis pro případ, že by v Münsteru, kde Trauttmansdorff působil jako hlavní císařský vyjednavač na mírových jednáních, potkal nějakého šťastlivce, který by snad mohl znát klíč. Sám Bournonville si asi byl vědom, že by mohlo jít jen o velmi šťastnou náhodu, a nic nenasvědčuje tomu, že by dopis byl nakonec dešifrován či rozluštěn.

Oba zmiňované dopisy byly napsány v Neuss poblíž Düsseldorfu a oba byly psány německy. Nešifrovaný dopis byl datován 13. července 1646, zatímco datace šifrovaného dopisu je nejistá. V jeho opisu, který byl zaslán Trauttmansdorffovi, je uvedeno datum 11. nebo 13. června 1646. Druhá číslice v číslovce označující den je totiž přepsaná, a to pravděpodobně tak, že původní číslice „11“ byla přepsána na „13“. Pozdější archivní datace uvedená v levém horním rohu dokonce dopis datuje 18. června 1646, ale tato varianta se zdá být ze všech ostatních nejméně pravděpodobná.

Pokud bychom zůstali u datace 13. (případně 11.) června 1646, bylo by trochu zarážející, že by Bournonville Trauttmansdorffovi zasílal k případnému dešifrování dopis, který by byl již více než měsíc starý. Samozřejmě to nelze vyloučit, ale na druhou stranu se dá očekávat, že by se snažil získat informace co nejdříve od zachycení dopisu, aby nezastaraly. Navíc Bournonville uváděl, že oba dopisy byly zachyceny u Arnsbergu. Není příliš pravděpodobné, že by byl jeden dopis zachycen na jednom místě a druhý pak o měsíc později tamtéž. Přijatelnější variantou se zdá být, že oba dopisy byly součástí jedné zásilky. To by se snad dalo vysvětlit tím, že se Bournonvillův písař mohl při opisování dopisu přepsat a omylem zaměnit červenec

(Juli) za červen (Juni), a tak dopis mohl ve skutečnosti vzniknout o měsíc později. Tuto domněnku by mohl potvrzovat především fakt, že sám Rabenhaupt se v nešifrovaném dopise z 13. července zmiňuje o listu, který odeslal 11. téhož měsíce, tedy před pouhými dvěma dny. V něm prý vyslovil domněnku, že křik, který bylo zdáli slyšet, pochází od stahující se armády vikomta de Turenne. V dopise ze 13. července ale upřesňuje, že tento křik ve skutečnosti pocházel od koní Turennova dělostřelectva, kteří utonuli v Mosele. To svádí k domněnce, že šifrovaný dopis by mohl teoreticky být právě oním dopisem z 11. července. Pokud by tento předpoklad byl správný, mohla by snad informace o obsahu jedné části šifrovaného dopisu usnadnit i samotné luštění. S jistotou však zmiňovaný dopis z 11. července s šifrovaným dopisem, který máme k dispozici, ztotožnit nemůžeme. Další teoretickou možností je, že písařova oprava z „11." na „13." je správná a že se mohl splést pouze v měsíci. Takový dopis by pak mohl být vyhotoven až po nešifrovaném dopise, ale ve stejný den, jako reakce na nově zjištěné skutečnosti a jako doplnění dopisu předchozího. Tím by se dal ještě lépe vysvětlit již zmiňovaný fakt, že oba dopisy byly pravděpodobně obsahem jedné zásilky. Další možností samozřejmě zůstává, že se písař v dataci nespletl a dopis skutečně pocházel z června. Na tyto otázky budeme pravděpodobně schopni uspokojivě odpovědět až po případném rozluštění šifrovaného dopisu.

Vzhledem k tomu, že se domnívám, že tento úkol nebude jednoduchý, dohodli jsme se, že pro účastníky soutěže bude připravena nápověda. Ne všichni totiž musejí být vždy sběhlí v raně novověké paleografii, a tak těm řešitelům, kteří se do soutěže zaregistrují, bude zaslán přepis jak celého Rabenhauptova dopisu, který nebyl šifrován, tak těch pasáží šifrovaného dopisu, které jsou psané otevřeným textem. Nešifrovaný dopis předkládáme především pro představu o „pravopisu" či o způsobu psaní dopisů v té době. Přitom je však třeba mít na vědomí, že ne vždy bylo při psaní otevřeného a šifrového textu užíváno zcela totožného „pravopisu". Ačkoli samotné přepisy dostanete až po registrování se do soutěže, informace k těmto textům předkládáme již na tomto místě.

Při přepisu těchto textů bylo postupováno metodou transliterace (tj. věrným přepisem jednotlivých písmen) a přepsaný text nebyl až na malé výjimky, které nemají vliv na samotné luštění, přizpůsoben současnému pravopisu. Jednou z uvedených výjimek je například slučování slov, která se v moderní němčině obvykle píší dohromady, ale ve starších dobách se mohla psát i zvlášť. Ne vždy je totiž evidentní, zda jsou slova oddělena, či ne (např. slovo na řádce č. 6 nešifrovaného dopisu přepisuji ve tvaru „Grabengeschütz", nikoli „Graben Geschütz"). Dále byl současný pravopis zohledněn při psaní velkých a malých písmen. V originálu také nejsou užívána diakritická znaménka pro přehlásky, ovšem v přepisu doplněna jsou. Zde je však třeba upozornit na to, že v šifrovém textu z této doby se obvykle neužívá odlišných šifrových znaků pro samohlásku bez přehlásky a pro samohlásku s přehláskou. Šifrový text obvykle užívá pro obě stejný šifrový znak anebo (a možná častěji) přepisuje šifrované slovo foneticky (např. místo „Geschütz" se užije podoby „Geschitz" či „Geschiz"). Naopak předložka „zu" byla v této době oproti současnému pravopisu na konci věty obvykle psána dohromady s infinitivem, což je zachováno i v přepisu. Písmeno „ß" je ponecháno všude, kde je užit podobný grafický znak, a to i v případech, že se v tomto slovu obvykle nepsalo ani před zavedením nového německého pravopisu (např. slovo „alß" na řádce č. 28). V šifrové abecedě se ale podobně jako v otevřeném textu obvykle mezi písmeny „s" a „ß" nerozlišovalo. Zkratky jsou obvykle rozepsány do hranatých závorek. Hranatými závorkami jsou označena též slova, jejichž přepisem jsem si nebyl jistý. Některé pasáže dopisu jsou hůře čitelné, a tak nelze vyloučit, že při přepisu mohlo dojít

k drobným chybám. Ty by však neměly výraznějším způsobem ovlivnit výslednou podobu textu. Bylo zachováno umístění slov na řádkách, tak jak jsou vidět na reprodukci. U nešifrovaného dopisu byla očíslována každá pátá řádka, u přepisu pasáží ze šifrovaného dopisu jsou čísla řádek uvedena u každé pasáže otevřeného textu. Tři tečky naznačují, že na stejné řádce se nachází šifrovaný text před nebo za textem otevřeným.

