Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 15, číslo 1-2/2013 **24. únor**

1-2/2013

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1322 registrovaných odběratelů)

Obsah :

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

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

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

Jakub MÍRKA, SOA Plzeň, mirka@soaplzen.cz

Obrazové přílohy, které jsou umístěny přímo v textu, lze nalézt v lepší kvalitě v příloze Crypto-Worldu (Obrazová příloha k části II. http://crypto-world.info/casop14/cast2.zip). Ve všech případech jde o kopie archiválií uložených ve Státním oblastním archivu v Plzni.

Dalším fondem s významným obsahem šifrované korespondence je Rodinný archiv Windischgrätzů. Ve fondu se kromě šifrovaných dopisů nachází také sbírka šifrovacích klíčů, která byla vytvořena již při pořádání archivu koncem 18. století.[1] V této sbírce je uloženo několik desítek klíčů – od těch nejjednodušších až po složité nomenklátory blížící se svou podobou kódové knize. Korespondence i klíče pocházejí ze druhé poloviny 17. a z první poloviny 18. století. Jen několik z nich je datovaných a u většiny ani není uvedeno, pro které osoby byly určeny. Mnohé z klíčů lze ale datovat alespoň přibližně podle jejich provedení nebo podle jmen významných osob, která často bývají v těchto klíčích kódována. V několika případech bylo možné klíče použít pro dešifrování dochovaných dopisů, ale k naprosté většině klíčů se mi odpovídající korespondenci nalézt nepodařilo.[2] (viz obr.7)

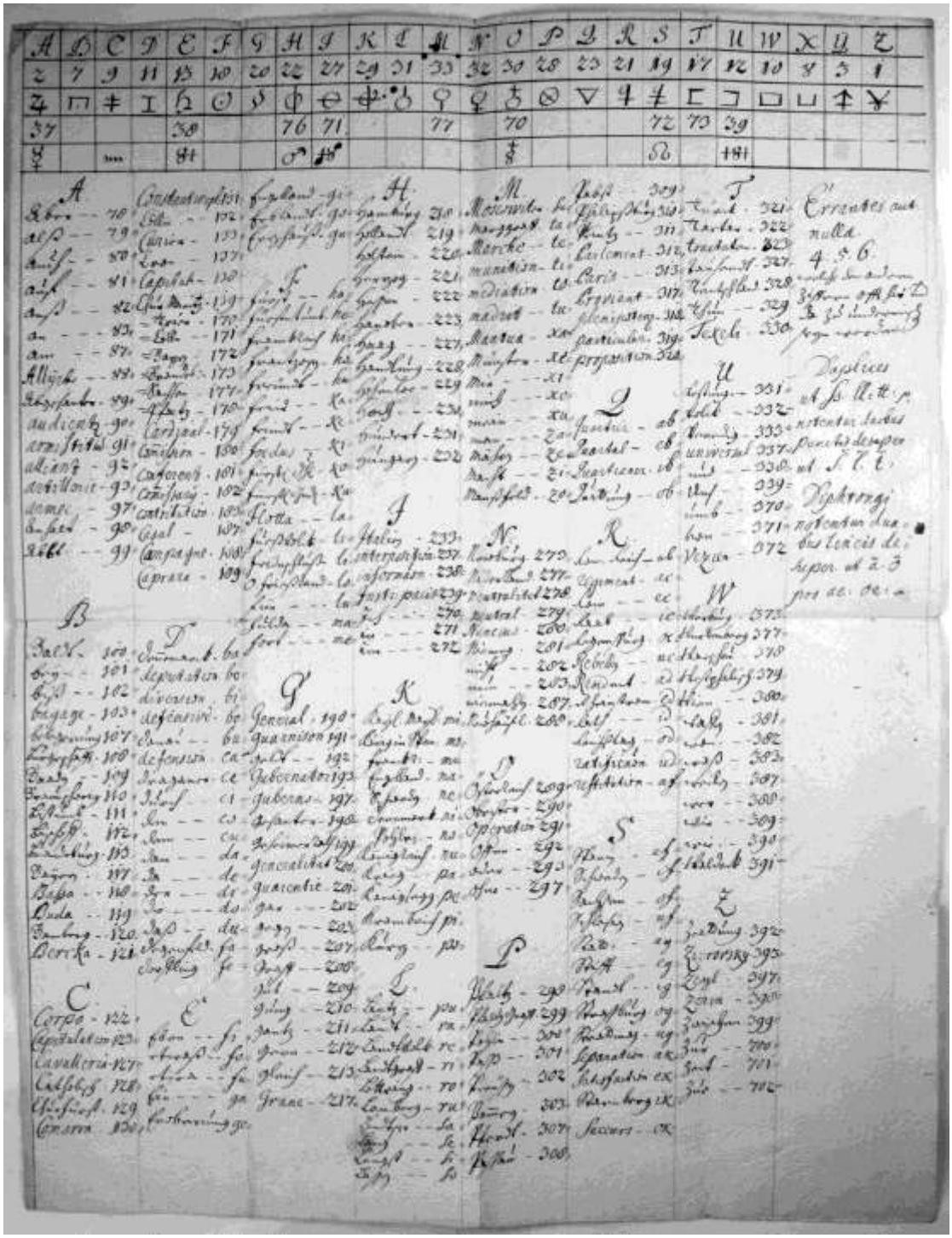
Zatímco ve fondu Rodinný archiv Trauttmansdorffů se šifrovaná korespondence nachází patrně jen v pozůstalosti Maxmiliána z Trauttmansdorffu, v Rodinném archivu Windischgrätzů pochází z činnosti několika členů rodu, působících v císařských diplomatických službách. Nejstarším z nich byl Gottlieb z Windischgrätzu (1630–1695), jeden z nejvýznamnějších diplomatů své doby, který v průběhu své kariéry působil jako vyslanec na mnohých evropských dvorech a jako vyjednavač se účastnil důležitých jednání evropských mocností a kongresů. K nejvýznamnějším patřila jeho mise u dvora francouzského krále v Paříži roku 1670 nebo jednání na kongresu v Haagu v letech 1690–1693. Od roku 1694 až do své smrti 25. prosince 1695 také zastával funkci říšského vicekancléře. Jako první z rodu Windischgrätzů se také usadil v Čechách. Český inkolát získal roku 1685.[3]

---

[1] K dějinám pořádání fondu HOFMANN, Gustav. *Rodinný archiv Windischgrätzů a jeho vývoj*. Sborník archivních prací 27, 1977, s. 110–142.

[2] SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 164, i. č. 1403, sign. 103. Jeden z mnoha klíčů uložených ve sbírce je možno spatřit na obr. č. 7. Na jiném místě fondu se také dochoval jeden osamělý klíč pro korespondenci s Vitalianem Borromeem ze druhé poloviny 17. století. Tamtéž, karton č. 219, i. č. 1445, sign. 145.

[3] Více k jeho osobě viz HOFMANN, Gustav. *Rodinný archiv Windischgrätz 1226–1945, I. Úvod (inventář)*. Klatovy : Státní oblastní archiv v Plzni 1975, s. XV–XVIII; ZWIEDINECK–SÜDENHORST, Hans von. Windisch–Graetz, Freiherr und Reichsgraf Gottlieb Amadeus. In: *Allgemeine Deutsche Biographie. Band 43*. Leipzig : Duncker & Humblot 1898, s. 416. K diplomatické činnosti Gottlieba Amadea z Windischgrätzu viz např. JÍRŮ, Roman. Der Reichstag in Regensburg und Gottlieb von Windischgrätz im Spiegel der Dokumente aus den Jahren 1683 bis 1688. *Verhandlungen des historischen Vereins für Oberpfalz und Regensburg* 131, 1991, s. 325–327.



Obrázek 7 – nomenklátor ke generální šifře pro korespondenci císařských ministrů, [cca 1680–1690]. Obsahuje klíč pro homofonní substituci, kódy, důmyslné klamače a šifrové znaky pro dvojhlásky.

