Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 15, číslo 3-4/2013 **14. duben**

3-4/2013

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1323 registrovaných odběratelů)

Obsah : str.

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

A. Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni, část III.

Jakub MÍRKA, SOA Plzeň, mirka@soaplzen.cz

Obrazová příloha k části III. http://crypto-world.info/casop15/obr3.zip).

UŽÍVÁNÍ ŠIFER VE STŘEDOEVROPSKÉM PROSTORU

Pro dobu před rokem 1618 se v českých archivech nachází jen malé množství šifrované korespondence. Z této skutečnosti však nelze ukvapeně usuzovat, že v předbělohorském období nebylo v Čechách šifrování téměř vůbec používáno. Za prvé se v našich archivech pro tuto dobu ve srovnání např. se zbytkem 17. století dochovalo obecně poměrně málo archiválií, za druhé je docela pravděpodobné, že je v archivech uloženo více relevantních archiválií, než je mi dosud známo. Již výše jsem se zmínil o Sbírce fotonegativů v MZA v Brně,[1] korespondenci Viléma z Rožmberka v SOA v Třeboni[2] a souboru kopií dopisů významných domácích i zahraničních představitelů protestantské strany.[3] Za zvláštní zmínku stojí také již dříve uvedená šifrovaná korespondence z let 1608–1612 uložená v Archivu Národního muzea. Jde o soubor korespondence císaře Rudolfa, uherského krále Matyáše, arcivévodů Leopolda a Albrechta a pánů Václava z Vchynic a Adolfa z Althannu z let 1608–1612. Před polovinou 19. století byl tento soubor ve vlastnictví Václava Hanky a jeho součástí bylo více než 60 česky a německy psaných a zčásti šifrovaných dopisů. Hanka všechny dopisy až na jeden dešifroval pomocí přiložených klíčů a roku 1847 publikoval jejich edici.[4] Její součástí byla i litografie českého klíče, sestávajícího z jednoduché substituce a několika kódů. Další litografie zobrazovala jediný nedešifrovaný český text,[5] který zhruba o deset let později vyluštil Antonín Vánkomil Maloch.[6] Zajímavostí vymykající se obvyklému způsobu šifrování té doby je česko-latinská kryptologická příručka Rafaela Mnišovského ze Sebuzína. Sloužila totiž pro utajování zpráv pomocí polyalfabetického šifrovacího systému. V současné době je

---

[1] Tyto fotokopie archiválií uložených ve Vídni a v Simancasu sice vznikly při bohemikálních výzkumech, ale bez jejich bližšího zkoumání nelze určit, zda byly Čechy také zemí původu reprodukovaných archiválií, nebo zda byl jejich vztah k Čechám jiného rázu. Viz CULKOVÁ, Dagmar. Výzkum bohemik v zahraničí do roku 1939 organizovaný našimi archivy. In: *Sborník archivních prací.* Praha 1979, roč. 29, s. 173.

[2] VERŽOVSKIJ, Fedor. *Dve kandidatury na polskij prestol Vilgelma iz Rozenberga i ercgercoga Ferdinanda 1574–1575 po neizdannym istočnikam.* Varšava : Tipografija K. Kovalevskago 1889, s. 3–73 (Priloženija).

[3] Opisy uloženy v Národním archivu. Více viz HULEC, Otakar. Konspirativní charakter předbělohorské protistavovské opozice. *Jihočeský sborník historický* 30, 1961, s. 97–102. Otakar Hulec se ve svém článku zabývá především formální stránkou vzájemného styku protestantské opozice. Ilustrativně popisuje způsob předávání a utajování korespondence těchto nejvyšších představitelů protestantské opozice a s pomocí získaných poznatků poukazuje na konspirativní charakter jejich jednání.

[4] HANKA, Václav. Correspondenz zwischen Kaiser Rudolf, dem ungarischen Könige Matthias, den Erzherzogen Leopold und Albrecht, dann den Herren Wenceslaw von Wchynicz und Adolf von Althan. *Abhandlungen der königlichen böhmischen Gesellschaft der Wissenschaften, Vierter Band von den Jahren 1845–1846.* Prag 1847, s. 155–238. Dnes uloženy v Archivu Národního muzea, Sbírka D, karton č. 9, písemnosti z let 1606–1611.

[5] Litografie *tamtéž*, vložena mezi s. 196 a 197.

uložena v univerzitní knihovně v Uppsale pod sign. MS Slav. 60. Podrobněji se jí i osobou jejího autora zabýval Jaroslav Kašpar[7] a před ním Carin Davidssonová,[8] která si jako první povšimla, že nejde o učebnici češtiny, ale o šifrovací pomůcku. Z výše uvedeného je zřejmé, že se v Čechách užívalo šifrování již v době před Bílou horou, ale vzhledem k omezenému množství pramenů se dá těžko usuzovat, jak rozšířené bylo.

V případě šifrované korespondence z doby třicetileté války, dochované v našich archivech, už většinou nelze mluvit o její české provenienci. Naprostá většina dokumentů pochází z činnosti vysokých císařských diplomatů a generálů původem z jiných, často románských zemí, kteří se v Čechách z velké části usadili až v důsledku pobělohorských konfiskací. Jejich korespondence tak převážně vznikala na různých místech výkonu diplomatických misí či na bojištích celé Evropy, především pak ale ve střední Evropě, resp. na území Říše.[9] Téměř všechna tato korespondence, alespoň co se týká té dosud prozkoumané, byla výsledkem výměny informací mezi významnými činiteli katolické strany. Dopisy osob vystupujících na straně protestantů se mezi zkoumanými archiváliemi objevují prakticky jen v těch případech, kdy byly při doručování zachyceny nepřáteli.[10]

Zdá se, že minimálně ve střední Evropě se šifrování nejvíce rozšířilo až ve druhé polovině třicetileté války.[11] Je ale známa i šifrovaná korespondence z krátkého válečného období před bitvou na Bílé hoře. Ve fondu Rodinný archiv Buquoyů v SOA v Třeboni je uloženo několik dopisů adresovaných Karlovi Bonaventurovi de Longueval hraběti Buquoyovi. Jejich odesilateli byli např. španělský vyslanec u císařského dvora Íñigo Vélez de Guevara y Tassis hrabě de Oñate;[12] císařský vojevůdce francouzského původu Henri Duval de Dampierre;[13] španělský generál Ambrosio Spinola, markýz de los Balbases[14] a další.[15] Dopisy jsou z převážné části šifrovány jednoduchou substituční šifrou, u několika se ale objevuje i homofonie. Zajímavý je také způsob šifrování užívaný ve stejné době vrcholnými představiteli druhé strany konfliktu. Český král Fridrich Falcký používal pro svou

---

[6] MALOCH, Antonín V. Rozluštění chiffrovaného písma v češtině. *Lumír* 1858, s. 205–206.

[7] KAŠPAR, Jaroslav. *Soubor statí o novověkém písmu*. Praha : Univerzita Karlova 1993, s. 189–190.

[8] DAVIDSSON, Carin. Johannes Trithemius' Polygraphia als tschechisches Lehrbuch. Cod. Slav. 60 bei der Universitätsbibliothek in Uppsala. *Scando–Slavica* 5, 1959, s. 148–164.

[9] To platí i pro několik málo přímo z Čech pocházejících osobností třicetileté války, jejichž šifrovaná korespondence se nám dochovala – např. Albrecht z Valdštejna nebo Karel Robmhap ze Suché. K šifrované korespondenci v registratuře Albrechta z Valdštejna viz ROUBÍK, František. Šifrované dopisy v registratuře Albrechta z Valdštejna. In: *Sborník prací věnovaných prof. Dru Gustavu Friedrichovi k šedesátým narozeninám, 1871–1931*. Praha : Historický spolek v Praze 1931, s. 359–368. Dopisy Robmhapa ze Suché viz SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 10, i. č. 209.

[10] Kopie dopisu Alexandera Erskiho z 15. července 1644 radovi a dvorskému kancléři švédského krále a vyslance na mírových jednáních v Německu Johanu Adlerovi Salviovi. SOA v Litoměřicích – pobočka Děčín, HS Clam Gallas karton č. 381, i. č. 1397, sign. XV/9. Opisy zadržených dopisů Karla Robmhapa ze Suché landkraběnce hesenské. SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 10, i. č. 209.

[11] Také v edici *Documenta Bohemica belli tricennale illustrantia* je v největší míře šifrovaná korespondence zastoupena v posledních dvou dílech z let 1635–1649.

[12] SOA v Třeboni, RA Buquoyů, sign. 172, 246.

[13] Tamtéž, sign. 69/1–2; tamtéž, sign. KB 50 Q, KB 171 Q.

[14] Tamtéž, sign. KB 756/6.

[15] Některé šifrované dopisy z RA Buquoyů jsou uvedeny v edici ČECHOVÁ, Gabriela – KOČÍ, Josef – POLIŠENSKÝ, Josef (edd). *Documenta Bohemica Belli Tricennale Illustrantia Tomus II.* Praha : Academia 1972, s. 76, 82, 89, 92, 99, 133, 135, 138, 182.

korespondenci s nizozemskými stavy a Mořicem Oranžským ve druhé polovině roku 1620 homofonní substituční šifry obsahující také nepříliš velký počet kódů.[16]

Dopisy z druhé poloviny dvacátých let 17. století, dochované např. v registratuře válečné kanceláře Albrechta z Valdštejna,[17] většinou bývají šifrovány buď pomocí jednoduché, nebo homofonní substituce, a občas jsou doplněny nepříliš velkým počtem kódů. Císařský rezident v Konstantinopoli Sebastian Lustrier utajoval obsah dopisů pomocí homofonní substituce bez kódů.[18] Trochu složitější typ klíče užíval Vilém Verdugo ve své korespondenci s Jeanem de Croy.[19] Kromě homofonní substituce a kódů obsahuje také bigramy. Použití komplikovanějšího nomenklátoru než v ostatních případech je pravděpodobně dáno především tím, že Vilém Verdugo působil ve službách Španělského království, v němž byla v této době kryptologie, a vůbec obecné užívání šifer, nesporně na vyšší úrovni než v Říši.