Těm čtenářům, kteří se dosud nesetkali s historickými šiframi v této podobě, by snad mohl být užitečný článek o raně novověké šifrované korespondenci ve Státním oblastním archivu v Plzni, který jsem publikoval ve třech částech na stránkách Crypto-Worldu a v němž jsem se pokusil o alespoň základní uvedení do problematiky.[8] Především by pak mohla být prospěšná jeho třetí část. V tomto článku lze nalézt také odkazy na další užitečnou literaturu. Zároveň bych čtenářům doporučil internetové stránky věnované vyluštění Codexu Copiale, na nichž je uveden i přesný postup luštění šifry užité v tomto kodexu (http://stp.lingfil.uu.se/~bea/copiale/). Ta sice pochází z jiné doby a její systém bude patrně poněkud odlišný od systému Rabenhauptovy šifry, přesto se domnívám, že určité zde představené postupy mohou být do jisté míry velmi užitečné i při jejím řešení. Výčet další užitečné literatury by mohl být určitě mnohem delší, ale zde už nechám pátrání na samotných řešitelích.

Na závěr už chci jen popřát všem účastníkům soutěže pevné nervy, trochu toho štěstí a především dobrou zábavu!

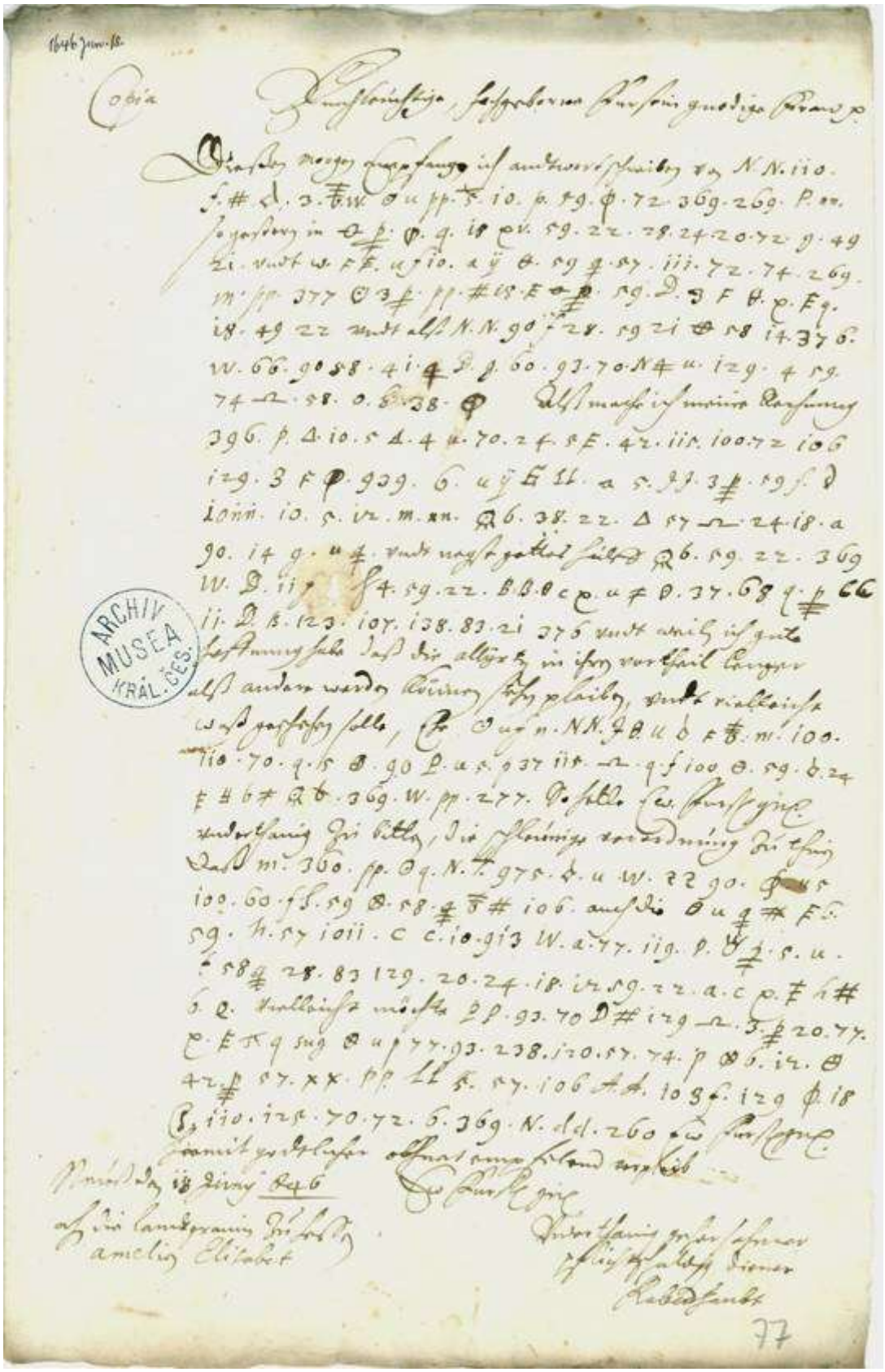
Následující tři obrázky / dopisy si můžete stáhnout v lepší kvalitě ze stránky věnované letošní soutěži:

Obr. č. 1 – 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

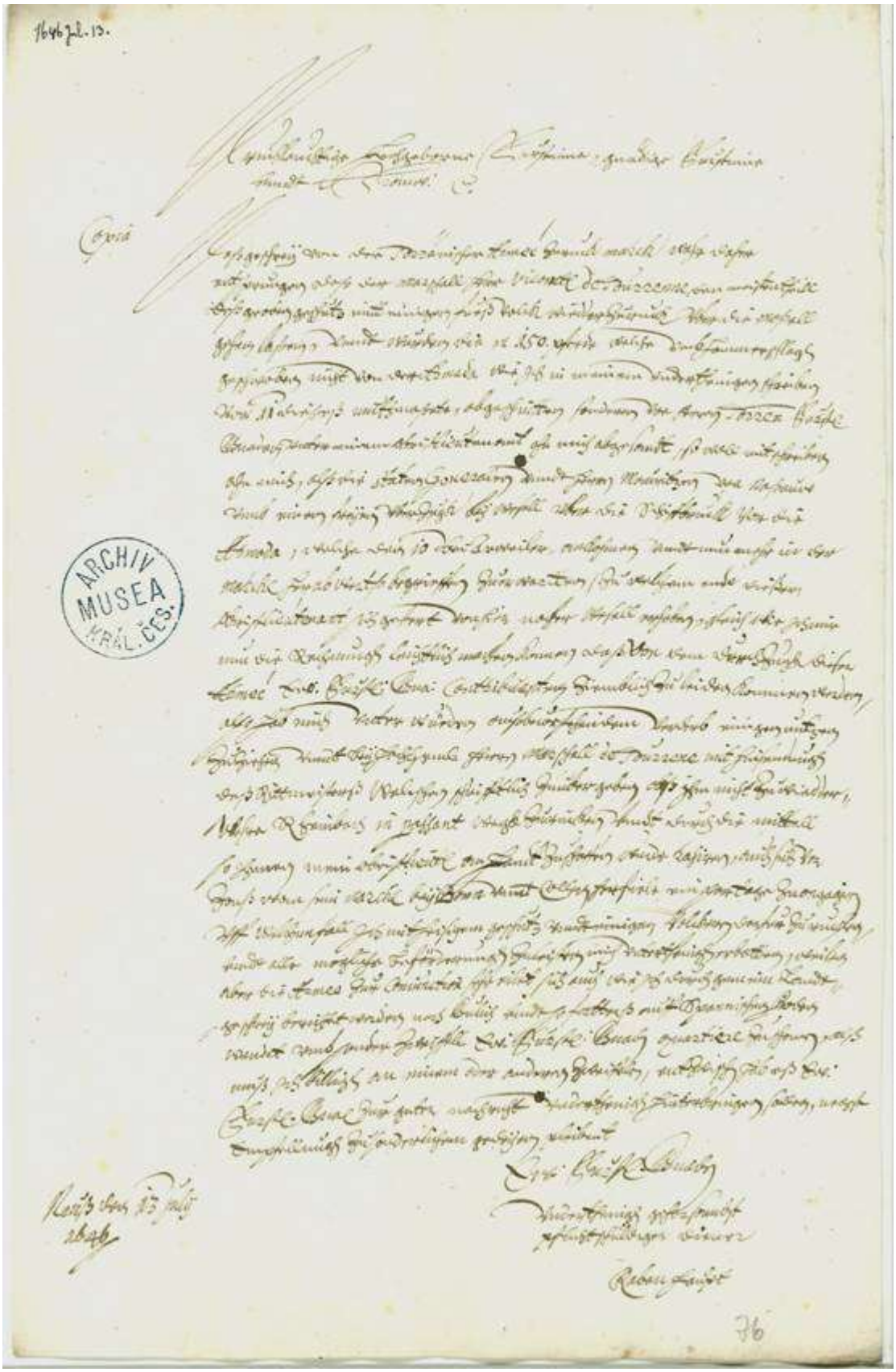
Obr. č. 2 – Opis nešifrovaného dopisu Karla Rabenhaupta ze Suché zaslaného lantkraběnce Amálii Alžbětě 13. července 1646. *SOA v Plzni, pracoviště Klášter, Rodinný archiv Trauttmansdorffů, inv. č. 125.*
http://soutez2013.crypto-world.info/dopisy/obr2.jpg

Obr. č. 3 – 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.*
http://soutez2013.crypto-world.info/dopisy/obr3.jpg

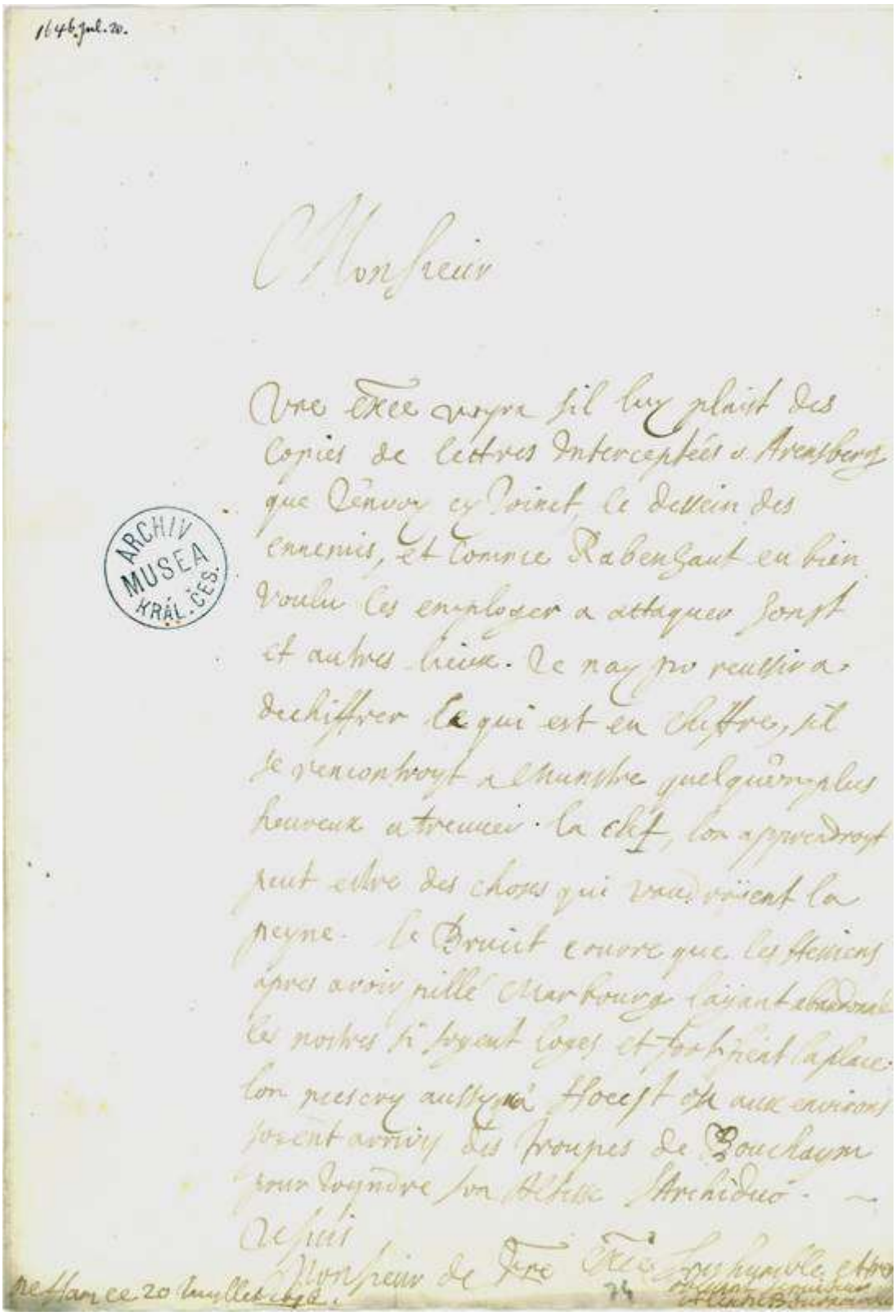
[8] Viz pozn. č. 1.