Zatímco ve fondu Rodinný archiv Trauttmansdorffů se šifrovaná korespondence nachází patrně jen v pozůstalosti Maxmiliána z Trauttmansdorffu, v Rodinném archivu Windischgrätzů pochází z činnosti několika členů rodu, působících v císařských diplomatických službách. Nejstarším z nich byl Gottlieb z Windischgrätzu (1630–1695), jeden z nejvýznamnějších diplomatů své doby, který v průběhu své kariéry působil jako

vyslanec na mnohých evropských dvorech a jako vyjednavač se účastnil důležitých jednání evropských mocností a kongresů. K nejvýznamnějším patřila jeho mise u dvora francouzského krále v Paříži roku 1670 nebo jednání na kongresu v Haagu v letech 1690–1693. Od roku 1694 až do své smrti 25. prosince 1695 také zastával funkci říšského vicekancléře. Jako první z rodu Windischgrätzů se také usadil v Čechách. Český inkolát získal roku 1685.[4]

Ve fondu se mimo jiné dochoval soubor konceptů Gottliebových pravidelných diplomatických relací dvorské kanceláři z let 1673–1675. Relací je celkem 84 a Gottlieb z Windischgrätzu v nich dvorské komoře podával velmi podrobné zprávy o činnosti svého poselstva v Říši. Nejdelší dobu pobýval v Braunschweigu, odkud pochází 41 relací. Další zprávy podával např. z Norimberka, Lipska, Hamburku, Lüneburgu a jiných německých měst. V říjnu až prosinci roku 1673 zavítal do Kodaně, odkud zaslal osm relací. Mezi nimi se nachází jediné tři šifrované relace ze všech 84. V nich především komentuje vnitřní záležitosti Dánska a podává informace o politické situaci a významných osobách na královském dvoře a jejich kontaktech. Nejčastěji je zmiňováno jméno tehdejšího dánského nejvyššího státního sekretáře Pedera hraběte Griffenfelda. Dalšími zmiňovanými představiteli dánského státního aparátu jsou např. tajný sekretář Konrad Biermann, který měl údajně být Griffenfeldovou pravou rukou, nebo dánští místodržící v Norsku a v Holštýnsku. Velmi často také zmiňuje francouzského vyslance na dánském dvoře Huguese rytíře de Terlon.[5]

Další šifrovanou korespondenci Gottlieba z Windischgrätzu jsem nenalezl, ale ve fondu se dochovalo značné množství korespondence jiných významných diplomatů té doby. Jde o několik desítek originálních dopisů odeslaných jedním z nejvlivnějších mužů na vídeňském dvoře Františkem Oldřichem hrabětem Kinským neuvedenému adresátovi.[6] Pocházejí z let 1694–1699.[7] Z jejich obsahu a z přiložených opisů dalších souvisejících listů jiných odesilatelů se dá s největší pravděpodobností usuzovat, že adresátem byl další významný císařský diplomat Dominik Ondřej hrabě Kounic.[8] Dopisy vesměs reagovaly na jeho pravidelné relace z významných diplomatických jednání, jichž se účastnil. Ve sbírce šifrovacích klíčů v tomto fondu se nachází nomenklátor, podle nějž byla šifra k těmto dopisům sestavena a který je označen slovy *Ziffra particularis cu[m] S[acra] Caes[are]a M[aiesta]te*.[9] To znamená, že šlo o nomenklátor, který používal i sám císař. Jednotlivé dopisy

---

[4] Více k jeho osobě viz HOFMANN, Gustav. *Rodinný archiv Windischgrätz 1226–1945, I. Úvod (inventář)*. Klatovy : Státní oblastní archiv v Plzni 1975, s. XV–XVIII; ZWIEDINECK–SÜDENHORST, Hans von. Windisch–Graetz, Freiherr und Reichsgraf Gottlieb Amadeus. In: *Allgemeine Deutsche Biographie. Band 43*. Leipzig : Duncker & Humblot 1898, s. 416. K diplomatické činnosti Gottlieba Amadea z Windischgrätzu viz např. JÍRŮ, Roman. Der Reichstag in Regensburg und Gottlieb von Windischgrätz im Spiegel der Dokumente aus den Jahren 1683 bis 1688. *Verhandlungen des historischen Vereins für Oberpfalz und Regensburg* 131, 1991, s. 325–327.

[5] SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 192–193, i. č. 1423, sign. 123.

[6] Ačkoli dopisy zaujímají téměř celý jeden karton (rozdělený do dvou), nepodařilo se mi mezi nimi nalézt jedinou obálku s uvedením adresáta.

[7] Šifrované jsou především dopisy z let 1697 a 1698.

[8] K jeho osobě a kariéře více viz FELGEL, Anton. V. Kaunitz, Dominik Andreas Freiherr, seit 1682 Graf. In: *Neue Deutsche Biographie. Band 11*. Berlin : Duncker & Humblot 1977, s. 363.

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

jsou ve francouzštině, ale šifrované pasáže jsou psány německy, protože nomenklátor je koncipovaný pro německý text. Nejčastěji je v šifrovém textu řešena otázka španělského dědictví. Z dopisů je patrné, že již před smrtí Karla II. probíhaly intenzivní diplomatické přípravy na získání španělského trůnu pro rakouské Habsburky. Především šlo o zajištění trvalejšího míru s Turky, přičemž panovaly obavy, že by tato jednání mohly zmařit Polsko a Moskva. Dále se mluvilo o tom, že by bylo vhodné uzavřít spojenectví s Benátkami a že Anglie a Holandsko jsou spíše na straně Francie. Důležitým tématem také bylo, kdo na svou stranu získá Bavorsko. Předmětem této korespondence ale byly i jiné otázky, např. jednání o svatbě římského krále, budoucího císaře Josefa I.[10]

Šifrovaná korespondence se zachovala i v písemné pozůstalosti dvou Gottliebových synů – Ernsta Fridricha (1670–1727) a Leopolda Viktorína (1686–1746). Oba byli také významnými diplomaty a zastávali vysoké dvorské úřady. Ernst Fridrich se roku 1714 stal prezidentem říšské dvorské rady a roku 1724 státním a konferenčním ministrem. Mladší Leopold Viktorín, jímž pokračoval rod Windischgrätzů, byl mimo jiné členem říšské tajné rady a roku 1630 získal velký palatinát. Stejně jako jejich otec nebo výše uvedený Maxmilián z Trauttmansdorffu byli oba bratři také držiteli Řádu zlatého rouna, jedné z nejvyšších poct, jaké mohli šlechtici v habsburských zemích dosáhnout.[11]

Ernstovi Fridrichovi adresoval roku 1711 několik šifrovaných dopisů císařský londýnský vyslanec Jan Václav hrabě z Gallasu. Jejich hlavním tématem je volba nového císaře, jíž se Ernst Fridrich účastnil jako člen českého poselstva. Gallas mu oznamuje, že na volbu císaře se vydává i lord Petersborough a také jej zpravuje o situaci v Anglii a o evropské politice.[12] K dopisům je přiložen také Gallasův dopis adresovaný Evženovi Savojskému, který se měl podle něj nacházet někde u své armády na Rýně. Dopis měl být údajně velice důležitý a měl mu být předán na nějakém bezpečném místě, nejlépe mezi čtyřmi stěnami. Přestože se zdá, že dopis ke svému adresátovi nedoputoval, je otevřený. Není ovšem dešifrován a nelze na něj aplikovat stejný klíč jako u dopisů adresovaných Windischgrätzovi.[13]

Také v písemné pozůstalosti Leopolda Viktorína z Windischgrätzu, mladšího bratra Ernsta Fridricha, se nachází šifrovaná korespondence. Nejzajímavější je asi soubor dvanácti nepříliš dlouhých dopisů od císaře Karla VI. (viz *obr. 8*). Tři z nich zaslal císař roku 1720 Leopoldu Viktorínovi do Haagu, kde působil jako vyslanec, a zbývajících devět roku 1722 na kongres do Cambray. Dopisy se ve fondu dochovaly v opisu v kopiáři *Codex diplomaticus Windischgrätzianus*,[14] a většina z nich také v originále.[15] Dopisy zaslané do Haagu jsou

[10] Tamtéž, karton 148–149, i. č. 1395, sign. 95.