V průběhu třicátých a především čtyřicátých let 17. století se především v nomenklátorech užívaných císařem a jeho nejvýznamnějšími dvořany objevují bigramy. V korespondenci vojenských osob se bigramy nacházejí jen zřídka, dokonce v ní ještě občas narazíme i na jednoduchou substituci. Obvyklou, ovšem ne nezbytnou, výbavou nomenklátorů se v té době stávají také klamače. Opět se častěji vyskytují ve složitějších nomenklátorech výše postavených osob, ve kterých byla samozřejmostí i homofonie. Kódy naopak ve všech nebývaly. Vzhledem k tomu, že kvůli rostoucí převaze homofonie a užívání bigramů a kódů stále vzrůstal počet potřebných znaků šifrové abecedy, začínaly se pro zobrazení těchto znaků ve větší míře prosazovat číslice. Obvykle dvouciferné číslice nahrazovaly jednotlivá písmena abecedy, případně bigramy, zatímco trojciferné číslice byly používány pro kódy. Ovšem i tato zvyklost samozřejmě měla své výjimky. Jiné formy znaků (písmena latinské, řecké či hebrejské abecedy; astrologické značky; geometrické tvary aj.), které dříve bývaly jednou z možných alternativ, sice zcela nevymizely, ale objevovaly se čím dál méně často a i tak už byly ve většině případů jen doplňkem číslic.[20]

Pro dobu po třicetileté válce mohu na základě dosud zjištěných sporých pramenů, především z fondu Rodinný archiv Windischgrätzů, do jisté míry sledovat zejména vývoj nomenklátorů v prostředí císařského dvora a jeho diplomatického aparátu.[21] Ve druhé polovině 17. století se začal objevovat nový důmyslnější systém klamačů, který bylo možné použít pouze v převažujícím číslicovém systému šifrových znaků. Spočíval v tom, že bylo

---

[16] Dopisy jsou uloženy ve Státním archivu v Haagu a české odborné veřejnosti je přiblížila Anna Vavroušková. Viz VAVROUŠKOVÁ, Anna. Šifrované dopisy Fridricha Falckého. In: *Sborník prací věnovaných Janu Bedřichu Novákovi k šedesátým narozeninám*. Praha : Československá archivní společnost 1932, s. 486–494.

[17] Viz ROUBÍK, František. Šifrované dopisy v registratuře Albrechta z Valdštejna. In: *Sborník prací věnovaných prof. Dru Gustavu Friedrichovi k šedesátým narozeninám, 1871–1931*. Praha : Historický spolek v Praze 1931, s. 359–368.

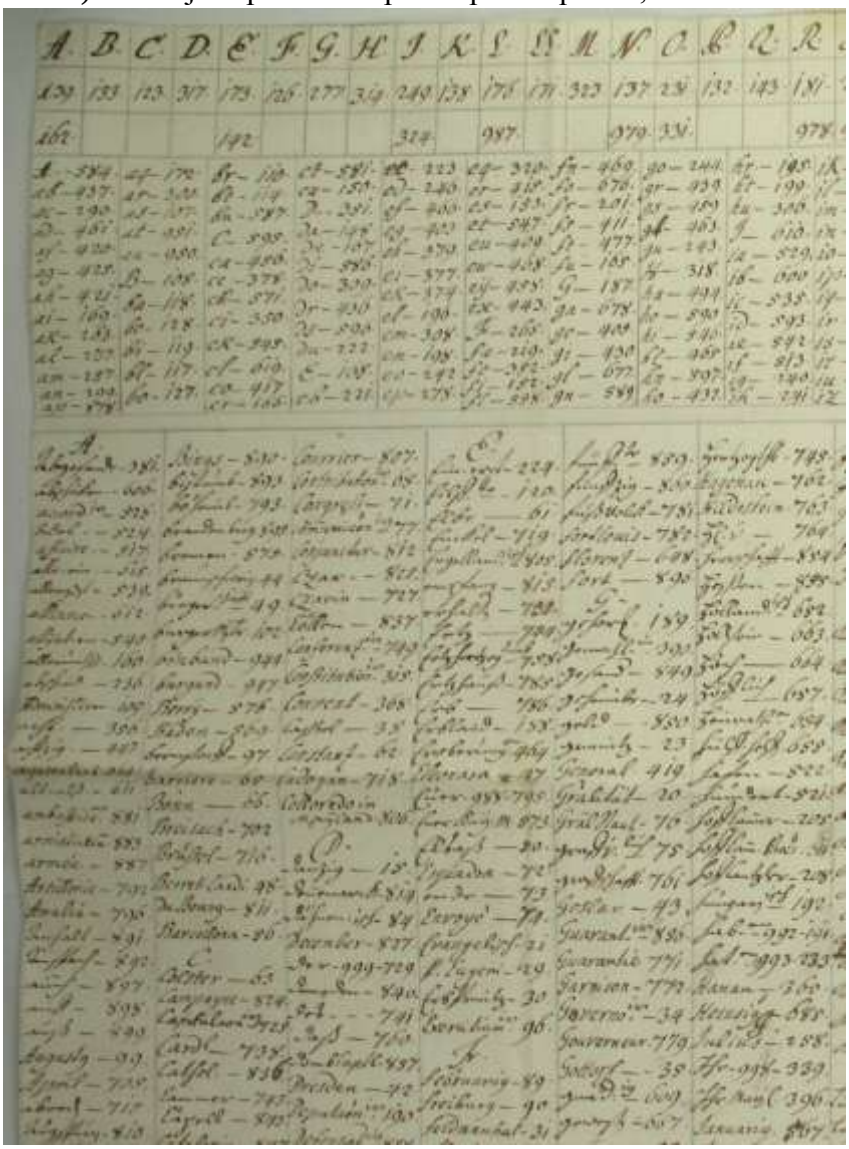
[18] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 12, i. č. 330.

[19] Tamtéž, RA Verdugů, karton č. 2, i. č. 29.

[20] Z jiných způsobů psaní znaků šifrové abecedy mohl číslicím nejlépe konkurovat systém, v němž se šifrové znaky zapisovaly pomocí kombinace písmen (např. ab, ac, ad...). Při stejné míře bezpečnosti obou systémů je ale jeho nevýhodou, že se v něm uživatelům hůře orientuje než v zažité desítkové soustavě.

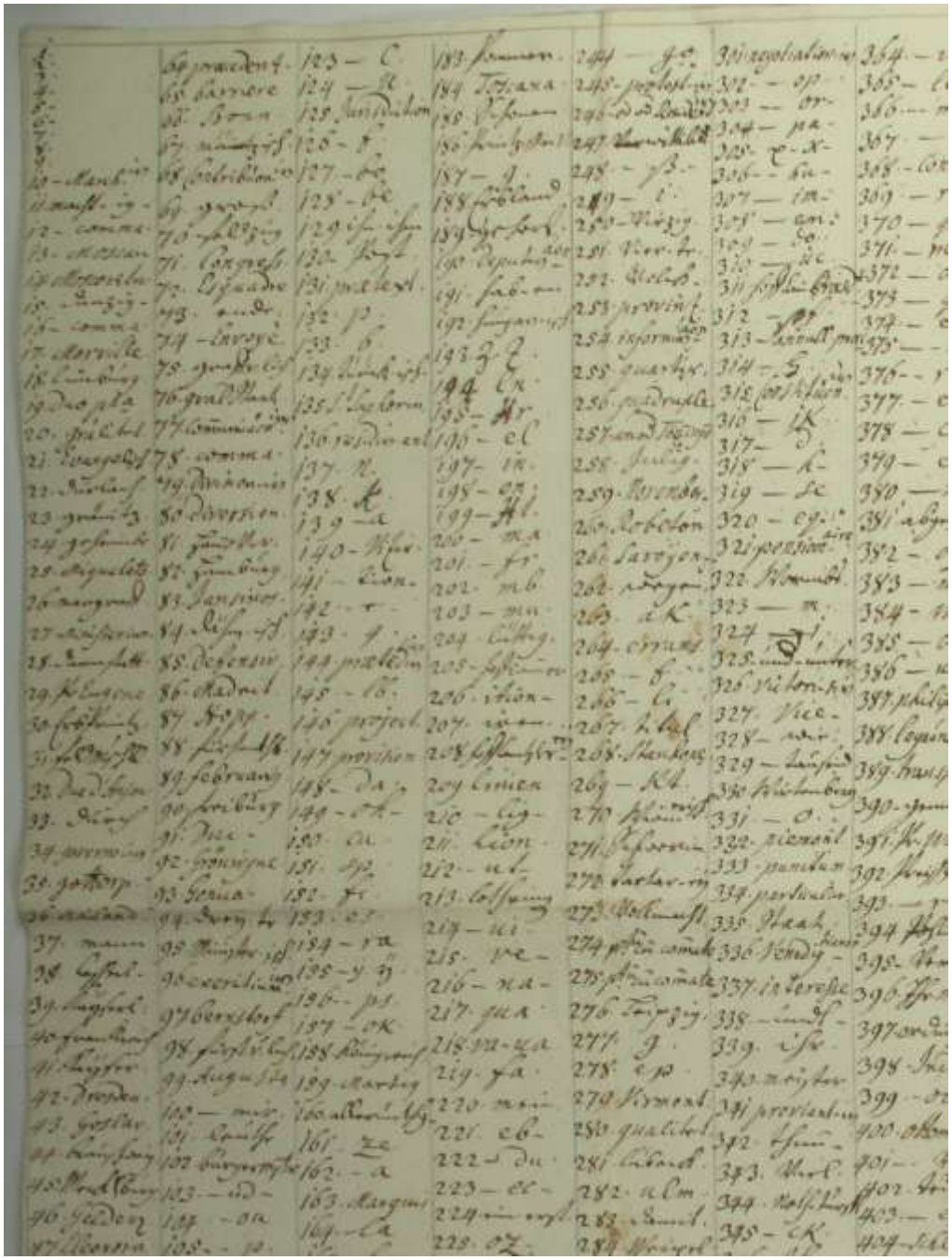
[21] Pro názorné sledování tohoto vývoje výborně poslouží především sbírka klíčů. SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 164, i. č. 1403, sign. 103. Klíče sice většinou nejsou datované, ale ve velkém množství případů je lze datovat alespoň přibližně. K možnostem datace se vyjadřuji výše.

vybráno několik číslic (zpravidla tři), které se odmýšlely i pokud byly součástí víceciferné číslice. Pokud bychom za tyto klamače zvolili číslice 1, 2 a 3, pak by se číslice 167 četla jako 67, 627 nebo 1367 také jako 67 a např. číslice 123 by neoznačovala vůbec nic. V novějších nomenklátorech se také postupně objevuje čím dál více kódů a v 18. století už bylo obvyklé, že jich bylo i mnoho set. Nejdříve se u složitějších nomenklátorů postupně zvětšovala velikost papíru, na němž byly zapsány, až začaly být zaznamenávány do sešitů, v nichž lze spatřovat zárodek kódové knihy. Další změna postihla způsob tvorby kódů. Dříve bylo obvyklé řadit všechny kódy v nomenklátoru podle abecedy a v rámci této abecední řady jim vzestupně přidělovat číslice (např. aber = 100, als = 101, allezeit = 102, auch = 103, auf = 104, alsogleich = 106, alle = 107 atd.).[22] Jak je z předchozí posloupnosti patrné, v rámci okruhu slov začínajících na stejné písmeno většinou nebylo abecední řazení důsledné. Výhodou bylo, že se takový klíč mohl pohodlně užívat pro psaní i čtení šifrovaných zpráv, a naopak nevýhodou, že to mohlo případnému luštiteli šifry velice ulehčit její prolomení. Porušením této zvyklosti a přiřazováním číslic ke kódům víceméně náhodně se tedy výrazně posílila bezpečnost šifry, ale na druhou stranu bylo potřeba vytvořit dva odlišné klíče pro šifrování a dešifrování zprávy. V prvním byly kódy řazeny abecedně a ve druhém podle číslic (viz *obr. č. 12* a *13*).