Obr. č. 1 – 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.* (soutěžní text)



Obr. č. 2 – 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.*



Obr. č. 3 – 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.*

C. Soutež 2013, luštění originálního šifrového dopisu ze 17. století
P. Vondruška

Úvod

Vážení čtenáři, s radostí mohu oznámit, že navazujeme na tradiční soutěže v luštění, které jsme od roku 2000 do roku 2011 vždy na podzim pravidelně pořádali.

Díky Jakubovi Mírkovi, máme letos pro vás připravenu originální soutěž, která vám přinese zcela jedinečný zážitek. Máte možnost otestovat své schopnosti při luštění reálného zašifrovaného dopisu ze 17. století. Místo vymyšleného doprovodného příběhu k soutěžním příkladům, jak tomu bylo v posledních letech, sepsal nyní Jakub článek „Dosud nevyluštěný dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché z doby třicetileté války“, kde jsou uvedeny známé reálie jak ze života autora dopisu, tak i k šifrovému dopisu samotnému.

Předložený zašifrovaný text nebyl dosud nikdy rozluštěn a máte tedy šanci se stát prvními, kdo se dozví tajemství, které jeho autor před více jak 350 lety zašifroval.

Předpokládám, že byl použit nomenklátor, a proto při tak krátkém textu může být vyluštění (částečné vyluštění) složité. Přesto však je pravděpodobně možné jej získat. V minulých letech řada soutěžících dokázala, že si dokáže poradit se značně složitými úkoly. Věřím, že hledání tohoto řešení vás proto nezaskočí a jste na něj dostatečně připraveni.
Vzhledem k náročnosti hledaného řešení předpokládám, že (třetí) úloha bude odolávat v řádu týdnů (možná měsíců) a nehrozí to, co se stalo při luštění lehkých klasických úloh, kdy o vítězství rozhodovaly minuty (či v jednom případě dokonce vteřina ☺).

Doporučuji se před hledáním řešení seznámit se seriálem:
Jakub MÍRKA: Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni
Část I. Crypto-World 11-12/2012, str. 12 - 28
Část II. Crypto-World 1- 2/2013, str. 2 - 12
Část III. Crypto-World 3- 4/2013, str. 2 -14

Pro registraci, ukládání doprovodných textů, vkládání řešení a přehled dosažených výsledků slouží již sice poněkud zastaralé, ale pro soutěžící z předchozích let známé, soutěžní prostředí, které bylo pro účely letošní soutěže jen nepatrně aktualizováno.
K dispozici je na „tradiční adrese“ : http://soutez2013.crypto-world.info/ .
Registrace bude možná ihned po rozeslání údajů ke stažení tohoto Crypto-Worldu.

Závěrem mi dovolte, abych všem soutěžícím popřál mnoho krásných chvil při luštění tohoto starého tajemství!

Věřím, že se najde úspěšný řešitel, řešitelé. Pro ně jsou připraveny ceny, ale především jistě krásný zážitek z okamžiku, kdy se jim podaří odhalit ten správný postup.

Celkového vítěze (pokud stihne zaslat řešení do konce listopadu) čeká také účast na kryptografickém workshopu Mikulášská kryptobesídka, který se koná 28. - 29. listopadu v Praze. Potěšilo by mne a organizátory, kdyby byl ochoten vystoupit na večerním rump-session s krátkým minutovým příspěvkem, ve kterém by informoval o vyluštění tohoto textu a postupu, který použil.

Start soutěže

Soutěž začíná 18. 8. 2013 rozesláním e-zinu Crypto-World 7-8/2013 a skončí měsíc po prvém uznaném vyluštění předloženého šifrového textu.

Vstup na stránku soutěže je přes domovskou stránku Crypto-Worldu http://crypto-world.info/ - ikona ***Soutěže*** nebo přímým voláním soutěžní stránky http://soutez2013.crypto-world.info/ .

Registrace

Soutěžící se musí nejprve zaregistrovat. Při registraci soutěžící použije kód „Soutěž 2013“, který mu byl zaslán v e-mailu společně s údaji ke stažení e-zinu Crypto-World 7-8/2013.
Kód k registraci do soutěže bude zaslán i všem nově registrovaným odběratelům e-zinu Crypto-World, kteří se během soutěže k jeho odběru přihlásí.
Kód k registraci do soutěže bude opakovaně zaslán na vyžádání každému registrovanému odběrateli e-zinu Crypto-World. Žádost o zaslání zasílejte na adresu ezin@crypto-world.info, předmět REGISTRACE.
(Registrace k odběru e-zinu je bezplatná a provádí pomocí formuláře umístěného na domovské stránce.)
Soutěžící při registraci do soutěže zadá své uživatelské jméno (login), autentizační heslo pro opětovné přihlášení a dále e-mail, na který mu je zasílán e-zin Crypto-World.
Tento e-mail se dále na stránce nezobrazuje a je pro ostatní návštěvníky soutěže nedostupný. Slouží k zasílání pokynů a informací soutěžícím a k ověření zda uživatel je registrovaným odběratelem e-zinu.

Prvá nápověda

Soutěžícím budou do 24 hodin po registraci zaslány tyto dva pomocné texty:
- Přepis nešifrovaného dopisu z 13. července 1646
- Přepis pasáží šifrovaného dopisu, které byly psány otevřeným textem

Řešení úloh

Registrovaný řešitel zadává svá řešení soutěžních úloh přes www rozhraní, zadává je vždy velkými písmeny!

Za vyřešení úlohy se připisují soutěžícímu body.

Jako důkaz správného řešení se zadává "klíčové" slovo související s předloženým soutěžním textem. Odpověď bude automaticky vyhodnocena a řešitel se ihned dozví, zda odpověděl správně nebo ne.

Prvé dvě úlohy jsou velmi lehké a slouží k otestování funkčnosti prostředí a ujištění, že je soutěžící správně zaregistrován, umí rozhraní použít a seznámil se s reáliemi dopisů :-).

V prvé úloze soutěžící zadá jméno autora zobrazeného dopisu.
Ve druhé úloze je "klíčovým slovem“ poslední slovo předloženého textu.
Klíčové slovo pro třetí úlohu je řešiteli poskytnuto až po uznání jím zaslaného řešení. Soutěžící tedy musí nejdříve zaslat k vyhodnocení své řešení na adresu:
ezin@crypto-world.info , předmět ŘEŠENÍ.
K uznání řešení je nutno zaslat vyluštěný text (alespoň podstatnou jeho část) a popis použitého šifrového systému (např. pokud byl použit nomenklátor, pak tabulku homofonní záměny, případně další znaky šifrové abecedy uvedené v nomenklátoru – převodové znaky pro bigramy, kódy, klamače), nutností je zaslat popis, jak soutěžící při řešení postupoval.