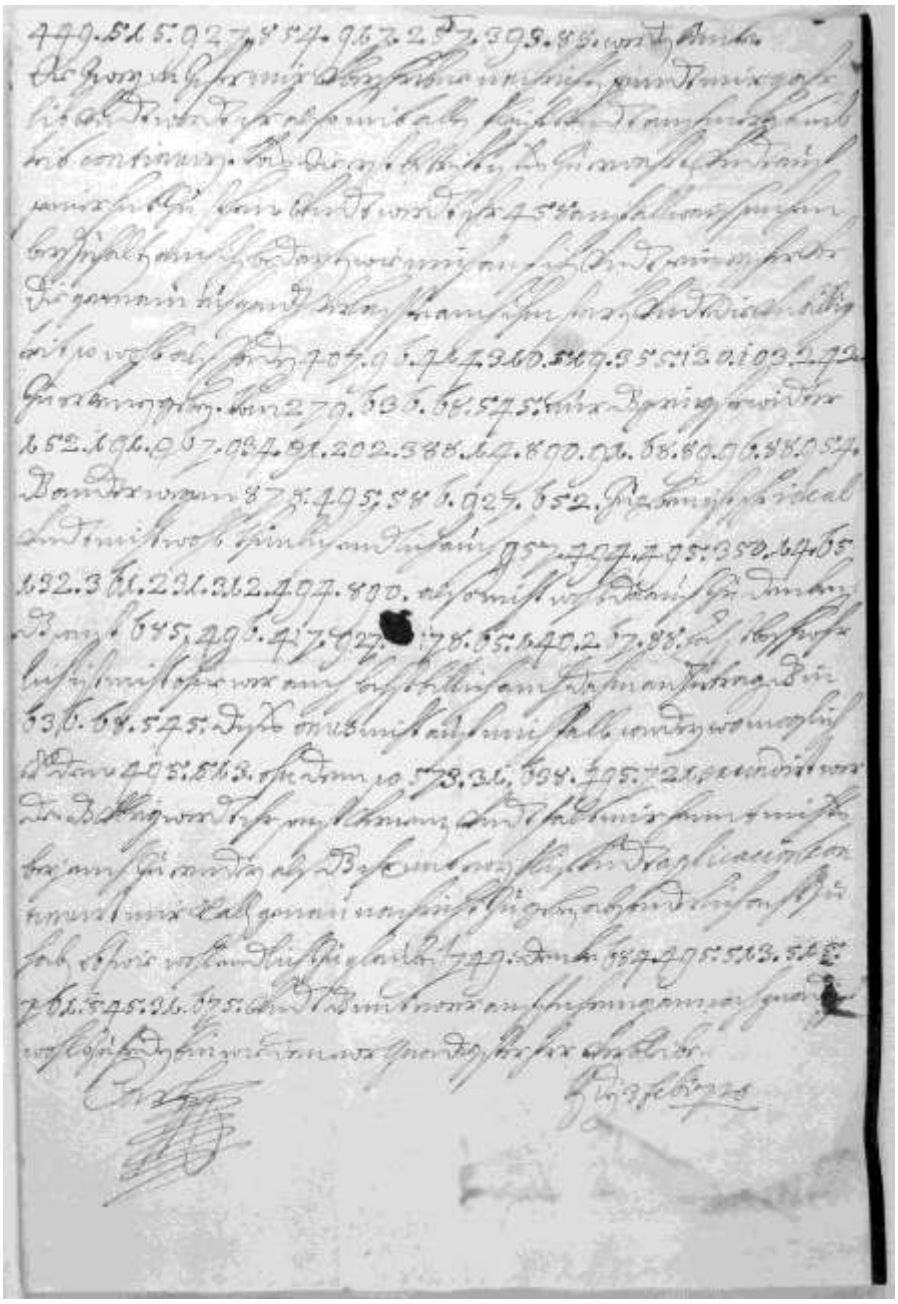
[11] Více k Ernstu Fridrichovi a Leopoldu Viktorínovi z Windischgrätzu viz HOFMANN, Gustav. *Rodinný archiv Windischgrätz 1226–1945, I. Úvod (inventář)*. Klatovy : Státní oblastní archiv v Plzni 1975, s. XVIII–XX; ZWIEDINECK–SÜDENHORST, Hans von. Windisch–Graetz, Reichsgraf Ernst Friedrich. In: *Allgemeine Deutsche Biographie. Band 43*. Leipzig : Duncker & Humblot 1898, s. 415; Týž. Windisch–Graetz, Reichsgraf Leopold Viktorin. *Tamtéž*, s. 415–416.

[12] Více k užívání šifrované korespondence hrabětem Gallasem VLNAS, Vít. Princ Evžen Savojský. Praha, Litomyšl : Paseka, Národní galerie v Praze 2001, s. 419.

[13] SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 211, i. č. 1437, sign. 137.

[14] Jde o šestidílný kopiář z konce 18. století, v němž jsou opisy nejdůležitějších dokumentů rodu z let 1091–1793. Opisy uvedených dopisů se nacházejí v pátém svazku. Tamtéž, kniha č. 5, i. č. 5, s. 402–416.

všechny šifrované, ale otevřený text má převahu. Mezi dopisy zaslanými do Cambray je šifrovaný jen jeden. Císař dával Windischgrätzovi především instrukce ohledně jeho diplomatických jednání a také ve věci psaní zpráv. Zajímavé je např. poučení o tom, pro jaký typ zpráv má užívat šifrování a také pokyny k výměně šifrovacího klíče, ke které došlo hned po odeslání prvního dopisu. O tom se ale ještě zmíním níže. Text sice není dešifrován, ale ve sbírce šifrovacích klíčů se nacházejí nomenklátory pro oba užívané způsoby šifrování.[16]



Obrázek 8 – dopis císaře Karla VI. Leopoldu Viktorínovi z Windischgrätzu ze 3. února 1720 z Vídně (poslední strana s vlastnoručním podpisem císaře). Dopis není dešifrován, ale lze jej přečíst s pomocí jednoho z nomenklátorů uloženého ve sbírce klíčů.

[15] Tamtéž, karton č. 5, i. č. 694, sign. 669A/III. b.

V roce 1721 si Leopold Viktorín z Windischgrätzu vyměnil několik šifrovaných dopisů s anglickým obchodníkem Johnem Colebrookem,[17] který v té době pobýval ve Vídni a snažil se přesvědčit císaře a jeho blízké okolí k založení obchodní společnosti po vzoru britské, holandské nebo francouzské východoindické společnosti. Roku 1722 Karel VI. skutečně založil Ostendskou obchodní společnost, která byla již roku 1727 na nátlak Anglie a Nizozemí zrušena.[18] Korespondence Leopolda Viktorína Windischgrätze s Johnem Colebrookem je tedy zajímavým pramenem ke krátkým dějinám tohoto podniku. Zároveň se jedná o jediný případ ve fondech 5. oddělení SOA v Plzni, kdy lze doložit, že šifrování užíval obchodník. Ovšem vzhledem k tomu, že Colebrooke byl obchodníkem, anebo spíše spekulantem až hochštaplerem velkého formátu, není tato skutečnost natolik překvapivá, zvláště když je známo, že prvotní iniciátor celého podniku a Colebrookův společník John Ker of Kersland dříve pracoval jako anglický špion mezi skotskými jakobity.[19]

Ernst Fridrich a Leopold Viktorín někdy používali šifrování i ve své vzájemné soukromé korespondenci. Dochovalo se několik šifrovaných dopisů z podzimu 1721.[20] Při jejich šifrování užívali jednoduché substituce a kódů. Část dopisů byla dešifrována, a tak nebyl problém sestavit klíč k jednoduché substituci. Vzhledem k malému rozsahu šifrovaného textu se naopak podařilo získat pouze několik kódů. Šifrovány byly totiž jen kratičké pasáže. Ernst Fridrich se v té době zdržoval v Rakousku – ve Vídni a na panství St. Peter in der Au, zatímco Leopold Viktorín psal z Bruselu. Jejich zprávy se týkaly jak majetkových, tak politických záležitostí. Ernst Fridrich také bratra informoval o dění u dvora.

Několik šifrovaných dopisů se nachází také v Rodinném archivu Verdugů, Doupov v pozůstalosti Viléma Verduga,[21] velitele španělské tercie a místodržitele Španělskem obsazené Dolní Falce. Ve fondu jsou uloženy dva šifrované dopisy z roku 1627 z Madridu pravděpodobně od Jeana de Croy, hraběte de Solre (viz *obr. 10*).[22] Jsou psány španělsky a k jednomu z nich je přiložen dešifrovaný text. Opět tedy nebyl větší problém sestavit klíč. Jde o trochu složitější nomenklátor, který obsahuje homofonní substituci, bigramy i kódy.

---

[16] Tamtéž.

[17] Tamtéž, karton č. 208, i. č. 1435, sign. 135.