Obrázek 12 – Detail nomenklátoru užívaného pro korespondenci říšské dvorní rady s císařským vyslancem v Nizozemí – Leopoldem Viktorínem z Windischgrätzu, [kolem roku 1720]. Nomenklátor byl vyhotoven ve dvou variantách. V této variantě jsou bigramy i kódy seřazeny podle abecedy a sloužila pro šifrování. *SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 164, i. č. 1403, sign. 103.*

[22] Viz klíč hraběte Windischgrätze s Christianem Pentenriederem svobodným pánem z Adelshausenu. Tamtéž.



Obrázek 13 – Detail nomenklátoru užívaného pro korespondenci říšské dvorní rady s císařským vyslancem v Nizozemí – Leopoldem Viktorínem z Windischgrätzu, [kolem roku 1720]. V této variantě jsou bigramy i kódy seřazeny podle číselné hodnoty znaků šifrové abecedy a sloužila pro dešifrování. *SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 164, i. č. 1403, sign. 103.*

Ze zkoumaných pramenů je patrné, že používání šifer prošlo ve sledovaném období výrazným vývojem. Ten však nebyl ani tak odrazem nejnovějších vědeckých poznatků, které byly v dané době oproti běžné praxi na mnohem vyšší úrovni, ale spíše výsledkem konkrétních potřeb pisatelů. Ty byly určovány především nároky na bezpečnost a zároveň co nejpohodlnější použití šifry. Složitost šifrovacího systému tedy byla volena především s ohledem na závažnost předávaného sdělení a s tím související představu šifranta o motivaci a

schopnosti případného luštitele šifru zlomit. Nejsložitější šifry tedy byly logicky používány v prostředí panovnického dvora a pro diplomatickou korespondenci.

Ve vojenském prostředí bývaly obvykle klíče o něco jednodušší. V době války většinou vyvstala potřeba předávat zprávy velmi rychle. Přitom obvykle bylo přirozenou vlastností skutečně naléhavých zpráv, že také rychle zastarávaly. Vojevůdci tak mohli mít minimálně dva dobré důvody, proč užívat jednodušších klíčů. Jednak se s jejich pomocí rychleji šifrovalo a dešifrovalo, jednak mohli u velkého množství zpráv důvěřovat v to, že doba, kterou by nepřítel šifrovanou zprávu luštil, by snížila hodnotu informace v ní předávané. Zůstával ale problém, že protivník by po vyluštění zprávy získal klíč, s jehož pomocí by mohl dešifrovat další zachycené zprávy. Pro tento případ se ale asi dalo oprávněně očekávat, že by se odesilatel o zachycení zprávy relativně brzy dozvěděl (nejpozději v okamžik očekávané odpovědi) a měl možnost pro další potřebu klíč změnit. Ze zkoumaných pramenů je patrné, že k zachycování dopisů skutečně docházelo. Již výše byly uvedeny opisy zadržených dopisů Karla Robmhapa ze Suché Alžbětě Amálii landkraběnce hesenské.[23] Mezi písemnostmi válečné kanceláře Matyáše Gallase se dochovala také kopie dopisu Alexandra Erskiho z 15. července 1644, adresovaného Johanu Adlerovi Salviovi, radovi a dvorskému kancléři švédského krále a vyslance na mírových jednáních v Německu.[24] I v tomto případě šlo nepochybně o kopii zachyceného dopisu, protože na jeho zadní straně je připsáno *Copia Intercipirten Schreibens*. Ani jeden ze zadržených dopisů není dešifrován, a tak se zdá, že v tomto případě šifrování splnilo svůj účel.

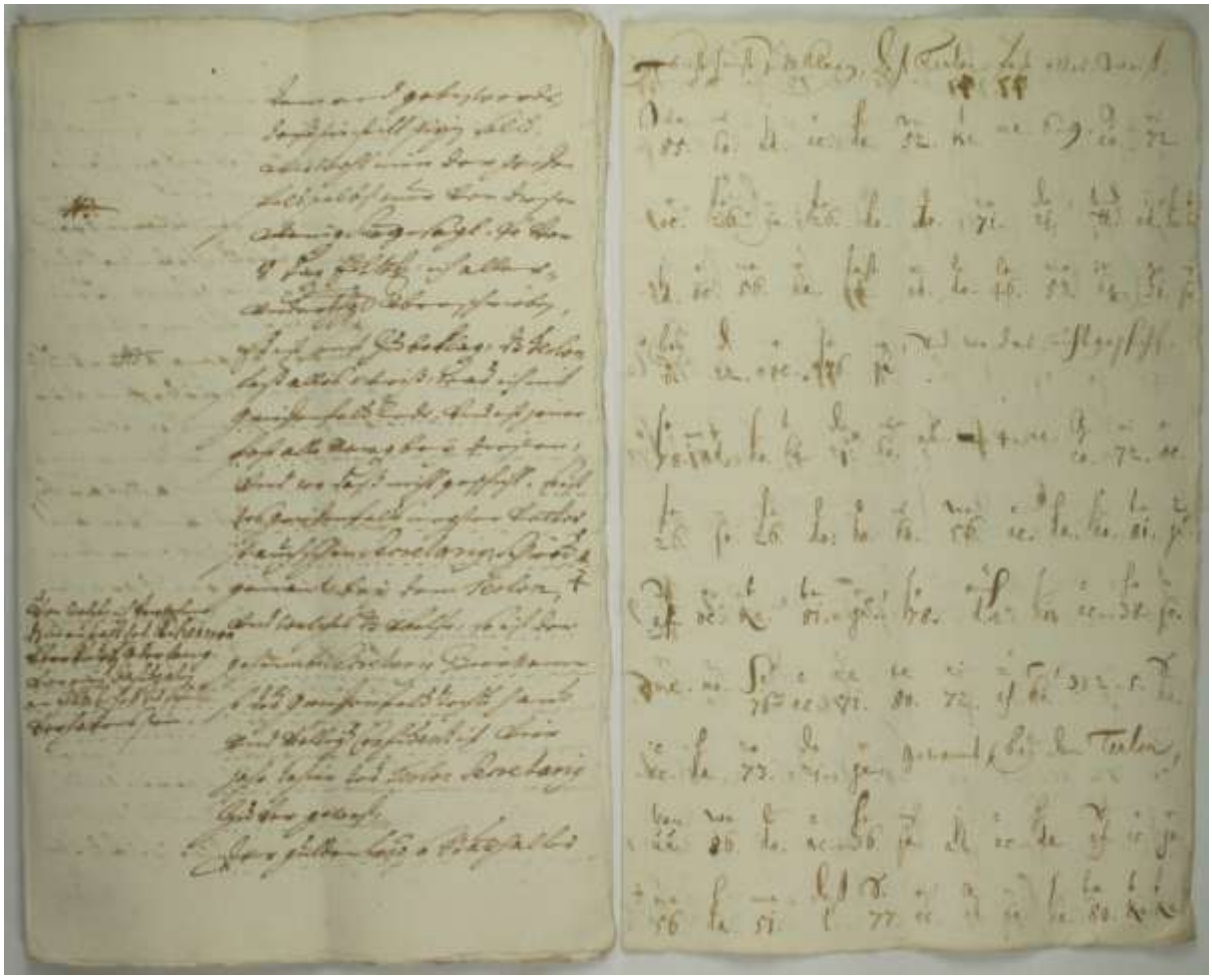
Nejjednodušší klíče byly obvykle užívány pro soukromou korespondenci, u níž se dalo v mnohem menší míře očekávat, že by se někdo znalý luštění šifer snažil o její zachycení a rozluštění obsahu. Většinou chránila pravděpodobně jen před náhodným nechtěným čtenářem. Příkladem může být klíč, který roku 1721 pro vzájemnou korespondenci užívali bratři Leopold Viktorín a Ernst Fridrich Windischgrätzové.[25] Ačkoli oba byli zvyklí při písemném styku se dvorem používat složité nomenklátory, pro jejich vlastní potřebu jim stačila mnohem jednodušší homofonní šifra a asi 200 kódů. Vzhledem k jejich postavení bylo nebezpečí snahy o získání obsahu jejich dopisů nepovolanou osobou větší než u ryze soukromých osob. Přesto tento klíč pokládali za dostačující.[26]

Některé klíče byly určeny vyloženě pro korespondenci pouze dvou osob, jiné sloužily většímu okruhu pisatelů. Druhý případ míval více podob. Např. již dříve uvedený Jan Hartvík z Nostitz používal stálého osobního klíče, který sloužil pro okruh jeho důvěrných korespondentů, ale není příliš pravděpodobné, že by oni sami užívali tento klíč pro korespondenci mezi sebou.[27] Některé klíče byly zase užívány určitým více či méně omezeným okruhem osob, aniž by jedna z nich byla ústřední postavou. Z označení některých

[23] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 10, i. č. 209.
[24] SOA v Litoměřicích – pobočka Děčín, HS Clam–Gallasů karton č. 381, i. č. 1397, sign. XV/9.
[25] SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 202, i. č. 1433, sign. 133.
[26] Ve svých dopisech se ostatně kromě hospodářských záležitostí rodiny zabývali především politickými záležitostmi a děním u dvora.
[27] Dopisy šifrované pomocí tohoto klíče viz SOA v Plzni, pracoviště Klášter, RA Nostitz–Rienecků, karton č. 13–14, i. č. 77–78, sign. FF 8, FF 9.

klíčů vyplývá, že ve dvorském prostředí se klíče mimo jiné označovaly jako *cifra particularis*, která sloužila pro korespondenci dvou nebo o něco málo většího počtu osob, anebo *cifra generalis*, která byla užívána širokým okruhem pisatelů, např. císařem a všemi jeho ministry.[28]

Zkoumané prameny také poskytují informace o samotném vzniku konkrétních šifrovaných zpráv. Proces vyhotovení šifrovaného dopisu patrně většinou probíhal zhruba takto: Odesilatel napsal nebo nadiktoval písaři koncept dopisu. V něm byly podtrženy či jinak vyznačeny pasáže, které měly být šifrované. Vyznačené části textu písař přepsal na zvláštní papír, přičemž mezi jednotlivými písmeny obvykle ponechával mezeru, aby se nad ně vešly odpovídající znaky šifrové abecedy (viz *obr. 14*).