Průběh soutěže

Na stránce soutěže bude zveřejňován aktuální průběh soutěže. U každého řešitele bude v celkovém žebříčku uveden počet dosažených bodů a lze se podívat i na pořadí úloh, ve kterém je soutěžící vyřešil. O pořadí soutěžících rozhoduje celkový počet dosažených bodů, v případě rovnosti bodů je rozhodující, kdo dosáhl tohoto počtu bodů dříve!

CENY

Podmínkou získání ceny je dosažení 100 bodů (tedy vyřešení všech tří úloh) a samozřejmě obsazení příslušného pořadí.

1. cena

Pro řešitele, který jako první vyřeší všechny tři úlohy je připravena tradiční **hlavní cena** - bezplatná účast na mezinárodním kryptologickém workshopu Mikulášská kryptobesídka, který se koná 28. - 29. listopadu v Praze. Pořadatel 13. ročníku Trusted Network Solutions (pořádá za podpory Centre for Research on Cryptohraphy and Security) hradí za vítěze registrační poplatek a srdečně jej zve vítěze na tuto akci. Další odměnou je sponzorský dar firmy DIGNITA, s.r.o. , kterým je tablet GOCLEVER TAB R76.2 včetně pouzdra s klávesnicí.

2. cena a 3. cena

Druhou a třetí cenu věnuje opět firma DIGNITA, s.r.o. . Cenou je užitečné univerzální rádio se svítilnou a dobíječkou mobilních telefonů Evolve RadioLight .

Loga sponzorů:

TNS (Trusted Network Solutions)

Centre for Research on Cryptohraphy and Security

DIGNITA s.r.o.

D. Diskrétní logaritmus a metody jeho výpočtu

Jiří Pulec, ji.pulec@post.cz,Ústav mikroelektroniky; Fakulta elektrotechniky a komunikačních technologií, VUT Brno

Článek se nejprve zabývá objasněním pojmu diskrétního logaritmu a jeho využitím v kryptografii. Dále je ilustrován postup při šifrování a dešifrování dat v ElGamalově systému, jehož bezpečnost je založena na obtížnosti výpočtu diskrétního logaritmu (praktické neřešitelnosti). V další části budou představeny metody, které lze k výpočtu diskrétního logaritmu využít.

Klíčová slova: diskrétní logaritmus, výpočet, složitost, algoritmus

1 Úvod

V problematice utajování zpráv je původní otevřená zpráva (*plaintext*) odesílatelem nahrazena zprávou zašifrovanou (*ciphertext*), která je takto odeslána příjemci, který ji dešifruje. Přitom je pro dešifrování nutné, aby příjemce věděl, jakým způsobem byla zpráva šifrována, a podle parametru charakterizujícího šifrování (*šifrovacího klíče*) zvolil odpovídající způsob dešifrování (*dešifrovací klíč*). Dešifrovací klíč je možné u některých systémů v reálném čase odvodit z klíče šifrovacího (*symetrické kryptosystémy*), nebo toto možné není a potom znalost šifrovacího klíče a kryptogramu nedostačuje pro zjištění původní zprávy (*kryptosystémy asymetrické*). Potom je možné zavést pojem *veřejného klíče*, který každému uživateli umožní šifrovat zprávu a tuto zprávu potom odeslat. Přitom zašifrovanou zprávu je možné dešifrovat pouze pomocí *soukromého* (tajného) *klíče*. Zatímco otevřenou zprávu může zašifrovat kdokoli, již šifrovanou zprávu může dešifrovat a číst pouze držitel soukromého klíče.

2 Diskrétní logaritmus

V konečné multiplikativní grupě $(G, .)$ nazýváme diskrétním logaritmem z prvku β při základu α takový prvek a, pro který platí, že

$$\beta = \alpha^a.$$

Platí, že řád prvku α je n a že $0 \leq a \leq n - 1$ [1].

Užití diskrétního logaritmu v kryptografii spočívá v tom, že zatímco nalezení prvku a tak, aby platilo $\beta = \alpha^a$, je při zadaném β a α obtížné, je výpočet β pro zadané α a a snadný, lze ho definovat jako a-násobný součin prvku α.

3 ElGamalův asymetrický kryptosystém

Nyní definujeme *ElGamalův kryptosystém*, jehož bezpečnost je založena právě na obtížnosti výpočtu diskrétního logaritmu.

ElGamalův systém je systémem asymetrickým, není zde možné určit dešifrovací klíč z klíče šifrovacího [2]. Při znalosti kryptogramu a šifrovacího klíče není možné určit původní text.

El Gamalův kryptosystém je založen na multiplikativní grupě $(Z_p, .)$, kde p je prvočíslo. V této grupě je prvek $\alpha \in Z_p$ prvočíslem. Prostorem zpráv je multiplikativní grupa Z_p , prostorem kryptogramů je kartézský součin $Z_p \times Z_p$ [1], [3]. Prostor klíčů je množina čtveřic (p, α, a, β), přitom platí, že $\beta \equiv \alpha^a \pmod p$. Hodnoty p, α a β jsou veřejně známé, zatímco a je tajné (soukromý klíč). Dále se

pro čtveřici $K = (p, \alpha, a, \beta)$ a pro náhodně zvolené číslo $k \in Z_{p-1}$ definuje

$$e_K(x, k) = (y_1, y_2),$$

kde platí, že

$$y_1 = \alpha^k \bmod p,$$

$$y_2 = x\beta^k \bmod p.$$

Dešifrovací klíč je definován jako $d_K(y_1, y_2) = y_2 (y_1^{\,a})^{-1} \bmod p$.

Příklad: Nyní uveďme příklad šifrování a dešifrování v ElGamalově kryptosystému [1]:

$$p = 2579,$$

$$\alpha = 2,$$

Dále definujeme soukromý klíč a, v tomto případě $a = 765$. Dále počítáme β, jako

$$\beta = \alpha^a = 2^{765} \bmod 2579 = 949.$$

Formálně je zde klíčem čtveřice (2579, 2, 765, 949).

Odesílatel chce tedy poslat příjemci zprávu $x = 1299$. K zašifrování zvolí $k = 853$. Následně odesílatel vypočítá:

$$y_1 = 2^{853} \bmod 2579 = 435$$

a

$$y_2 = 1299 \times 949^{853} \bmod 2579 = 2396$$

Tedy kryptogram y:

$$y = (435, 2396).$$

Poté, co příjemce obdrží tento kryptogram, vypočítá

$$x = 1396 \times (435^{765})^{-1} \bmod p = 1299.$$

Bezpečnost spočívá v nemožnosti v reálném čase spočítat hodnotu $a = \log_\alpha \beta$. Jakmile je útočník schopen tuto hodnotu vypočítat, může přijímat a číst zprávy stejně jako oprávněný příjemce. V takovém případě nebude kryptosystém bezpečný. Jeho bezpečnost spočívá v neexistenci algoritmu, který by daný problém umožnil řešit v polynomiálním čase.