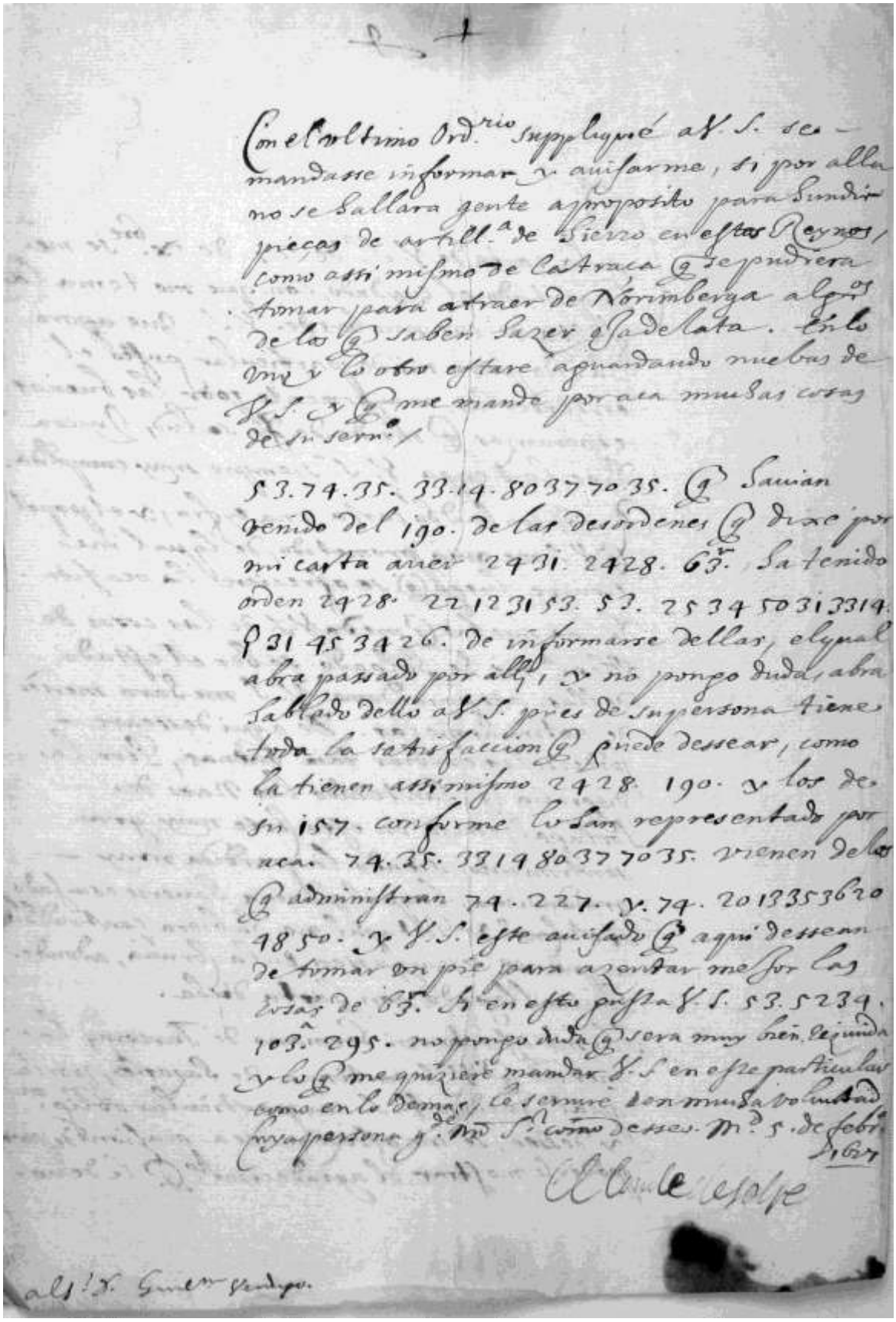
[18] K ustanovení Ostendské obchodní společnosti viz WANNER, Michal. The Establishment of the General Company in Ostend in the Context of the Habsburg Maritime Plans 1714–1723. In: SKŘIVAN, Aleš – SUPPAN, Arnold (edd.). *Prague Papers on the History of International Relations*. Prague : Institute of World History 2007, s. 33–62.

[19] K účasti Colebrooka na ustanovení společnosti viz Tamtéž, s. 52–53. Ker of Kersland ve svých pamětech vzpomíná, že císař Colebrooka krátce po jeho příjezdu do Bruselu poručil dát zadržet. Tomu se prý však podařilo uprchnout. KER OF KERSLAND, John. *The Memoirs of John Ker of Kersland in North Britain Esq.* London 1726, s. 180.

[20] SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 202, i. č. 1433, sign. 133.

[21] K jeho osobě více viz HAUBERT, Jan. *Rodinný archiv Verdugo – Doupov (inventář).* Plzeň : Státní oblastní archiv v Plzni, s. 2–3.

[22] Dopis je podepsán pouze El Conde de Solre a je zařazen mezi neurčenou korespondencí. SOA v Plzni, pracoviště Klášter, RA Verdugů, karton č. 2, i. č. 29.



Obrázek 9 – dopis Jeana de Croy, hraběte de Solre Vilémovi Verdugovi z 5. února 1627 z Madridu (druhá strana).

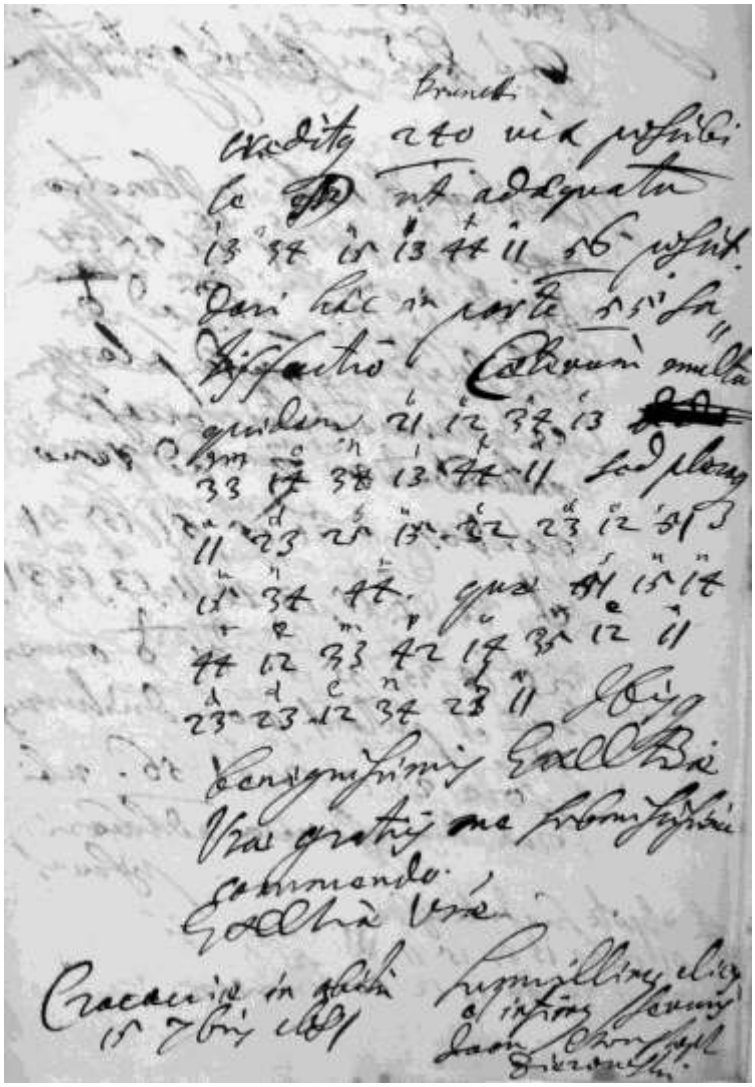
Ve stejném fondu se nacházejí francouzsky psané dopisy Kristiána knížete z Anhaltu, adresované také Vilémovi Verdugovi. Dva z nich jsou šifrované a pocházejí z let 1626–1627 (1. 2. 1626 a 26. 2. 1627).[23] Jejich text není dešifrován a klíč se nedochoval. K dopisům jsou přiloženy dva nomenklátory, ale ty nelze na danou šifru aplikovat.[24] Vzhledem k tomu, že text je velmi krátký, není možné jej vyluštit. Bylo by to ale zřejmě velice obtížné, i kdyby se dochoval delší text, protože vzhledem k počtu znaků šifrové abecedy je klíčem pravděpodobně opět složitější nomenklátor.