Obrázek 14 – Koncept relace Gottlieba Amadea z Windischgrätzu dvorské kanceláři z 11. listopadu 1673 z Kodaně. Na levém snímku je celkový koncept s vyznačeným textem určeným k šifrování (podtržen přerušovanou čarou) a na pravém snímku následně vyhotovený koncept sloužící pro zašifrování téhož textu. *SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 193, i. č. 1423, sign. 123.*

V případě, že šlo o homofonní substituci, snažil se znaky šifrové abecedy určené pro jeden znak otevřené abecedy pokud možno pravidelně střídat. Poté s pomocí listu se šifrovým

[28] Viz např. SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 164, i. č. 1403, sign. 103.

textem a původního konceptu vyhotovil čistopis. Adresát nebo jeho sekretář pak po doručení dopisu pomocí dohodnutého klíče dešifroval text buď na zvláštní list papíru, anebo vepsal otevřený text přímo do dopisu. Ve druhém případě text vpisoval na prázdné okraje dopisu nebo přímo do řádků. Někdy dokonce vypisoval získaná písmena přímo nad znaky šifrového textu. Otevřený text dešifrovaný jedním z těchto způsobů se dochoval pro většinu dopisů, které jsem zkoumal. Někdy třeba jen v jednom dopise z celého souboru, ale to stačí pro získání klíče ke všem zprávám utajeným stejnou šifrou.[29]

Ve vzorku zhruba čtyřiceti zkoumaných šifer jsem mohl zhruba k 70 % z nich získat klíč díky tomu, že alespoň jeden dopis z korespondence dvou osob byl dešifrován přímo adresátem. Přibližně v 10 % případů dopisy dešifrovány nebyly, ale bylo na ně možné aplikovat klíče, které se nacházely na jiném místě fondu.[30] Ve zbývajících asi 20 % nebyl dopis ani dešifrován, ani jsem nenalezl klíč. Z nich kolem 8 % tvořily dopisy, které nebyly dešifrovány, protože se nedostaly do rukou adresáta a jejich skutečný příjemce neznal klíč. Zbývá tedy pouhých asi 12 % ze všech souborů dopisů, u nichž se nedochoval žádný dešifrovaný text, ačkoli adresát musel znát klíč. Navíc bylo možné část z nich vyluštit kvůli chybě písaře nebo díky tomu, že jsou šifrovány pomocí jednoduché substituce. Díky značnému množství dešifrovaných zpráv se mi podařilo částečně nebo úplně sestavit přes třicet různých klíčů. Několik desítek klíčů také bylo uloženo ve sbírkách klíčů[31] nebo bylo přiloženo ke korespondenci. Většinu z nich ale nebylo možné použít pro dešifrování dochovaných dopisů.

V méně početných případech, kdy text není dešifrován, existuje několik možností, jak k němu získat klíč. Předně je možné pokusit se hledat klíč na jiném místě téhož fondu, např. ve sbírce klíčů, pokud se ve fondu nachází. Další možností je zjistit srovnáním, zda na šifrový text nelze uplatnit některý z klíčů stejného adresáta a ze stejné doby. Složitější možností je pátrání v jiných fondech či archivech po dopisech stejného odesilatele, nejlépe pak přímo v písemné pozůstalosti odesilatele, v němž by se mohla nacházet přijatá korespondence od adresáta původního dopisu.[32] Tento způsob však většinou vyžaduje i značnou dávku štěstí a v některých případech může být zdlouhavější než luštění šifry. Mám tím na mysli především ty případy, kdy je text utajen pomocí jednoduché substituce. Ta se dá poměrně spolehlivě luštit v celkem krátkém časovém úseku. Jednoduchou substituci lze většinou rozpoznat tak, že počet znaků šifrové abecedy zhruba odpovídá počtu znaků abecedy otevřené. Složitější je její rozpoznání v případě, že je doplněna kódy.

---

[29] Pro uvedený postup šifrování dopisů poslouží jako názorný příklad např. koncepty šifrovaných relací Gottlieba z Windischgrätzu dvorské kanceláři z let 1773–1775. Tamtéž, karton č. 192–193, i. č. 1423, sign. 193.

[30] Ani jednou jsem se ve zkoumaném vzorku korespondence nesetkal s tím, že by byl přímo k ní přiložen správný klíč. Ačkoli klíče v několika případech ke korespondenci přiložené byly, nebylo možné je na ni aplikovat.

[31] Mezi zkoumanými archiváliemi se největší sbírka nachází ve fondu RA Windischgrätzů. SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 164, i. č. 1403, sign. 103. Menší soubor klíčů se nachází i v SOA v Litoměřicích – pobočka Děčín, HS Clam–Gallasů, karton č. 392, i. č. 1397, sign. XV/20.

[32] Např. vzájemná korespondence Matyáše Gallase a Ottavia Piccolominiho se nachází jak ve fondu HS Clam–Gallasů, tak ve fondu RA Piccolomini. V tomto případě jsou ale dopisy dešifrovány v obou fondech. SOA v Litoměřicích – pobočka Děčín, HS Clam–Gallasů, karton č. 350, i. č. 1397, sign. XVIII/8; SOA v Zámrsku,

Naopak luštit složitější nomenklátory s homofonní substitucí a bigramy je velmi složité. Existují ale způsoby, jak řešit i tento druh šifer. Ani homofonní substituce totiž obvykle nebývá dokonale odolná vůči frekvenční analýze. Pomoci zde může především analýza četnosti bigramů, trigramů, ale i delších řetězců znaků. Vždy záleží na složitosti nomenklátoru a také na délce textu. Obecně platí, že čím delší text, tím lépe se provádí kryptoanalýza. Ačkoli tedy nejsou ani takové úlohy neřešitelné, luštění může zabrat velké množství času s nejistým výsledkem.

Velikým pomocníkem v luštění je dnes výpočetní technika. Počítače však dodnes nedokáží řešit tento druh šifer tzv. „hrubou silou“, tj. výpočtem všech kombinací, a tak nám mohou pomoci především mnohonásobně rychlejším mechanickým propočtem kombinací znaků. Existují dokonce i programy, které umí v šifrovém textu určit samohlásky, ovšem hlavně u jednoduché substituce. Vcelku ale současným luštitelům zůstávají obdobné postupy, jakých užívali kryptoanalytikové v 16.–18. století. Nespornou výhodou současníků je možnost využití již zmíněných počítačů a do jisté míry nevýhodou vesměs malá zkušenost s tímto konkrétním typem šifer, protože se v současné době již prakticky neužívají, a také výrazně menší znalost dobových reálií.

Velkou pomocí při luštění mohou být chyby šifrantů. Nejčastěji vyskytující se chybou je oddělování jednotlivých slov textu. To přináší jen pramalý užitek pro urychlení dešifrování textu, ale výraznou měrou to napomáhá kryptoanalytikovi v luštění.[33] Vyloženě hrubou chybou je psaní diakritických znamének a interpunkce. Jako příklad mohu uvést dopis zaslaný Maxmiliánu Trauttmansdorffovi od Johanna Karla Schönburga z 20. června 1637 z Madridu.[34] Část textu dopisu byla utajena homofonní šifrou a nebyla dešifrována. Vzhledem k nepříliš dlouhému šifrovému textu by pravděpodobně bylo obtížné šifru rozluštit i přesto, že Schönburg, nebo spíše jeho sekretář, odděloval slova. Kromě toho ale také psal za zkratky dvojtečku a dokonce ještě drobným písmem nahoře za dvojtečkou dopisoval koncovky zkrácených slov. V šifrovém textu takovýmto způsobem použil v té době obvyklé německé zkratky pro španělského krále *Cath[olische] König[liche] May[estät]*, která se dokonce objevuje ve stejném dopise v otevřeném textu o několik řádek výše. Díky tomu jsem mohl získat několik znaků šifrové abecedy, které po doplnění do textu pomohly odhalit další znaky. Dosazením byla mimo jiné vyluštěna část slova *ni.ht* (tedy zcela jistě *nicht*), čímž byl odhalen další šifrový znak pro *C*. Po jeho dosazení získalo zřetelnější obrysy další slovo – *.ico...i.i.* Vzhledem k době, ze které dopis pochází, se zdálo nanejvýš pravděpodobné, že neúplné slovo označovalo jméno jednoho z císařských generálů, jímž byl (Ottavio) *Picolomini*.[35] Tím bylo možné získat další znaky a postupovat obdobným postupem dále až k získání celého klíče (viz *obr. 15*).[36]

RA Piccolominiů, i. č. 17880, sign. 25/1.