4 Výpočet diskrétního logaritmu

Problém diskrétního logaritmu tedy spočívá v nalezení takového prvku α řádu n, aby platila rovnost [3]:

$$\beta = \alpha^a$$

V současné době není znám efektivní algoritmus, jehož pomocí by bylo možné diskrétní logaritmus vypočítat. Existuje nicméně množství algoritmů, které převádějí časovou náročnost výpočtu diskrétního logaritmu na náročnost paměťovou. V této části budou uvedeny tři takové algoritmy [1]:

- Shankův algoritmus
- Pollardův ró algoritmus
- Pohligův – Hellmanův algoritmus

Žádný z uvedených algoritmů přitom neumožňuje provádět výpočet diskrétního logaritmu se srovnatelnou efektivitou, jako je efektivita algoritmu používaného k umocňování. Pokud by takový algoritmus byl znám, nebyl by ElGamalův kryptosystém bezpečný.

Při analýze algoritmů předpokládáme podle [1], že časová složitost násobení dvou prvků v grupě G je rovna $O(1)$, tj. konstantní.

První možností vedoucí k výpočtu diskrétního logaritmu je vyčerpávající zkoušení všech možností s paměťovou složitostí $O(1)$ a časovou složitostí $O(n)$.

4.1 Shankův algoritmus

Shankův algoritmus je jedním z algoritmů vedoucích k výpočtu diskrétního logaritmu.

Tento algoritmus, jehož vstupem je čtveřice (G, a, α, β), kde G je multiplikativní grupa, n je řád prvku α, algoritmus je definován ve formě pseudokódu takto:

1. $m := \lfloor \sqrt{n} \rfloor$

2. **for** $j := 0$ **to** $m - 1$
   do počítej α^{mj}

3. seřaď všechny dvojice (j, α^{mj}) podle jejich druhého členu, výsledkem budiž seznam L_1

4. **for** $i := 0$ **to** m -1
   do počítej $\beta\alpha^{-1}$

5. seřaď m uspořádaných dvojic $(i, \beta\alpha^{-1})$ podle jejich druhého členu, výsledek: L_2

6. Najdi dvojici $(j, y) \in L_1$ a dvojici $(i, y) \in L_2$ (obě dvojice mají tentýž druhý člen)

7. $\log_\alpha \beta := (mj + i) \bmod m$

V uvedeném algoritmu je možné, aby kroky 2 a 3 byly vypočítané dopředu. Je důležité, že pokud $(j, y) \in L_1$ a $(i, y) \in L_2$, potom

$$\alpha^{mj} = y = \beta\alpha^{-1}$$

a tedy

$$\alpha^{mj+i} = \beta,$$

jak požadujeme.

Časová složitost kroku 2 je $O(m)$, pokud je tento výpočet proveden dopředu (tj. před vlastním provedením algoritmu), transformuje se tato časová složitost na složitost paměťovou.

Rovněž časová složitost kroku 4 je $O(m)$, časová složitost kroků 3 a 5 je $O(m \log m)$. Je běžné tuto složitost (pro její logaritmickou povahu) zanedbávat. Výpočet kroku 6 má časovou složitost $O(m)$.

4.2 Pollardův ró algoritmus diskrétního logaritmu

Jiným algoritmem požívaným pro výpočet diskrétního logaritmu, je Pollardův ró algoritmus. Varianta tohoto algoritmu je používána pro faktorizaci čísel [1]. Nechť je $(G, .)$ grupa a α je prvek této grupy o řádu n. Podgrupa

$$< \alpha > = \{\alpha^i : 0 \leq a \leq n-1\}$$

obsahuje prvek β, potřebujeme zjistit diskrétní logaritmus právě tohoto prvku. Pokud zvolíme libovolnou polynomiální funkci (např. $f(x) = x^2 + a$; a je konstanta), počítáme posloupnost $x_1, \ldots x_m$ podle předpisu

$$x_j = f(x_{j-1}) \bmod a,$$

pro každé $j \geq 2$. V okamžiku, kdy se v posloupnosti objeví takové x_i a x_j, že platí $i < j$ a současně $x_i = x_j$, tak je možné počítat $\log_\alpha \beta$.

Dále definujeme rozklad grupy G do tří množin zhruba stejné velikosti, S_1, S_2, a S_3. Následně definujeme funkci f.

$$f: < \alpha > \times Z_p \times Z_p \rightarrow < \alpha > \times Z_p \times Z_p$$

Ta je definována předpisem:

$f(x, a, b) = (\beta x, a, b+1)$ pro $x \in S_1$
$f(x, a, b) = (x^2, 2a, 2b)$ pro $x \in S_2$
$f(x, a, b) = (\alpha x, a+1, b)$ pro $x \in S_3$

Od každé takto vytvořené trojice se požaduje vlastnost $x = \alpha^a \beta^b$. Řekněme, že první trojice, která má tuto vlastnost, je (1, 0, 0). Zřejmě $f(x, a, b)$ splňuje požadovanou vlastnost, když ji splňuje i (x, a, b). Dále definujme:

$(x_i, a_i, b_i) = (1, 0, 0)$ pro $i = 0$
$(x_i, a_i, b_i) = f(x_{i-1}, a_{i-1}, b_{i-1})$ pro $i \geq 1$

Nyní porovnáme každé dvě trojice

(x_i, a_i, b_i) a (x_{2i}, a_{2i}, b_{2i}), než nalezneme hodnotu $i \geq 1$, aby platilo $x_{2i} = x_i$. Jakmile se tak stane, získáme

$$\alpha^{a_{2i}} \beta^{b_{2i}} = \alpha^{a_i} \beta^{b_i}$$

Pokud se označí $c = log_\alpha \beta$, musí platit , že

$$\alpha^{a_{2i}+cb_{2i}} = \alpha^{a_i+cb_i}$$

Protože α má řád n, platí

$$a_{2i} + cb_{2i} \equiv a_i + cb_i \pmod{n}.$$

Což může být dále transformováno na

$$c(b_{2i} - b_i) \equiv a_i - a_{2i} \pmod{n}$$

Je-li největší společný dělitel $(b_{2i} - b_i, n) = 1$, můžeme stanovit c následovně:

$$c = (a_i - a_{2i})(b_{2i} - b_i)^{-1} \bmod n.$$

Předchozí poznatky lze shrnout do formy pseudokódu:

procedure $f(x, a, b)$
  if $x \in S_1$
    then $f := (\beta \times x, a, (b + 1) \bmod n)$
    else if $x \in S_2$
    then $f := (x^2, 2a \bmod n, 2b \bmod n)$
    else $f := (\alpha \times x, (a + 1) \bmod n, b)$
return (f)

main
  definuj rozklad $G = S_1 \cup S_2 \cup S_3$
  $(x, a, b) := f(1,0,0)$
  $(x', a', b') := f(x, a, b)$
while $x \neq x'$
  do
    $\{(x, a, b) := f(x, a, b)$
    $(x', a', b') := f(x', a', b')$
    $(x', a', b') := f(x', a', b')\}$

if $\gcd(b' - b, n) \neq 1$
  then return („failure“)
  else return $((a - a')(b' - b)^{-1} \bmod n)$

Podle [1], pokud uvažujeme funkci f jako skutečně náhodnou, časová složitost v cyklické grupě G řádu n je rovna $O(\sqrt{n})$.