Posledními fondy, ve kterých se mi podařilo dohledat šifrovanou korespondenci, jsou rodinné archivy obou českých větví říšského hraběcího rodu Nostitzů, původně pocházejícího z Lužice. Ve fondu Rodinný archiv Nostitz-Rienecků, Sokolov je uložena korespondence jednoho z nejvýznamnějších členů rodu, Jana Hartvíka z Nostitz (1610–1683), který byl v letech 1652–1683 nejvyšším kancléřem Českého království.[25] V jeho písemné pozůstalosti je mimo jiné uložen složitější nomenklátor pro korespondenci s císařskými ministry, obsahující šifrové znaky pro jednotlivá písmena abecedy (homofonní), dvojhlásky a klamače a také přibližně 300 kódů.[26] Stejný nomenklátor[27] je také ve sbírce šifrovacích klíčů v Rodinném archivu Windischgrätzů.[28] I v tomto fondu je uvedeno, že klíč je určen pro korespondenci s císařskými ministry. Navíc se zde nachází ve třech různých vyhotoveních. První dvě jsou psána jedním písařem. Jedno sloužilo pro psaní šifrového textu a druhé pro jeho dešifrování.[29] Třetí vyhotovení je psáno jiným písařem a díky němu je možné přibližně určit dobu jeho užívání. Na zadní straně je totiž napsáno, že bylo vytvořeno na pokyn (říšského) vicekancléře z 27. dubna 1687 a podle klíče z roku 1683. Pokud je datum vzniku nomenklátoru uvedeno správně, znamená to, že Jan Hartvík z Nostitz klíč obdržel patrně krátce před svou smrtí 24. března 1683. Ve fondu jsem také nenalezl žádnou korespondenci psanou pomocí této šifry.

Kromě klíče se v písemné pozůstalosti Jana Hartvíka z Nostitz nacházejí šifrované dopisy tří různých odesilatelů, psané pomocí velice jednoduché a ve všech případech stejné šifry. Nejstarší dopisy jsou od Kryštofa Leopolda svobodného pána von Schaffgotsch z roku 1663.[30] Schaffgotsch užil stejného klíče také v korespondenci z roku 1673.[31] V té době už byl slezským nejvyšším zemským hejtmanem. Vzhledem ke svému původu a úřadu nejvyššího kancléře Českého království se Jan Hartvík také aktivně zajímal o politické dění v Polsku. Z let 1669–1671 pochází italsky psané dopisy od císařova vyslance na polském dvoře Augustina svobodného pána von Mayerberg,[32] a konečně z roku 1681 latinsky psané dopisy od dalšího

[23] Tamtéž, karton č. 2, i. č. 13.
[24] Jeden z těchto klíčů je na zadní straně označen *Cor[r]espondance du Ch[e]v[a]l[ie]r de M.*
[25] Více k Janu Hartvíkovi z Nostitz HAUBERTOVÁ, Květoslava. *Rodinný archiv falknovské větve Nostitz–Rienecků (1240) 1364–1945 (inventář)*. Žlutice : Státní oblastní archiv v Plzni 1973, s. 3–5; LUFT, Robert. Nostitz, Johann Hartwig Freiherr. In: Neue Deutsche Biographie. Band 19. Berlin : Duncker & Humblot 1999, s. 354–355.
[26] SOA v Plzni, pracoviště Klášter, RA Nostitz–Rienecků, Sokolov, karton č. 18, i. č. 91, H3.
[27] Je totožný svým obsahem, ale písař se liší.
[28] SOA v Plzni, pracoviště Klášter, RA Windischgrätzů, karton č. 164, i. č. 1403, sign. 103.
[29] O rozdílu mezi klíči pro psaní šifrového textu a pro dešifrování se podrobněji zmíním níže.
[30] SOA v Plzni, pracoviště Klášter, RA Nostitz–Rienecků, Sokolov, karton č. 13, i. č. 77, sign. FF 8.
[31] Tamtéž, karton č. 14, i. č. 78, sign. FF 9.
[32] Tamtéž, karton č. 13, i. č. 77, sign. FF 8.

císařského vyslance tamtéž Jana Krzysztofa svobodného pána Zierowského (viz *obr. 10*).[33] Jak vyplývá z výše uvedených informací, Jan Hartvík z Nostitz užíval stejného šifrovacího klíče při korespondenci s různými osobami po dobu nejméně 18 let. Pravděpodobně tedy šlo o jeho osobní klíč. Nostitz pro korespondenci používal jednoduché záměny písmen abecedy, která nahrazoval dvoucifernými číslicemi.



Obrázek 10 – dopis Jana Krzysztofa Zierowského Janu Hartvíkovi z Nostitz z 15. září 1681 z Krakova (poslední strana). Text dešifrován mezi řádky.

Nepatrné stopy šifrované korespondence lze najít také ve fondu Rodinný archiv Nostitzů, Planá v písemné pozůstalosti Kryštofa Václava hraběte z Nostitz. Kryštof Václav byl během svého života mimo jiné hejtmanem několika slezských knížectví a pro svůj rod získal říšský hraběcí titul. Vedl také významné diplomatické mise – roku 1686 do Braniborska a roku 1693 do Polska a Litvy. Nejvíce však proslul jako mecenáš a sběratel umění a knih.[34] Mezi přijatou

[33] Tamtéž.

[34] Více k osobě Kryštofa Václava z Nostitz viz KUBEŠ, Jiří – MAREŠOVÁ, Marie – PANOCH, Pavel. Rodová paměť a „sebe-představení“ v podání Kryštofa Václava z Nostic (1648–1712): Příspěvek k reprezentačním strategiím barokní slezské šlechty. In: DÁŇOVÁ, Helena – KLÍPA, Jan – STOLÁROVÁ,

korespondencí se nacházejí šifrované dopisy od viceprezidenta slezské komory Karla Ignáce svobodného pána Zehentner von Zehentgrub z roku 1686 z Vratislavi.[35] Jsou psány jednoduchou šifrou, fungující na stejném principu jako šifra Jana Hartvíka z Nostitz. Klíč byl ovšem odlišný.

Mezi korespondencí Kryštofa Václava z Nostitz s jeho agenty jsou uloženy tři klíče, jejichž obsahem jsou výhradně kódy pro jména důležitých osob a pro názvy institucí a geografické názvy. Kódy byly tvořeny buď pomocí čísel, nebo kryptonym. Zajímavější je druhý případ, kdy byla jednotlivá jména nahrazována jmény jinými, pocházejícími zejména z řecké a římské mytologie, filosofie a historie. V mnoha případech jsou dokonce nahrazována tak, že v daném kontextu dopisu, a někdy dokonce i mimo něj, by nemuselo být obtížné si domyslet správné jméno. Tak např. kód pro císaře zněl *Jupiter* a pro císařovnu *Pallas*. Z dalších kódů uvedu pro zajímavost jen několik dalších. Nejvyšší kancléř Českého království byl označován *Dictator*; zemští hejtmané některých slezských knížectví např. *Plato, Scipio, Moyses* nebo *Frater turbans*; stavy těchto knížectví např. *Trojani, Carthaginenses, Seductores* nebo *Neutrales*; válečná rada *Campus Martis*; jezuité die *Tempelherren*; Horní Slezsko *Schottland*, Dolní Slezsko *Engelland* a České království *Irrland* aj. (viz *obr. 11*).[36] Kryptonyma byla běžně užívána i v osobní korespondenci šlechticů. Většinou šlo ale o spontánně vytvořené přezdívky, které vyplývaly z vlastností jejich nositele nebo z jiných okolností souvisejících s jeho osobou a které byly dobře známé oběma pisatelům a často nejen jim, ale i širšímu okruhu osob.[37] Z toho důvodu nebylo nutné pro taková kryptonyma vytvářet klíče a i přes některé shodné znaky nelze mluvit o stejném způsobu utajování jmen jako v případě kódů z písemné pozůstalosti Kryštofa Václava z Nostitz. (viz Obr. 11)

Z obsahu jednotlivých klíčů v písemné pozůstalosti Kryštofa Václava z Nostitz je patrné, že jeden byl užíván především pro korespondenci týkající Slezska, druhý asi především pro záležitosti Českého království a třetí pravděpodobně pro záležitosti Svaté říše římské. Nezdá se ale, že by mezi nimi byla nějaká bližší souvislost. Jsou psány odlišnými písaři a také pravděpodobně pocházejí z různých let. Přesto všechny zapadají do zhruba stejného časového rámce na přelomu 17. a 18. století, čemuž napovídají jména osob v nich uvedených.[38]

V jiných fondech SOA v Plzni jsem dosud na šifry nenarazil.[39] I přesto je množství dochované šifrované korespondence dostatečné k vytvoření si alespoň základní představy o

---

Lenka (edd.). *Slezsko – země Koruny české. Historie a kultura 1300–1740.* Praha : Národní galerie 2008, s. 347–374; KUBEŠ, Jiří (ed.). *Kryštof Václav z Nostic, Deník z cesty do Nizozemí roku 1705*. Praha : Scriptorium 2004.