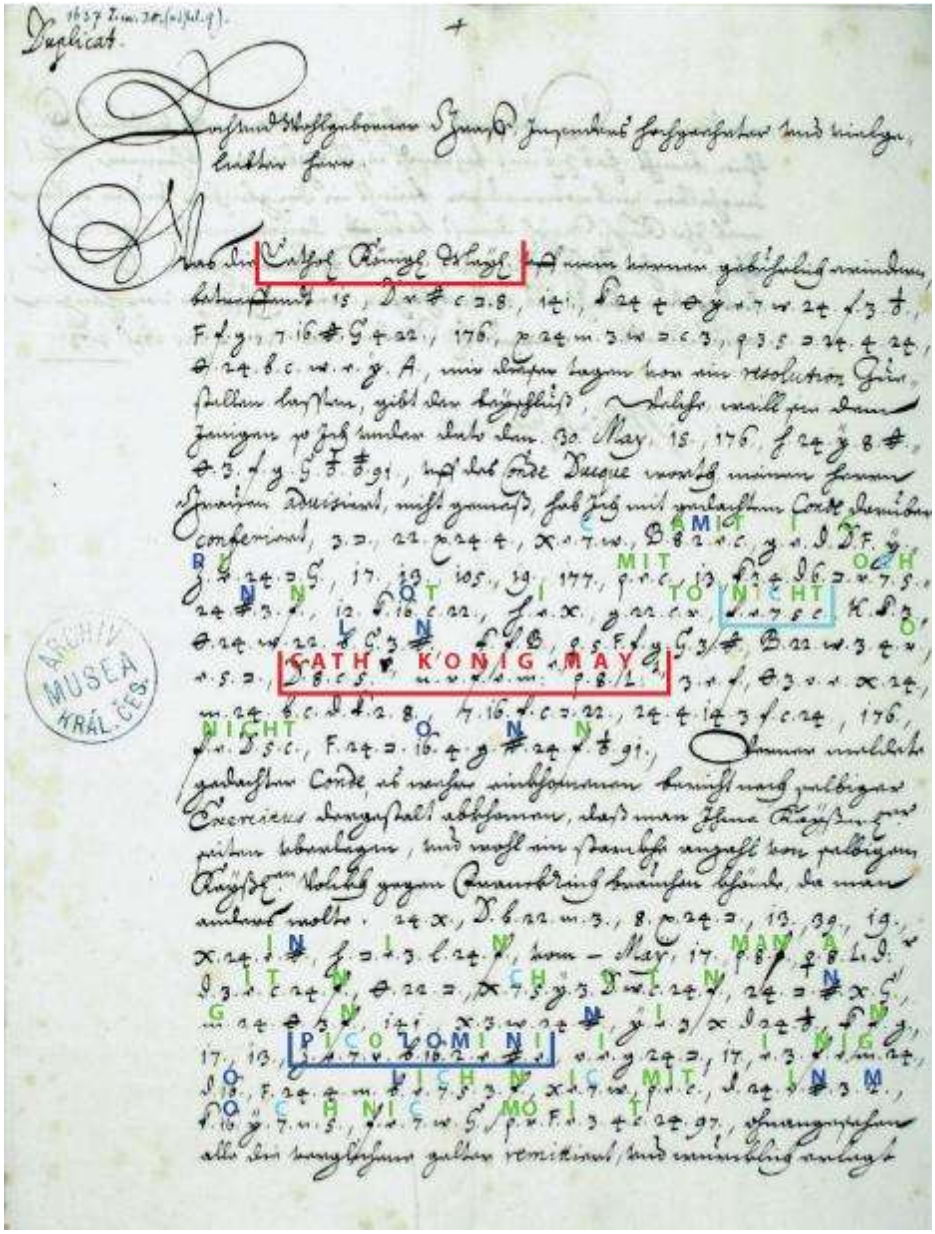
[33] Mezi zkoumanými dopisy se objevuje několik, v nichž jsou slova oddělována, ve většině z nich je však psán text jednolitě.

[34] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 12, i. č. 271.

[35] Správně *Piccolomini*, ovšem dvojhláska byla šifrantem zjednodušena.

[36] Později jsem zjistil, že tento klíč byl již dříve publikován. Hildegard Ernst jej nalezla v Rakouském státním archivu. Viz ERNST, Hildegard. Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid

Obrázek 15 – Dopis Johanna Karla von Schönburg Maxmiliáno z Trauttmansdorffu z 20. června 1637 z Madridu (první strana). Při šifrování tohoto dopisu se dopustil šifrant hrubé chyby, když v šifrovém textu vyznačil obvyklým způsobem zkratku *Cath[olische] König[liche] May[estät]*. Díky této chybě mohl být rozluštěn celý text. První čtyři kroky luštění jsou znázorněny na tomto obrázku. 1. krok – dosazení červených písmen za šifrový text, 2. krok – dosazení zelených písmen, 3. krok – dosazení modrých písmen, 4. krok – dosazení fialových písmen. *SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 8, i. č. 148.*



und Brüssel, 1635–1642. *Mitteilungen des Österreichischen Staatsarchivs*, 42, 1992, s. 117. To sice snižuje hodnotu luštitelského úspěchu, ale nic neubírá na názornosti tohoto příkladu možných chyb šifrantů. Je nanejvýš pravděpodobné, že pro zkušeného kryptoanalytika té doby by vyluštění této šifry nepředstavovalo větší problém. Hildegard Ernst se ve druhém díle svého článku zabývá podobnou chybou písaře jiného císařského vyslance v Madridu Františka markýze dal Caretto, di Grana e Savona, hraběte di Millesimo. V tomto případě pisatel nešifroval číslice, za nimiž se vzhledem k jejich vysoké hodnotě dal očekávat název měnové jednotky (v tomto případě Taller). Na základě této zásadní chyby dokázala autorka šifru rozluštit. Dále v textu sděluje, že ani v říšské kanceláři pravděpodobně neexistovalo systematické zaškolování šifrantů do způsobů, jak si počínat při vyhotovování šifry. To by mohlo vysvětlovat poměrně překvapující zjištění, že šifrované dopisy dvou tak velmi významných osob, jimiž císařští vyslanci na španělském dvoře bezpochyby byli, vykazují tak závažné nedostatky. Jako další možný důvod uvádí možnou časovou tíseň. Článek přináší také příklady dalších možných chyb šifrantů. TÁŽ. Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel, *1635–1642. Teil II. Mitteilungen des Österreichischen Staatsarchivs*, 45, 1997, s. 211–221.

Zajímavou otázkou také je, zda bylo bezpečnější psát pomocí šifer dlouhý jednolitý text, nebo naopak jen jednotlivá důležitá slova. Psaní dlouhého souvislého textu umožňuje případnému luštiteli získat poměrně velký počet znaků šifrové abecedy pro provedení frekvenční analýzy. Dosazování jen jednotlivých slov nebo jejich krátkých řetězců má zase tu nevýhodu, že si je lze spíše domyslet. Tento postup ale naopak poskytuje mnohem méně prostoru pro frekvenční analýzu. Jen těžko lze rozhodnout, který z uvedených způsobů je lepší, a pravděpodobně bude platit, že záleží na šikovnosti šifranta a na způsobu provedení šifrování v daném konkrétním případě. Nejméně šťastným řešením je ale patrně jakýsi kompromis mezi oběma řešeními, tj. psaní dlouhého šifrového textu, ale hojně prokládaného textem otevřeným. Nejobtížnější a myslím, že pro současníka téměř neřešitelné, jsou šifry s výraznou převahou kódů. Kódy samy o sobě se luští mnohem hůře než substituční šifry a navíc je při tom potřeba perfektně se orientovat v dobových reáliích, což současník zřejmě nikdy nezvládne tak dobře, jako přímí aktéři soudobého politického dění.

Při luštění musí také kryptoanalytik počítat se zvláštnostmi dobového jazyka. Dochované šifrované dopisy jsou psány většinou nejvýznamnějšími evropskými jazyky té doby – německy, francouzsky, italsky, španělsky a latinsky. Jako příklad pro jazykové odlišnosti si vyberu němčinu, jejíž pravopis v té době byl ze všech vyjmenovaných jazyků asi nejméně ustálený. Přesto jsem na vzorku dobové korespondence zjistil, že frekvence jednotlivých písmen v raně novověkých textech celkem odpovídá i jejich současnému výskytu.[37] V úvahu je však třeba vzít některé zvláštnosti tehdejšího pravopisu. Např. hlásky *z* a *d* byly často psány jako *tz* a *dt* (např. *Hertzog, baldt*). Zajímavé však je, že šifranti si pravopis pro účely sestavení šifrového textu často zjednodušovali a psali foneticky a mnohdy tím vlastně předběhli pozdější pravopisné změny, když právě např. výše zmíněné znaky *tz* a *dt* zkracovali na dnes obvyklé *z* a *d*. Při aplikování těchto zásad někdy mohlo dojít i k poměrně velké změně grafické podoby slova, např. *geführet* mohlo být zapsáno jako *gefirt*. Často také byly zjednodušovány dvojhlásky (např. *ll, ss, tt* ad.). Tyto úpravy sice nedělali úplně všichni šifranti, ale při luštění textu je s nimi třeba počítat.

Dochovaná korespondence také zachycuje pohled jejích pisatelů na způsoby využívání šifer a na jejich bezpečnost. Některé dochované zprávy potvrzují logický předpoklad, že šifrování bylo obvykle využíváno skutečně v těch nejnaléhavějších případech. Například český a uherský král Ferdinand III. na konci svého dopisu Maxmiliánu Trauttmansdorffovi z 13. listopadu 1634 výslovně zmiňuje, že dopis raději šifruje a posílá s ním svého osobního posla.[38] Přitom žádný jiný z jeho dopisů Trauttmansdorffovi, jejichž opisy se ve fondu

[37] Provedl jsem frekvenční analýzu prvních 1000 znaků z edice korespondence císaře Leopolda I. s jeho vyslancem ve Španělsku Františkem Eusebiem hrabětem z Pöttingu. LANDWEHR VON PRAGENAU, Moriz – PRIBRAM, Alfred Francis (edd.). *Privatbriefe Kaiser Leopold I. an den Grafen F. E. Pötting 1662–1673*. Wien : Carl Gerold´s Sohn 1903.

[38] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 6, i. č. 68.

dochovaly, šifrován nebyl. Na druhou stranu je vidět, že ani šifrování nebylo považováno za dokonale bezpečný způsob utajení zprávy. To je patrné např. ze zprávy Petera hraběte von Holzappel témuž adresátovi z 31. července 1646,[39] v níž sděluje, že se v místě jeho pobytu dějí takové věci, že neví, zda je vůbec může nechat psát. Nejraději by Trauttmansdorffovi vše sdělil osobně. Zde pravděpodobně hrála roli kromě strachu ze zachycení dopisu nepřáteli také obava z toho, že by obsah zprávy sdělil další osobě, tj. písaři. Vzhledem k tomu, že se písaři či sekretáři obvykle zabývali i šifrováním a dešifrováním dopisů, museli je jejich pánové považovat za velmi spolehlivé osoby. I přesto ale zřejmě mohl existovat okruh informací, které si netroufali sdělit ani jim. I když dá se předpokládat, že v těchto úvahách hrála rozhodující roli míra důvěry mezi pánem a sekretářem, která se mohla lišit v jednotlivých případech.