4.3 Pohligův – Hellmanův algoritmus

Dalším algoritmem použitelným v problematice řešení problému diskrétního logaritmu je algoritmus Pohligův – Hellmanův. Nejprve uvažujme:

$$n = \prod_{i=1}^{k} p_i^{c_i}$$

kde všechna p_i jsou prvočísla. Hodnota $a = \log_\alpha \beta$ je dána jednoznačně až na záměnu s jinou kongruentní hodnotou modulo n. Nejprve si povšimněme, že je možné vypočítat a mod n pomocí čínské věty o zbytcích. Nechť je tedy q prvočíslo splňující:

$$n \equiv 0 \pmod{q^c}$$

a přitom neplatí:

$$n \equiv 0 \pmod{q^{c+1}}$$

Nyní ukážeme, jak vypočítáme hodnotu

$$x = a \bmod q^c$$

kde $0 \leq x \leq q^c - 1$.

Nyní vyjádřeme x pomocí q jako

$$x = \sum_{i=0}^{c-1} a_i q^i$$

kde $0 \leq a_i \leq q - 1$ pro $0 \leq i \leq c - 1$. Nyní si povšimněme, že je a možné vyjádřit jako

$$a = x + sq^c$$

pro celé číslo s. Potom dostáváme, že

$$a = \sum_{i=0}^{c-1} a_i q^i + sq^c$$

Prvním krokem v algoritmu je vypočítat a_0. Přitom platí, že:

$$\beta^{n/q} = \alpha^{a_0 n/q}$$

Pohligův - Hellmanův algoritmus ve formě pseudokódu může vypadat následovně:

$j := 0$
$\beta_j := \beta$
while $j \leq c - 1$
do
{ $\delta := \beta_j^{n/q^{j+1}}$;
najdi i takové že $\delta = \alpha^{in/q}$
$a_j := i$
$\beta_{j+1} := \beta_j \alpha^{-a_j q^j}$
$j := j + 1$ }
return $(a_0, \ldots, a_{c-1})$

Budeme-li uvažovat časovou složitost algoritmu, podle [1] je tato $O(cq)$. Časovou složitost lze nicméně zlepšit, neboť podle [1] je každý výpočet hodnoty i samostatným výpočtem diskrétního logaritmu takového, že

$i = \log_{\alpha^{n/q}} \delta$.

Zde má prvek α řád q, a tudíž každé i může být počítáno Shankovým algoritmem v čase $O(\sqrt{q})$. Potom je výpočetní časová složitost Pohligova – Hellmanova algoritmu snížena na $O(c\sqrt{q})$.

5 Shrnutí

Neexistence efektivního algoritmu, který by umožnil řešit úlohu diskrétního logaritmu je podmínkou bezpečnosti některých asymetrických kryptografických systémů (ElGamalův). Tento článek z mnoha metod výpočtu diskrétního logaritmu popisuje tři. Ohledně časové náročnosti je Shankův algoritmus srovnatelný s algoritmem Pollardovým, časová náročnost je zde rovna druhé odmocnině řádu grupy (při obvyklém zanedbání logaritmických členů u Shankova algoritmu). Shankův algoritmus umožňuje, aby některé jeho kroky byly provedeny dopředu (což zvyšuje paměťovou náročnost), nicméně má jednoduchou implementaci, proto je vhodný tam, kde je k dispozici dostatečný paměťový prostor k tomu, aby byly některé výpočty provedeny dopředu. Algoritmus Pohlig – Hellmanův má výpočetní časovou složitost $O(c\sqrt{q})$, je tedy výhodný tam, kde je možno vyjádřit n jako $n = q^c$ pro c blízké číslu 2.

Použité zdroje

[1] Stinson, D. Cryptography: theory and practice. New York: Chapman&Hall/CRC, 2006, 593 stran, ISBN 1-58488 –508 –4

[2] Přibyl, J. Informační bezpečnost a utajování zpráv. Praha: Vydavatelství ČVUT, 2004, 234 stran

[3] Soroka, O. Digitální podepisování pomocí asymetrické kryptografie. Výukový materiál – přednášky, dostupné online na http://kmlinux.fjfi.cvut.cz/~balkolub/Vyuka/leto2011/Soroka.pdf

E. Kaspersky v Praze: „Kybernetické zbraně jsou nejhorším vynálezem století“

Informace vznikla využitím tiskové zprávy, kterou k této příležitosti vydala agentura Grayling (kontakt viz závěr tohoto sdělení).

Na světě už nejsou žádná tajemství, všechno už bylo ukradeno nejméně dvakrát.
E. Kaspersky

Průmyslové systémy, kritická IT infrastruktura a telekomunikace – podle Eugena Kasperského dnešní tři nejzranitelnější cíle z pohledu IT bezpečnosti. Za klíčové aktéry ohrožující IT bezpečnost Kaspersky označil kyberzločince, hacktivisty, státní agentury a teroristé organizace. Majitel a generální ředitel Kaspersky Lab se koncem července zúčastnil několikadenní návštěvy v Praze, během které se 25.7. setkal s českými zákazníky, partnery a novináři.

Vedle finanční a politické motivace stojí za kybernetickými útoky podle Kasperského často také vojenské zájmy, snaha o poškození pověsti nebo sabotáž. Dokonalá ochrana proti internetovým hrozbám podle zakladatele největší soukromě vlastněné antivirové firmy není možná. *„Náš svět řídí počítače. Závisíme na IT systémech a jsme velmi zranitelní,“* uvedl Kaspersky a situaci ilustroval faktem, že i v počítačích mezinárodní kosmické stanice se nalézají viry, které se tam dostaly prostřednictvím infikovaných USB klíčů.

Ve své prezentaci varoval Kaspersky před kyberterorismem. Nová generace teroristů podle něj bude využívat internet k útokům na kritickou infrastrukturu. Kaspersky při tom odkázal na akční film Smrtonosná past 4, jehož části jsou prý doslova návodem pro podobné akce.