[35] SOA v Plzni, pracoviště Klášter, RA Nostitzů, Planá, karton č. 82, i. č. 296.

[36] Tamtéž, karton č. 84, i. č. 306.

[37] K užívání kryptonym viz např. MAŤA, Petr. Zdeněk Vojtěch z Lobkovic, Polyxena z Pernštejna a jejich korespondence. Poznámky k edici Pavla Marka. *Folia Historica Bohemica* 23, 2008, s. 155–160.

[38] SOA v Plzni, pracoviště Klášter, RA Nostitzů, Planá, karton č. 84, i. č. 306.

[39] Po odevzdání článku k redakční úpravě jsem nalezl další šifrovanou korespondenci mezi písemnostmi kardinála Toussainta de Forbin-Janson. Jde o dopisy [Jacquese] de Gaffarel Sauvans z roku 1677 z Říma. Tamtéž, RA Beaufort-Spontin, krabice 25.

užívání šifer ve středoevropském prostoru v raném novověku, které je předmětem závěrečné části článku.

Obrázek 11 – klíč s kryptonymy pro korespondenci především v záležitostech Slezska (první strana), [cca přelom 17. a 18. století].

Poznatky získané ze studia pramenů uložených v SOA v Plzni doplňuji ještě o informace, které poskytují fondy rodinných archivů v dalších státních oblastních archivech, jejichž výčet jsem uvedl výše. Je však třeba znovu připomenout, že tyto fondy a jejich archiválie jsem studoval pouze výběrově a naprostá většina z nich na podrobnější zkoumání teprve čeká.

(pokračování v příštím čísle)

B. Lúštitelia historických šifier - A.V. Maloch a Josef Šusta

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

Existuje zjavné protirečenie medzi vzrušením, ktoré podnecujú šifry popisované v literárnej fikcii a nezáživným dojmom, ktoré poskytujú ich reálne historické prípady výskytu. Populárni spisovatelia detektívnych diel či žánru sci-fi ako E. A. Poe, Isaac Asimov, A. C. Doyle, Agatha Christie či z novších autorov bestsellerov Umberto Eco a Dan Brown, v ktorých šifry zväčša zohrávajú hlavnú úlohu. Naproti tejto ich popularite, skutočné historické šifry - obzvlášť z ranomodernej doby - skôr vyvolávajú všeobecnú nudu a zdajú sa úplne neatraktívnymi prameňmi. Zvyčajne sa vyskytujú vo forme viac menej dlhokánskeho a nezaujímavého radu čísel alebo znakov. Jeden by mohol samozrejme namietnuť, že nie ich vzhľad, ale obsah je dôležitý. Táto námietka, akokoľvek sa môže zdať relevantná, nie je nutne pravdou. Približne deväťdesiat percent všetkých historických prameňov zašifrovaných čo i len jednoduchou zámenou a ktoré sa zachovali z ranomodernej doby sú rozlúštené: zvyčajne to bol adresát, ktorý starostlivo spísal otvorené znenie ponad príslušný šifrovaný text. Niekedy však sa vyskytnú prípady, kedy tento text nemáme k dispozícií a čo sa stalo, ak sa do ich zákutí zaplietli naši kandidáti, to sa v ďalšom texte vynasnažíme opísať.

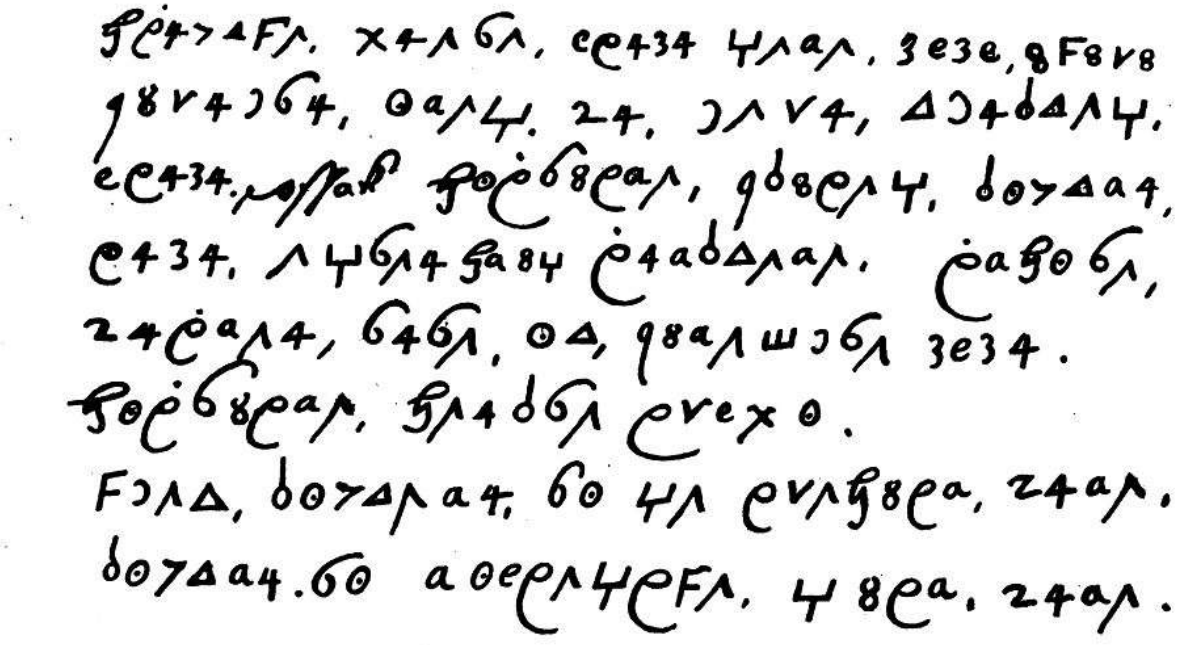
Prvotné zoznámenie

Obaja boli historikmi, jeden v pozícii váženého akademika a vedúceho poprednej českej vedeckej inštitúcie ďalší praktický „všeumelec“. Každý z nich celý svoj mimoriadne plodný život zasvätili práci pre spoznávanie a rozpracovanie dejín českého národa v mnohých vedeckých publikáciách. Poďme sa však najprv bližšie pozrieť na životné osudy prvého z menovaných velikánov. Antonín Maloch sa narodil v Prahe 30. augusta 1823. Pôsobil zväčša ako stredoškolský učiteľ v Prahe, Jindřichově Hradci a od roku 1851 ako profesor v Jičíne, kde vyučoval dočasne tiež spev. Napísal množstvo českých i v nemčine zostavených spisov a vlastivedných pojednaní. S Janem Tobiáškem, vtedajším jičínským kaplanom, vydal České zpěvy (Jičín 1856, Praha 1862, druhé vydání). Okrem muzikológie sa od dôb svojich štúdií práv a filozofie na pražskej univerzite naplno venoval topografii a už ako študent prispieval do svetoznámej monografie nemeckého bádateľa Hebera venovanej českým hradom. Mladý Maloch svojím historicko-kritickým prístupom k prameňom Heberovu prácu povzniesol do značnej úrovne čo sa týka kvality a po predčasnej Heberovej smrti sa dokonca pokúsil o jej pokračovanie. Zákonite sa črtal veľký sen o zostavenie monumentálneho historicko-topografického popisu Čiech, ktorý by sa opieral o autentické písomné pramene a ktorého hĺbka i rozsah by predstavoval konkurenciu nielen v Čechách, ale i v susedných krajinách. Za týmto účelom sa pustil do podrobného skúmania zemských dosiek, bohužiaľ však v tejto práci ďalej nemohol pokračovať, pretože bola náhle prerušená neočakávanou udalosťou.