V některých dopisech se také vyskytují rady nadřízených osob, kdy a jakým způsobem šifru používat. To činí např. císař Karel VI. ve svém psaní Leopoldu Viktorínovi z Windischgrätzu ze 3. února 1720.[40] Na dopisu je kromě toho zajímavé, že císař sděluje Windischgrätzovi, že mu bude buď s tímto, nebo s dalším listem zaslán nový klíč, který má užívat výhradně pro korespondenci s ním, zatímco starý klíč bude nadále sloužit pro výměnu zpráv s dvorskou kanceláří. Další dopisy Karla VI. už byly skutečně šifrovány podle nového klíče.[41] Občasná výměna klíče samozřejmě byla a dodnes je jedním z důležitých předpokladů pro minimalizování rizika odhalení utajovaných zpráv. Dalším příkladem je korespondence Maxmiliána z Taruttmansdorffu s Františkem Pavlem de Lisola, pro niž bylo v létě roku 1645 užíváno jiné šifry než v prosinci téhož roku.[42] Doklady o změně klíče se dochovaly i v jiných archivech. Např. ve fondu Historická sbírka Clam-Gallasů je uložen list papíru, na němž jsou uvedeny dva klíče pro korespondenci Matyáše Gallase a Ottavia Piccolominiho. Jeden z nich je označen jako starý klíč a druhý jako nový.[43]

V souvislosti s tématikou zabezpečení šifer vyvstává na závěr ještě otázka, jak bylo toto zabezpečení účinné v praxi a nakolik se dařilo v dané době šifrovanou korespondenci zachycovat a luštit. Ta byla nadnesena již výše, když byly uvedeny dva příklady dopisů, které byly uzmuty nepřáteli, a bylo řečeno, že ani v jednom případě nebyly dešifrovány. Z tak malého vzorku však nelze vyvozovat obecné závěry. Abychom se alespoň přiblížili řešení

[39] Tamtéž, karton č. 9, i. č. 184.
[40] SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 5, i. č. 694, sign. 669A/III. b.
[41] Oba klíče se dochovaly ve sbírce klíčů. Tamtéž, karton č. 164, i. č. 1403, sign. 103.
[42] Tamtéž, RA Trauttmansdorffů, karton č. 10, i. č. 209.
[43] SOA v Litoměřicích – pobočka Děčín, HS Clam–Gallasů, karton č. 392, i. č. 1397, sign. XV/20. Výměnou klíčů se zabývá také Hildegard Ernst, která zaznamenala i případy, kdy jeden klíč nenahrazoval definitivně klíč předchozí, ale oba klíče byly nadále používány paralelně. ERNST, Hildegard. Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel, 1635–1642. *Mitteilungen des Österreichischen Staatsarchivs*, 42, 1992, s. 110–111. Způsob výměny klíče pro korespondenci velkého množství osob ilustrativně popisuje také HULEC, Otakar. Konspirativní charakter předbělohorské protistavovské opozice. *Jihočeský sborník historický* 30, 1961, s. 100–101.

této, ale i mnohých dalších otázek, bude potřeba prostudovat nejen mnohem větší množství šifrovaných dopisů z různých archivů, ale i jejich obsah.

Obrázek 16 – Detail z portrétního obrazu Maxmiliána z Trauttmansdorffu, uloženého na Státním hradu a zámku v Horšovském Týně. *Foto převzato z archivu Marie Mírkové.*

Konec

B. Andreas Figl – rakúsky dôstojník a kryptológ

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

1 Úvod

Motiváciou k napísaniu tohto textu bol článok uverejnený pod názvom *Andreas Figl – Nestor rakúskej kryptológie* v časopise Crypto-World 7-8/2012 ([6], str. 2–13). Na tento príspevok by som tu chcel reagovať, upresniť a doplniť niektoré údaje v ňom uvedené.

Nasledujúci text je rozdelený na dve samostatné časti. Prvá sa týka života a pôsobenia Andreasa Figla ako kryptológa a druhá jeho knihy *Systeme des Dechiffrierens*. Tieto časti sú úplne nezávislé.

2 Andreas Figl

O živote a pôsobení Andreasa Figla toho nie je moc známe. Na nemeckej Wikipédii ([7]) nájdeme nasledovné údaje:

- narodil sa 22. júna 1873 vo Viedni,
- vyrastal vo Viedni a Sarajeve
- ako 14-ročný nastúpil do kadetskej školy
- v roku 1891 prišiel ako poručík do Dalmácie
- v roku 1910, po úraze, bol poslaný do výslužby
- v roku 1911 bol reaktivovaný a pomáhal zakladať lúštiteľskú službu
- v rokoch 1920 až 1937 pracoval na ministerstve zahraničných vecí
- v roku 1926 vyšla jeho kniha *Systeme des Chiffrierens*
- v roku 1960 sa stal poradcom povojnového Bundesheer-u (armády)
- umrel 11. novembra 1967 a je pochovaný v Salzburgu

V podstate identické údaje, ale v čestine, sa nachádzajú na Janečkovom kryptoblogu [4] a ešte aj na webovej stránke ponúkajúcej jeho biografiu od Otta J. Horaka (opäť v nemčine)[1]. Moc viac toho o Andreasovi Figlovi na webe nenájdeme.

Z knižných publikácií sú mi známe len dve knihy od Otta J. Horaka. Obe sú uvedené v použitej literatúre k [6].

V už spomínanom článku [6] sú uvedené v podstate všetky tieto biografické údaje a aj niektoré ďalšie a je to tam rozpísané trochu podrobnejšie a čitateľsky pútavejšie. Od stručných údajov uvedených vyššie sa tieto údaje líšia len v roku, kedy sa stal Figl poručíkom (1893 oproti 1891), čo je však nepodstatný detail.

Obr. 1: Andreas Figl (* 22. 6. 1873 – † 11. 11. 1967) [8]

K Figlovym biografickým údajom by som chcel jednu informáciu poopraviť a nastoliť jednu otázku. V článku [6] sa hneď na úvodnej strane píše:

> *... Počas II. svetovej vojny bol najatý na prácu kryptoanalytika pre nacistické Nemecko, ale predtým než bol prepustený, Tretej ríši slúžil len 18 mesiacov. ...*

Takto formulovaná veta vzbudzuje dojem, že Figl sa prostredníctvom nejakého konkurzu prihlásil a bol prijatý na prácu kryptoanalytika pre Tretiu

[1] `http://buchhandel.de/detailansicht.aspx?isbn=978-3-85487-779-0`

ríšu. Tento dojem je ale pomerne ďaleko od pravdy. Ako je známe, Rakúsko bolo 12. marca 1938 pri tzv. *Anschluß-e* pripojené k Tretej ríši. Tento akt nebol o nič priateľskejší než obsadenie Čiech a vytvorenie Protektorátu Čechy a Morava. V Rakúsku počas 30-tych rokov minulého storočia síce tiež vládol fašistický režim[2], ale jeho vzťahy s Treťou ríšou boli všetko iné, len nie priateľské. Nacistická strana bola, až do doby krátko pred Anschluß-om, v Rakúsku zakázaná a fungovala len v ilegalite. Je preto nemysliteľné aby existoval nejaký štátny zamestnanec a špeciálne vysoký dôstojník pracujúci v lúštiteľskej službe, ktorý by sa otvorene hlásil k nacizmu, alebo s ním čo len sympatizoval. Ihneď po Anschluß-e bolo mnoho rakúskych politikov, vysokých štátnych úradníkov a samozrejme aj dôstojníkov, zaistených gestapom ako nepriateľské prípadne nespoľahlivé osoby. Viacerí z nich skončili v koncentrákoch alebo na popraviskách. Medzi zaistenými a internovanými dôstojníkmi bol aj Andreas Figl a gestapo sa pri jeho zadržaní dostalo aj k viacerým dôležitým materiálom lúštiteľskej služby. Po dlhšom čase a prostredníctvom ďalších osôb si Figla všimol rakúšan a SS Sturmbannführer Wilhelm Höttl, ktorý bol v tom čase zástupcom vedúceho Amt VI_E[3] R.S.H.A.[4] Figl, ktorý bol až do polovice roku 1941 v internácii SS, potom oficiálne fungoval ako „poradca“ Höttla vo Wansee pri Berlíne a pracoval aj ako inštruktor kryptológie pre R.S.H.A. Počas tejto práce pre Höttla sa mohol volnejšie pohybovať a získal čiastočne slobodu. Tieto fakty popisujúce Figlovo zaistenie a neskôr prácu pre R.S.H.A. sa nachádzajú v [1] (str. 63), [2] (str. 60–61) a [5] (str. 449–453). V uvedených zdrojoch sa špekuluje aj nad tým, že Figl sa mohol počas práce pre Höttla podielať aj na zostavovaní bigramových šifrovacích tabuliek pre R.S.H.A. (príklad takejto tabuľky je notoricky známy a nachádza sa vo všetkých uvedených knihách, ako aj v článku [6]).

Otázka, ktorú by som chcel nastoliť v súvislosti s Figlovými biografickými údajmi, je jeho hodnosť. Priznám sa rovno, že nemám k dispozícii žiadne 100 % hodnoverné údaje a informácie uvedené v použitej literatúre (tu, aj v [6]) sa rozchádzajú. Takže nasledujúce vety sú len mojími špekuláciami. Väčšinou sa o Figlovi píše ako o plukovníkovi. Aj v záhlaví jeho knihy [3] je uvedená hodnosť „Oberst a. D.“ čo je v preklade „plukovník vo výslužbe“. Treba ale brať do úvahy fakt, že originál tejto knihy vznikol niekedy okolo

[2]Historici ho nazývajú *austrofašizmus*.

[3]Amt VI_E = úrad VI_E, 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.