Ve vystoupení Kasperského byly ale i odlehčenější chvíle. *„Umíte si představit, co by se stalo po rozsáhlém kybernetickém útoku na pivovary v České republice?“* Zeptal se například vizionář IT bezpečnosti publika. Na jeden z dotazů pak Kaspersky odpověděl, že používá kreditní kartu i pro platby online. Jde nicméně o tu, na které nemá velké obnosy peněz. *„Na světě už nejsou žádná tajemství, všechno už bylo ukradeno nejméně dvakrát,“* uzavřel Kaspersky.

O společnosti Kaspersky Lab

Kaspersky Lab je největším soukromě vlastněným poskytovatelem koncových bezpečnostních řešení na světě. Společnost se řadí mezi čtyři největší prodejce bezpečnostních řešení pro koncové uživatele. Již 15 let patří Kaspersky Lab mezi přední inovátory v oblasti informačních technologií a poskytuje efektivní digitální bezpečnostní řešení zákazníkům, malým a středním firmám i velkým podnikům. Aktuálně společnost působí v bezmála 200 zemích a oblastech a poskytuje ochranu více než 300 milionům uživatelů. Více informací o společnosti Kaspersky Lab najdete na **www.kaspersky.cz**.

Pro další informace prosím kontaktujte:

Michal Malysa, PR Consultant, Grayling Czech Republic
michal.malysa@grayling.com , Twitter.com/GraylingCZ

F. Pozvánka k podzimním kurzům Akademie CZ NIC

Akademie CZ.NIC je vzdělávací projekt sdružení CZ.NIC, správce české domény nejvyšší úrovně. Výukové centrum, jenž se pod tímto názvem skrývá, nabízí zájemcům možnost odborného vzdělávání v oblasti Internetu a internetových technologií. Kurzy jsou určeny všem, kteří se chtějí dozvědět více o vypsaných tématech, vyzkoušet si přednášenou látku v praxi, podělit se o zkušenosti s lektory, ale také s ostatními návštěvníky kurzů.

Lektory Akademie CZ.NIC jsou jak zaměstnanci sdružení, tak odborníci z praxe. Součástí výukového centra je také unikátní laboratoř vybavená hardwarem a softwarem potřebným k testování a experimentování v rámci výuky.

Kurzy Akademie CZ.NIC nabízejí možnost:

- absolvovat kurzy, které jiná výuková střediska nevypisují
- získat nové znalosti o aktuálních internetových technologiích
- vyzkoušet si, jak takové technologie fungují v reálném prostředí
- setkat se s odborníky z praxe

Jak se přihlásit

Pro přihlášení do kurzu stačí pouze vyplnit přihlašovací formulář a uhradit kurz. Pokud máte zájem o kurz, který není aktuálně vypsán, napište nám e-mail na akademie@nic.cz a budeme vás informovat o nejbližším termínu konání vybraného kurzu.

Místo konání kurzů

Akademie CZ.NIC
Americká 23 , 2.patro
120 00 Praha 2

http://www.nic.cz/akademie/contact/

Možnosti slevy

Studenti mají možnost, na základě vložení kopie dokladu o studiu do přihlašovacího formuláře, získat slevu 90 % z dané částky kurzu.

Seznam přednášejících, kurzů a termínů

Petr Černohouz

- **Implementace IPv6 , 20.8., 17.9.**

Kurz seznámí posluchače se základními vlastnostmi a principy internetového protokolu verze 6, dostupnými přechodovými mechanismy a příkazy pro práci s IPv6. Součástí kurzu jsou praktická cvičení, kde si účastnící mohou vyzkoušet konfiguraci a troubleshooting IPv6 na operačním systému Linux, IOS (Cisco), Junos (Juniper) a Windows.

Petr Hruška

- **IP telefonie – protokol SIP , 23.9.**

Se zvyšující se kvalitou přípojek k internetu se čím dál tím více prosazuje internetová telefonie jako náhrada analogové pevné linky. Nejpoužívaněj-ším protokolem pro internetovou telefonii je otevřený protokol SIP. Ačkoliv má SIP velké množství výhod, díky kterým je oprávněně nejpoužívaněj-ší, jeho velkou nevýhodou je relativně velká složitost. Neblahým důsled-kem je, že velká většina ústředen je nakonfigurována postupem pokus-omyl, což se mnohdy projevuje nekompatibilitou a poruchovostí. Tento kurz je určený správcům ústředen, kterým by měl poskytnout dostatek informací pro kvalifikované řešení problémů s protokolem SIP.

Pavel Vondruška

- **Problematika infrastruktury veřejných klíčů (PKI) , 24.9., 11.12.**

Kurz seznámí účastníky s principy fungování PKI z různých aspektů. Účastník se seznámí se základními principy asymetrických šifer, s definicemi a požadavky zákona o elektronickém podpisu, bude seznámen s technickým a legislativním pohledem na důvěru v certifikáty a ověření podpisu a certifikátu. Součástí budou některé jednoduché praktické dovednosti – zejména práce s certifikáty (generování, export, import, podpis, ověření) a práce s CRL.

Tomáš Hlaváček

- **Směrovací protokol BGP , 25.9. , 24.10. , 12.12.**

Kurz seznámí posluchače s vlastnostmi a principy směrovacího protokolu BGP, popíše nejběžnější konfigurace BGP, metody implementace smě-rovací politiky a možnosti zabezpečení BGP. V průběhu kurzu si účastníci prakticky vyzkouší konfiguraci a troubleshooting BGP.

Jan Kadlec

- **DNSSEC pro veřejnou správu , 6.11.**

Kurz je určen pro pracovníky státní správy a samosprávy, kteří se chtějí dozvědět o technologii DNSSEC. Praktická část je pak určena pro techniky, kteří spravují DNS a dohlížejí na jeho správné fungování a rozvoj.

- **DNSSEC - zabezpečení DNS , zatím nevypsáno**

Cílem setkání je seznámit jeho účastníky s technologií DNSSEC, s její návazností na systém DNS. Součástí kurzu budou i informace o použitelnosti dostupných nástrojů pro podepisování zónových souborů a návrh jednoduchého systému na podepisování včetně rotace DNSSEC klíčů. Kurz je určen pro techniky, kteří spravují DNS a dohlížejí na jeho správné fungování a rozvoj.

- **Principy a správa DNS , 02.-03.10., 30.-31.10.**

Obsahem kurzu bude seznámení se základními principy DNS, s provozem au-toritativních DNS serverů, s provozem rekurzivních DNS serverů a se zákla-dy DNS. Důraz bude kladen na provoz DNS ve vztahu k registraci doméno-vých jmen v zóně .CZ. Kurz seznámí účastníky s konfigurací DNS imple-mentací BIND verze 9.x, NSD 3.x a Unbound 1.x.

G. 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

Crypto-World 5-6/2013

H. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "***Kryptologické sekce Jednoty českých matematiků a fyziků***" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem 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 Kollár 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/