Obr. 1 Antonín Vánkomil (Zefyrin) Maloch

Nečakaný nález

V roku 1847 niekoľko týždňov po bližšie nešpecifikovanej nehode strávil A. V. Maloch v Pelhřimove. Pri tejto príležitosti si začal krátiť voľné chvíle rôznymi formami duševného cvičenia. Keď sa dokonale a s plnou kratochvíľou rozptýlil počas častých prechádzok po meste a v jeho blízkom okolí, náhodou naďabil na záhadný spis, ktorého príťažlivosť ho neomylne nasmerovala k pokusom lúštiť šifrované správy v nemeckom i latinskom jazyku. Tento spis, o jeho názve a pôvode sa Maloch bližšie nevyjadruje, sa mi nepodarilo dodatočne dohľadať, pretože sa nespomína nikde v dostupnej literatúre ba ani v ďalších známych článkoch z jeho pera. O dva roky neskôr, príjemne prekvapený nálezom listu zašifrovaného v jeho materinskom českom jazyku, uverejnenom v zborníku správ zo zasadania cisárskej českej spoločnosti prírodných vied z rokov 1845-46 na str. 156 - 238, ktorý bol súčasťou zbierky korešpondencie medzi cisárom Rudolfom II. a jeho bratom Matyášom a ďalšími vysokopostavenými šľachticmi, spracovanej významným českým spisovateľom, historikom a knihovníkom Václavom Hankom. Táto postava českého národného obrodenia ako je známe sa smutne preslávila viacerými zhotoveniami vyfabrikovaných "starodávnych" českých rukopisov, z ktorých najznámejšie boli **Rukopis královédvorský** a **Rukopis zelenohorský**. V predhovore k tejto nesporne zaujímavej zbierke listov sa píše: "*V záznamoch zo zasadania tejto spoločnosti vyšlo:* ***Osud pasovských žoldnierov Franza Kurza v Čechách až k ich rozprášeniu v roku 1611***" neskôr: "***O rokovaní s pánom von Rosenbergom počas Vpádu pasovských žoldnierov do Čiech v roku 1611***" *od slovutného pána von Hammer-Purgstall, ako celok k predchádzajúcemu a pripojiť k tejto veci ešte túto korešpondenciu za tým účelom, aby sme mohli trvale a vyčerpávajuco pochopiť. Táto sa skladá z viac než 60 pôvodných dokumentov, z ktorých časť bola písaná v šifrách, pri ktorých bolo našťastie viacero šifrových abecied, vložených na osobitých hárkoch. Iba jeden malý papierový lístok v češtine nebol podľa nich vôbec rozlúštiteľný -- ale i tak som ho tu litografický zaznamenal.*" Tieto riadky Malocha podľa jeho vyjadrení poriadne navnadili, keďže sa z nich dozvedel zaujímavé zistenie,"*že sa (pokiaľ je známe) doposiaľ nik o rozlúštenie chiffrovaného písma v českej reči nepokúsil.*" Preto sa sám pustil do vopred neznámeho písma s odhodlaním, že si na konci snaženia prečíta jeho otvorený text.



Obr. 2 Záhadný šifrovaný list

Postup lúštenia

Pozrime sa teraz bližšie upriamiť na zašifrovaný lístok. Ako si iste všimnete a čo pána profesora Malocha udrelo do očí ako prvé, v texte je jasne viditeľné slovíčko "však" (wssak), čo poukazuje na predpoklad, že lístok je napísaný v českom jazyku. Jeho výskyt uľačil odhad použitého jazyka čo neskôr po práve pán Maloch zhodnotil v r. 1863, keď pre Riegrův Slovník naučný zostavil tématické state o kryptografii a lúštení šifier a kódov: "*Objevení jazyka jest při rozlušťování úlohou nejprvnější a nejdůležitější.*"

Celkový popis základných pravidiel pána Malocha pre lúštenie jednoduchej zámeny je nasledovný:

"1. Každé slovo musí míti aspoň jednu samohlásku (v slovanštině i polohlásku l neb r); tyto se musí nejdříve vyhledati.
2. Jsouť slova sestávající jen z jednoho písmene (monogramm) neb ze dvou (bigramm) neb ze tří (trigramm); počet prvních dvou je nepatrný, třetích aspoň lehce dostižitelný: tato slova dají se nejlehčeji vyhledati a přečísti.
3. V jednotlivých jazycích se jistá samohláska a jistá souhláska nejčastěji objevují (k. př. v češtině i, v němčině e a n), jiná často, jiná opět buď zřídka, buď skoro nikdy (ku př. x).
4. Některé řeči užívají zdvojených hlásek (Zwillingsbuchstaben, aa, ll, ss atd.), jiné nikoli.
5. Počet písmen je nejméně 20, ale sahá v některých řečech až přes 30; dle toho dá se poněkud souditi o řeči, nížto spis psán jest."

Abecedné a gramatické zvláštnosti jazyka českého, ktoré si podľa Malocha najviac zasluhujú uviesť a sú upotrebiteľné pri lúštení:
"Čeština (a slovanština vůbec) má mnoho monogrammů (a, i, k, o, s, u, z) a bigrammů (ač, ach, aj, an, as, ať, až, ba, co, či, čí, do, ej, ha, he, ho, já, je, ji, jí, ke, ku, ký, má, mě, mi, mu, my, na, ne, ně, ni, ní, nu, ob, oč, od, ok, on, oň, os, ou, po, se, si, ta, tě, té, ti, to, tu, ty, uč, um, už, úd, úl, úp, ve, vy, za, ze, že) a zvláště trigrammů, veliký počet písmen (zvláště když se á, é, í, ó, ú, ů, ý, č, ď, ň, ř, š, ť, ž, ch vyznačí zvláštními znamínky - nikoli složenými jako cs, ss, rz atd.), vedlé samohlásek tvoří se slabiky též pomocí polohlásek (l, r) a měkkého ě jiným jazykům neznámého; s e nepočíná žádné slovo (leda cizí), není též žádné zdvojené hlásky (leda nahodilým sloučením, jako: bylli, poddaný)."

Pri riadení sa týmito pravidlami napokon dospel k doslovnému rozlúšteniu i so všetkými pravopisnými chybami:
"Wšeczki heini (=hájné) usebe miti bubu (=budu) okolo poledne, atim ge dile zderzim usebe.
Wssak
wašnosti prosim raczte sebe imniewtom šetrziti.
štwani geštie neni, az potiždni bube wašnosti wierni sluha.
Kdiz raczite na mi sliwost geti,
raczte na tausimski most geti."

Po takom (najmä z hľadiska možností tej doby) prácnom a zdĺhavom duševnom namáhaní však by sme tu mohli súhlasiť s pánom Malochom podľa článku [1] a skonštatovať, že obsah tohto listu po stránke historicko-odbornej nie je príliš zaujímavý.


LUMÍR.

BELLETRISTICKÝ TÝDENNÍK.

Odpovědný redaktor: Ferdinand B. Mikovec.

Číslo 9. 4. března 1858. VIII. ročník.

Obr. 3: Titulný list časopisu Lumír č. 9 z roku 1858

Keďže bol v r. 1849 ako mladý začínajúci učiteľ preložený na miesto zastupujúceho profesora do Jindřichova Hradce a neskôr v r. 1851 povolaný do Jičína, ktorý sa následne stal natrvalo jeho domovom až takmer do smrti v r. 1888. Pán prof. Maloch podľa svojich vyznaní v listoch historikovi Františkovi Palackému, či autorovi Slovníku naučného F.L. Riegrovi, nebol v Jičíně príliš rád. Pripadal si tu zastrčený, obmedzovaný, nedocenený, ďaleko od vytúženej Prahy - centra vedeckého diania, v ktorom by mohol lepšie rozvíjať svoje vlohy a zúročiť svoje znalosti. O "bídné nečinnosti", spomínanej v liste Palackému, se však nedá hovoriť. Už od svojho príchodu do Jičína vykazoval prof. Maloch široké vedecké aktivity. Spísal mnoho štúdií, najviac oceňovaný bol jeho úspech, keď Belgická akadémia vied vyhlásila súťaž o cenu 6 000 frankov o prácu na tému: Kde sa narodil cisár Karol Veľký?, ktorú on s prehľadom vyhral. Ako už bolo spomenuté vyššie, koncom 50. rokov 19. storočia sa Maloch výrazne podieľal na odbornej úrovni Riegrova slovníku naučného, do ktorého nielenže prispieval svojimi textami, ale rovnako tak ovplyvňoval štruktúru a celkovú koncepciu diela. Svoju erudíciu preukázal začiatkom 60. rokov 19. storočia, keď upozornil na jazykové nezrovnalosti vo vyššie spomínanom Rukopise královédvorském, pričom si všimol zvláštneho výskytu slova "tábor", ktorý sa vo význame vojenského ubytovania začal používať až v 15. storočí. Ďalej sa preslávil ako najväčší znalec a propagátor Prachovských skál, ktorých prieskumu a dokumentácii venoval mnoho rokov svojho života, stál u zrodu sústavného turistického zájmu o tento skalný komplex. Ako prvý tu vykonal aj archeologické výskumy. Táto naoko idyla sa však mala čoskoro skončiť.