[4]R.S.H.A.= Reichssicherheitshauptamt bol úrad vedený Reichsführerom SS Heinrichom Himmlerom a zahŕňal všetky zložky štátnej bezpečnosti (kriminálna polícia, gestapo, spravodajská služba,...)

roku 1926[5], čo bolo zhruba desať rokov pred Figlovým odchodom do penzie. V knihách [1] a [5] sa uvádza, že gestapo zaistilo generála Andreasa Figla. Podľa týchto zdrojov bol teda Figl v čase zaistenia generál. Rovnako aj v mojich rozhovoroch s nemeckými kryptohistorikmi bol Figl väčšinou spomínaný ako generál. V knihe [2] (anglický preklad [1]) sa Figl uvádza ako plukovník, ale v súvislosti s obdobím dlho pred jeho zaistením. V časti týkajúcej sa 2. svetovej vojny (str. 60–61) chýba celý odstavec pod čiarou, ktorý je v [1] na str. 63 a v ktorom sa píše o Figlovi ako o generálovi. Takže z inkriminovaného obdobia tam nie je žiadna zmienka o Figlovej hodnosti. No a napokon na webe ([4] a [7]) sa píše o Figlovi ako o plukovníkovi, ale opäť len v súvislosti s obdobím dlho pred jeho zaistením. Zostáva preto otázka, či bol Figl plukovník, alebo generál. Ja sa, na základe mne dostupných informácii, skôr prikláňam k druhej možnosti. Ale ako som už spomenul na začiatku tohto odstavca, nemám na to žiadne hodnoverné a overené zdroje.

3 Systeme des Deschiffrierens

Ako už bolo spomínané aj v článku [6], prepis knihy *Systeme des Deschiffrierens* sa nachádza v Bavorskej štátnej knižnici v Mníchove. Uložený je v oddelení rukopisov a je možné sa k nemu dostať. Či a kde existuje originál mi nie je známe. Rovnako nie je presne známy rok napísania knihy, ale podľa už pomenutých indícii to muselo byť niekedy okolo roku 1926. Každopádne prepis uložený v knižnici pochádza až z obdobia po 2. svetovej vojne, k čomu sa ešte vrátim neskôr.

Autor prepisu, podľa mne dostupných informácií, nie je známy. Na strane s obsahom jednotlivých dielov je uvedená poznámka hovoriaca o tom, že doplnenia pochádzajú od jedného Figlovho žiaka[6]. Meno tohto žiaka sa ale nikde v knihe neuvádza.

Presný termín vzniku prepisu tiež nie je známy, ale určite to bolo až nejaký čas po 2. svetovej vojne, pretože text knihy obsahuje poznámky a informácie vzťahujúce sa k vojnovým udalostiam, šifrám a pod. Najviac takýchto informácií sa dá nájsť v tretej časti, ale niekoľko ich je aj v druhej časti. Napr. na strane 356 v tretej časti je poznámka hovoriaca, že: *„... šifra „Kammverfahren“[7] bola počas 2. svetovej vojny používaná jednou zo susedných krajín ...“* Meno krajiny sa síce menovite neuvádza, ale je tam uvedené (č) a Rakúsko ani Nemecko nemajú veľa susedných krajín, ktorých meno by

[5]Vtedy bolo vydanie avizované v jeho predchádzajúcej knihe, ale publikovanie bolo napokon úradne zakázané.

[6]Strany s obsahom jednotlivých dielov sú uvedené na konci tohto textu.

[7]Kammverfahren = Zubatka

sa začínalo na Č. Okrem toho aj príklad, na ktorom sa popisuje lúštenie Zubatky, obsahuje český text. Podobne sa v tretej časti popisuje aj lúštenie rôznych dvojitých transpozícií aké sa používali napr. v československých šifrách a na strane 339 začína popis lúštenia transpozície s trojuholníkovou tabuľkou, aká sa využívala aj v československej šifre „Eva“. Naviac zrejme ani jednotlivé časti prepisu nevznikali v rovnakom čase. Už na prvý pohľad je napr. zrejmé, že tretia časť je písaná na inom písacom stroji než prvé dve časti.

Samotná kniha je rozdelená na tri časti, ktoré majú 134, 231 a 187 strán. Zhruba tretinu z uvedeného počtu strán zaberajú prílohy. Prvé dve časti majú strany číslované priebežne, tretia časť má na začiatku asi 60 strán, ktoré narúšajú priebežné číslovanie a potom pokračuje stranou 289, čo by zodpovedalo priebežnému číslovaniu. Toto je vidno aj z priložených obsahov.

Vo všetkých troch častiach autor vysvetľuje opisované metódy a postupy na príkladoch depeší. Použité depeše vyzerajú reálne a pravdepodobne sa jedná o skutočné depeše z Figlovho archívu. Väčsina z nich sa vzťahuje ku 1. svetovej vojne, ale v druhej časti a ešte viac v tretej časti sú aj príklady depeší, ktoré veľmi pravdepodobne (pri niektorých to je aj explicitne uvedené) pochádzajú z 2. svetovej vojny.

Prvý diel knihy sa venuje základnej terminológii, vlastnostiam jazyka a potom úvodnému skúmaniu šifrovaných textov. Figl podrobne rozpisuje kryptoanalyticky využiteľné vlastnosti desiatich jazykov: nemčina, angličtina, francúžština, taliančina, španielčina, ruština, srbochorváčtina, čeština, poľština a maďarčina. Popisuje charakteristiky týchto jazykov, frekvencie znakov, bigramov, pri väčšine jazykov aj trigramov a pri niektorých jazykoch aj tetra- a pentagramov. Figl v texte uvádza že údaje pre nemčinu prevzal od Fleissnera, pre španielčinu od Gioppiho, pre francúžštinu od Kasiského a zvyšok sú jeho výsledky na vzorkách aspoň 1000 znakov. Znaky jazykov delí na časté, stredne časté a zriedkavé a určuje percentuálne pokrytie príslušného jazyka týmito skupinami. Uvedené jazyky rozdelil na skupiny: germánske, románske, slovanské a maďarčina. Potom ukazuje na niektorých znakov ako vyzerajú ich charakteristiky v jednotlivých skupinách jazykov a na príkladoch ukazuje ako sa dá v zašifrovanom texte odhadnúť použitý jazyk. Od 19. kapitoly (od str. 68) popisuje charakteristické vlastnosti niektorých šifier[8] a to ako sa tieto charakteristiky dajú využiť pri lúštení. Potom až do konca prvého dielu uvázdza príklady analýzy zachytených depeší. Čiže ukazuje ako treba skúmať zachytenú depešu, zistiť, alebo aspoň odhadnúť odosielateľa, príjemcu, čas a miesto odoslania, typ šifry a použitý jazyk.

Celý druhý diel je venovaný lúšteniu substitučných šifier. Popisujú sa tam

[8]Samozrejme v celom texte je reč o klasických ručných šifrách.

viaceré klasické substitúcie, počnúc jednoduchou zámenou až po komplikovanejšie šifry s periodickým heslom, ktoré Figl nazýva *„Tritheimove šifry“*, prípadne *„rozšírenie Tritheima“*. Zaujímavý je napr. príklad lúštenia homofónnej substitúcie uvedený od str. 161. Jedná sa o jednoduchšiu homofónnu šifru s dvoma abecedami.

Posledný tretí diel je venovaný transpozičným šifrám. Opäť sa začína príkladmi jednoduchších transpozícii ako sú úplné a neúplné tabuľkové transpozície a postupne sa ukazujú príklady aj zložitejších transpozícii ako sú dvojité transpozície, tabuľky rôzneho tvaru, Zubatka a pod. V tomto diely je nazreteľnejšie to, že vznikol až po 2. svetovej vojne, pretože sa tam 2. svetová vojna a lúštenie šifier v nej používaných viackrát explicitne spomína a aj viaceré príklady depeší veľmi pripomínajú napr. aj československé šifry.

Moje celkové hodnotenie Figlovej knihy je pozitívne. Je to veľmi dobre napísaná učebnica lúštenia klasických ručných šifier. Na rozdiel od Friedmanových a Kullbackových kníh síce neobsahuje žiadne nové a prevratné matematické metódy, ale rovnako na rozdiel od týchto kníh obsahuje množstvo konkrétnych príkladov. Podľa informácií od nemeckých kryptológov túto knihu údajne používala rakúska armáda ako učebnicu klasickej kryptoanalýzy až do 80. rokov minulého storočia.

Literatúra

[1] Friedrich L. Bauer: Entzifferte Geheimnisse
Springer, 2000

[2] Friedrich L. Bauer: Decrypted Secrets
Springer, 2007

[3] Andreas Figl: Systeme des Dechiffrierens, Bd. 1, Bd. 2, Bd. 3
1926 ???

[4] Janeček Jiří: `http://janeckovokrypto.blogspot.sk`
Kryptogaleria 17, máj 2017

[5] Kahn David: The Codebreakers
Scribner, 1996

[6] Krajčovič Jozef: Andreas Figl – Nestor rakúskej kryptológie
Crypto-World, 7-8/2012

[7] Wikipedia: `http://de.wikipedia.org/wiki/Andreas_Figl`

[8] `http://www.sichere.it/new/index.php?id=8&kap=17&searchstr=T%DCRKEL%20Dr.%20Siegfried`

S Y S T E M E d e s D E C H I F F R I E R E N S

von Andreas F I G L, Hofrat i.R. und Oberst a.D.,
dem Altmeister der österreichischen Enträtselungskunst und kryptographischen Wissenschaft.
(Unter Erg.oder Ergänzung sind Beiträge eines seiner Schüler)

B A N D 1

INHALTSVERZEICHNIS :

I. T E I L

Obr. 2: *Systeme des Deschiffrierens* – obsah 1. dielu

S Y S T E M E des D E C H I F F R I E R E N S

von Andreas F I G L, Obst.a.D.,Hofrati.R.

mit Ergänzungen "ERG."

B A N D II

Ersatz - Verfahren

Anmerkung:

Die Kap.31,32,33(Seite 99 - 114),
Kap.36,37 (Seite 141 - 154) aus dem II.Teil des Werkes von Oberst FIGL wurden herausgenommen und scheinen in unserem BAND III unter den VERSETZUNGSVEFAHREN als solche auf.

Obr. 3: *Systeme des Deschiffrierens* – obsah 2. dielu

S Y S T E M E DES D E C H I F F R I E R E N S

von Andreas F I G L, Obst.a.D.,Hofrat i.R.

mit Ergänzungen " ERG "

B a n d III

IV.Abschnitt

ENTRÄTSELUNG VON BUCHSTABENVERFAHREN

Obr. 4: *Systeme des Deschiffrierens* – obsah 3. dielu

C. Central European Conference on Cryptology 2013

Marek Kumpost, xkumpost@fi.muni.cz

Central European Conference on Cryptology 2013

1st Announcement

The Central European Conference on Cryptology will take place in the Masaryk University Centre Telč, Czech Republic from Wednesday, June 26 to Friday, June 28, 2013.

The aim of the conference is to bring together researchers in all aspects of cryptology, including but not limited to:

* cryptanalysis,
* cryptographic applications in information security,
* design of cryptographic systems,
* encryption schemes,
* general cryptographic protocols,
* post-quantum cryptography,
* pseudorandomness,
* signature schemes,
* steganography.

The detailed information is provided at http://www.fi.muni.cz/cecc/

Important dates:

April 15, 2013: Submission of abstracts
April 29, 2013: Notification of acceptance/rejection
May 1, 2013: Preliminary conference program
May 22, 2013: Registration deadline
June 26-28: The conference
July 22, 2013: Deadline for full papers invited for journal publication

Program committee

Chair: **Vašek Matyáš** - Masaryk University, Brno, Czech Republic

PC members:
Laszlo Csirmaz - Central European University, Hungary
Otokar Grošek - Slovak University of Technology in Bratislava, Slovakia
Petr Hanáček - Brno University of Technology, Czech Republic
Tamás Herendi - Faculty of Informatics, University of Debrecen, Hungary
Miroslav Kureš - Brno University of Technology, Czech Republic
Miroslaw Kutylowski - Wroclaw University of Technology, Poland
Karol Nemoga - Slovak Academy of Sciences, Slovakia
Martin Stanek - Comenius University, Slovakia
Petr Švenda - Masaryk University, Brno, Czech Republic
Natalia Tokareva - Sobolev Institute of Mathematics, Novosibirsk, Russia
Jiří Tůma - Faculty of Mathematics and Physics, Charles University in Prague, Czech Republic
Pavol Zajac - Slovak University of Technology in Bratislava, Slovakia

D. call for papers - CYBERSPACE 2013

http://www.cyberspace.muni.cz

call for papers
CYBERSPACE 2013
www.cyberspace.muni.cz

Brno, Czech Republic, 22-23 November 2013
organized by Institute of Law and Technology, Faculty of Law in cooperation with
School of Social Studies, Masaryk University and European Academy of ICT Law

Paper abstracts are solicited for a submission to following streams:

Ideas for cyberspace, *chairs:* Herbert Hrachovec, Radim Polčák, *publication of papers:* MUJLT, *disciplines:* multidisciplinary, *illustrative topics:* any theoretic/philosophic thoughts for the present and future of cyberspace

Legal Informatics, *chair:* Jaromír Šavelka, *publication of papers:* MUJLT, *disciplines:* legal informatics, jurimetrics, *illustrative topics:* legal information systems, electronic publication of laws, public registries, automated processing of legal language, case-law on-line

Videogames and Society, *chair:* Cyril Brom, *publication of papers:* MUJLT/Cyberpsychology, *disciplines:* multidisciplinary, *illustrative topics:* social aspects of video games, digital game-based learning, serious games, on-line gaming, videogames as a research tool

Legal aspects of free and open software, *chair:* Matěj Myška, *publication of papers:* MUJLT, *disciplines:* IP/IT law, *illustrative topics:* enforceability of F/OSS licences compatibility of F/OSS licences, F/OSS and software patents, new F/OSS licences, current F/OSS case law; F/OSS and international private law; F/OSS and consumer protection; F/OSS and limitations of liability/damages

Cybersecurity, Cybercrime, *chairs:* Václav Stupka, *publication of papers:* MUJLT, *disciplines:* multidisciplinary, *illustrative topics:* cyberwars, cyberattacks, cyberterrorism, the role of response teams, hacker communities, child pornography, piracy, identity theft, hacking/cracking, phishing, dissemination of malicious code, digital forensics and criminal procedure, jurisdictional issues in cybercrime, botnets, cyberbullying

New Media and Society, *chair:* Kristian Daneback, *publication of papers:* Cyberpsychology, *disciplines:* psychology, sociology, media studies, communication sciences, social work, *illustrative topics:* digital media and civic participation, online public spheres, new media in everyday lives, web 2.0, internet governance, digital divide, communities in cyberspace, hacktivism, free culture movement, anthropology of cyberspace, gender and internet, gaming, society and cyberspace, new media and social services

Privacy, Personal Data and Surveillance, *chair:* Aleš Završnik, *publication of papers:* MUJLT, *disciplines:* multidisciplinary, *illustrative topics:* Internet surveillance, DPI (Deep Packet Inspection), smart surveillance systems, counter-cybersurveillance (e.g. darknet, TOR), privacy online, social networking sites surveillance, ISPs and law enforcement snooping, marketing surveillance, regulating cybersurveillance (e.g. data retention), PET technologies, right to be forgotten

New Media and Politics, *chairs:* Vaclav Stetka, Marta Fialova, *publication of papers:* Cyberpsychology, *disciplines:* political science, media studies, sociology, communication studies, *illustrative topics:* online political communication, new media and election, campaigns, the role of social media in democracy and democratization, social networks and transformation of journalism, new media and political mobilization, internet and transparency of government, the impact of WikiLeaks

International Internet Law, *chair:* Dan Svantesson, *publication of papers:* MUJLT, *disciplines:* international private law, international public law, *illustrative topics:* Brussels I Regulation, Rome I, Rome II and the internet, cross-border on-line defamation, conflict of laws on the internet, place of damage, electronic choice of law and choice of forum, jurisdiction of on-line arbiters, international on-line arbitration, cross-border eCommerce

Intellectual Property On-Line, *chair:* Andreas Wiebe, *publication of papers:* MUJLT, *disciplines:* multidisciplinary, *illustrative topics:* copyright, digital rights management, open source, open access, fair use, fair dealing, protection of software, licensing, P2P networks, trademarks on-line, intellectual property in third world countries, trademarks in auction and search servers

Religion in Cyberspace, *chair:* Vít Šisler, *publication of papers:* MUJLT/Cyberpsychology, *disciplines:* multidisciplinary, illustrative topics: religious normative frameworks in cyberspace, networking diasporas, religious collaborative environments, on-line counseling, on-line fatwas and cyber muftis, new religious movements, religious discourses in cyberspace

eFinance, *chair:* Libor Kyncl, *publication of papers:* MUJLT, *disciplines:* financial law, commercial law, economy, *illustrative topics:* e-banking, e-insurance, e-pensions, online investments, eFX markets, electronic payments, electronic money and virtual money, payment cards and payment portals, retail & large value payment systems, micropayment systems, informal value transfer systems, online AML measures, e-taxation, taxation in virtual worlds

Psychology of Cyberspace, *chair:* David Šmahel, *publication of papers:* Cyberpsychology, *disciplines:* psychology, sociology, media studies, communication sciences, *illustrative topics:* influence of the Internet use on individuals and family, children and adolescents in virtual worlds, Internet addiction, identity in virtual environment, counseling on the Internet, on-line therapy, Internet and sexuality, human personality on-line, virtual social groups, virtual communities, blogs, games on-line, MMORPG and virtual worlds, online communication, e-learning, opportunities of Internet use, cyberbullying, online victimisation, intimacy and Internet, technology and health

Government 2.0 - Recent Developments and Future Trends, *chair:* Ludwig Gramlich, *publication of papers:* MUJLT, *disciplines:* multidisciplinary, *illustrative topics:* electronic signatures, electronic filing, on-line dispute settlement, re-use of public sector information, on-line public procurement, legal information systems, electronic public registries, on-line access to law and case-law, data mining systems for lawyers, electronic storage of documents, on-line legal counselling, geographic information systems, identity issues, digital inclusion, government 2.0, mobile government, e-participation, improving e-democracy

eCommerce Law, *chair:* Zsolt Balogh, *publication of papers:* MUJLT, *disciplines:* business law, financial law, *illustrative topics:* information society services, EDI and EFT regulation and practice, UNCITRAL model laws on eCommerce, on-line gambling, taxation of e-commerce

Important dates

Abstract submission deadline:	31 July 2013
Notice on acceptance deadline:	31 August 2013
Conference dates:	22 – 23 November 2013
Papers for publication deadline:	11 January 2013

Abstract formal requirements

Range: max. 1.500 characters incl. spaces
Submission: on-line at www.cyberspace.muni.cz

Paper formal requirements and submission

Papers published in MUJLT: http://mujlt.law.muni.cz/instructions.php
Papers published in Cyberpsychology: http://www.cyberpsychology.eu/submission.php

Conference fees

full pass - speakers: 990 CZK (approx. 39 EUR)
full pass - delegates (not presenting a paper): 1290 CZK (approx. 52 EUR)
full pass - VIPs (upon an appointment): FREE
student pass - students of MU and of partner universities: FREE
last minute (on-site) registration: 1990 CZK (approx. 80 EUR)
dinner fee: Saturday conference dinner with free complimentary drinks - 550 CZK (approx. 22 EUR), last minute (on-site): 650 CZK (approx. 26 EUR)

Notes: The registration will be carried out on-line through the conference web at www.cyberspace.muni.cz. The registration system will provide for the conference registration, for the payment of the registration fee (by credit/debit card or bank transfer) incl. automated invoicing and for optional booking of accommodation in selected hotels at conference rates (from approx. 40 EUR/night). The registration opens 1 June 2013 and closes 5 November 2013.

Conference addresses

Conference website: http://cyberspace.muni.cz
Central conference e-mail address: cyberspace@law.muni.cz
Mailing address: Masaryk University, Faculty of Law
Institute of Law and Technology
Veveří 70
611 80 Brno
Czech Republic

Conference officials

General Chair	Radim Polčák
Deputy Chairs	Danuše Spáčilová, David Šmahel
Scientific Committee	Zsolt Balogh, Cyril Brom, Kristian Daneback, Marta Fialová, Ludwig Gramlich, Herbert Hrachovec, Libor Kyncl, Matěj Myška, Radim Polčák, Dan Svantesson, Jaromír Šavelka, Václav Stupka, Václav Štětka, Vít Šisler, David Šmahel, Andreas Wiebe, Aleš Završnik
Financial Officer	Libor Kyncl
Hospitality Officer	Matěj Myška
Publication Officer	Jaromír Šavelka
Programme Officer	Klára Vrbková

E. 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 3-4/2012

Crypto-World 5-6/2012

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

F. Závěrečné informace

1. Sešit

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

2. Registrace / zrušení registrace

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

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška Jozef Krajčovič Jozef Martin Kollar Vlastimil Klíma
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Jaroslav Pinkava
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jozef Martin Kollar	jmkollar@math.sk ,	
Jozef Krajčovič	kryptosvet@gmail.com ,	
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://webdesign.crypto-world.info