Na jar roku 1880 však prebehol na stránkach jičínskej tlače nešťastný a zbytočný spor medzi stredoškolským učiteľom Malochom a jičínskou verejnosťou. Podstata spočívala v tom, že jeho študenti si požičali originálne nákresy Prachovského skalného komplexu, ktoré v roku 1877 osobne zhotovil pomocou kompasu po podrobnom krokovaní a predal do tlače miestnemu litografovi, ktorý však náhle ochorel, preto ich nemohol prekresliť do finálnej podoby. Dnes už je jasné, že sa táto vec neúmyselne pretiahla a zamýšľané dielo nebolo nikdy dokončené. Celé to teda pokračovalo o dva roky neskôr, pri návšteve známeho vášnivého turistu Vojtu Náprstka. Študenti, podobní nadšenci, však zašli ešte ďalej a uverejnili svoj vlastný plánik v miestnej tlačiarni. Následne sa spor vyhrotil vzájomným obviňovaním na stránkach miestnych novín. Krátko nato, po odchode do Prahy s celou rodinou, prof. Maloch nečakane zomrel 3. apríla 1880. Vinou jeho náhlej smrti už nemohol byť spor urovnaný, napokon sa však po dlhých 130 rokoch aspoň zčasti všetko dobre skončilo.

Sľubný začiatok

Otec, Josef Šusta st., bol riaditeľ schwarzenbergských panstiev v Třeboni a významný odborník v oblasti rybníkárstva. Z takéhoto prostredia pochádzal významný historik Josef Šusta, ktorý vo svojich historických prvotinách nezaprel ohlasy juhočeského domova (napr. o Závišovi z Falkenštejna). Keďže bol nepochybne ovplyvnený rodinnou tradíciou, už čoskoro nato a vo svojej dobe sa prekvapivo venoval hospodárskym dejinám. Po absolvovaní Cisárskej kráľovskej českej reálky v Třeboni študoval históriu na Karlo-Ferdinandovej univerzite v Prahe a na Inštitúte pro rakúsky dejepis vo Viedni.

Obr. 4 Významný historik Josef Šusta (1874-1945)

V rokoch 1896 až 1899 pôsobil ako štipendista Rakúskeho historického ústavu v Ríme (ako uvidíme nižšie, počas pobytu práve tu rozlúštil šifrovanú korešpondenciu) a od septembra 1900 pôsobil ako profesor histórie na Československej obchodnej akadémii v Prahe, pričom sa takmer zároveň habilitoval na univerzite pre odbor všeobecné dejiny prácou Pius IV. Před pontifikátem a na začátku pontifikátu.. Práve pri zostavovaní tejto knihy potreboval vykonať hĺbkový výskum vo Vatikánskych archívoch.

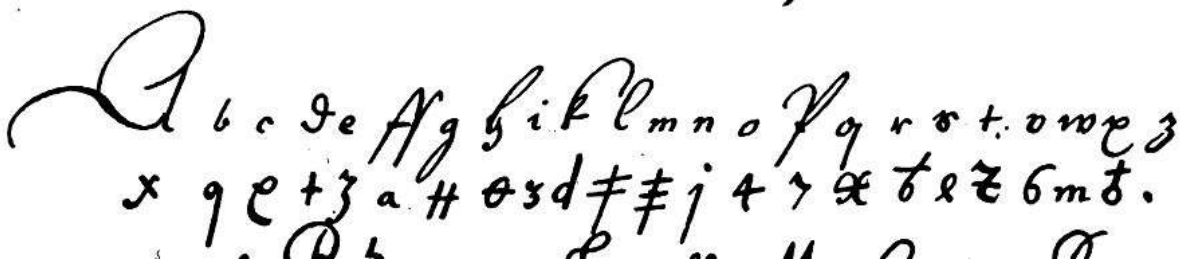
Priblíženie doby

Bol to čas veľkých spoločenských zmien, mimoriadnych vedeckých a zámorských objavov, vynálezov nielen v hospodárstve a vo vede ale aj na poli diplomacie a cirkevnej politiky. Cirkevné prostredie v sledovanom období počas tridentského koncilu poskytovalo mnohé zaujímavé momenty. Tento koncil bol prelomový z hľadiska postoja upevnenia a obnovy pápežstva po renesančných výstrelkoch v umení a literatúre a rozpustilých mravných pokleskoch predchádzajúcich zástupcov na stolci Petrovom. Započal ho už síce ešte "staromódne" zmýšľajúci Pavol III. dňa 23. mája 1937, zvolaním koncilu do Mantovy, z ktorej pochádzal aj neskorší predseda kardinál Ercole Gonzaga, ale o 8 rokov neskôr došlo k dlhšiemu prerušeniu kvôli rozhoreniu sa vojnového konfliktu s protestantským Šmalkaldským spolkom. Po nastolení formálnej dohody - zdanlivého kľudu zbraní - vďaka tzv. **Ausburgskému mieru** v r. 1555 už nič nestálo v ceste pokračovaniu koncilových rokovaní. Ale aj napriek tomu trvalo ďalších päť rokov, než nový pápež Pius IV. bulou **Ad Ecclesiae regimen** povolal všetko kresťanstvo do Tridentu. Prelátov ako zodpovedných za riadenie koncilu Pius IV. poveril 5 kardinálov, medzi ktorými najvyznamnejším bol už spomínaný mantovský kardinál Gonzaga. V ďalších konciliárnych jednaniach medzi priaznivcami a odporcami tzv. **Reformationslibell** (ktorá bola výsledkom cisárových poradcov z tajnej rady, okrem zrejmých návrhov ako oprava katechizmu, rozpracovanie spôsobu vydávania

"nezávadných" katolíckych kníh obsahovala dokonca povolenie prijímať pod obojím, obmedzenie pôstu a povolenie manželstva kňazov) ríšskonemeckého cisára Ferdinanda I., ktorého prekvapivo po ich príchode na koncil zčasti "podporila" francúzska časť prelátov, a to návrhmi, ktoré cisárski zástupcovia - Brus z Mohelnice - pražský arcibiskup, gróf Žigmund Thun a biskup Draškovič z Pécsa – slov. Päťkostolia hneď neignorovali. Cisár však ohrozil koncil tým, že pod zámienkou jeho "ochrany" sa presťahoval do Innsbrucku. A tu náhle uprostred tejto zdanlivo neriešiteľnej situácie zomrel vyčerpaním predseda koncilu kardinál z Mantovy. Hlavnou príčinou, prečo koncil neprerušil svoje jednania, bola zásluha nového predsedu koncilu, kardinála Moroneho, ktorého na tento post nominoval sám Pius IV. Dostal sa naň "priamo" z väzenia v Anjelskom hrade, aby sa nakoniec osvedčil svojou skúsenosťou (bol najstarším žijúcim kardinálom), diplomatickou obratnosťou a politickým nadaním a vyviedol koncil zo slepej uličky nesplnených túžob a požiadaviek, ukľudnil nespokojné svetské hlavy a za účelom predloženia konkrétnej vecnej a prijateľnej reformy navštíviť cisára v Innsbrucku. Ten o ňom po osobnom jednaní vyhlásil: "*Náš dobrý kardinál Morone bude starostlivo dbať na dobrú reformu cirkvi*". Predložil ju v júli 1563, rozpracovanú do 42 bodov, nasmerovanú k vnútornej obnove cirkevného života a v niekoľkých bodoch sa priblížila k požiadavkám Reformationslibell. Počas konciliárnych rokovaní mu dokonca samotný Pius IV. vyšiel v ústrety.

Zaujímavé odhalenie

V približne trojstoročnom období od objavenia sa primitívnych značiek a bodiek ako náhradných znakov za samohlásky, roztrúsených po rukopisoch v rámci pápežskej kancelárie v 13. a 14. storočí, počínajúc primitívnym kódom sa dajú načrtnúť niektoré základné trendy. Centrálne pápežstvo a jeho tajomníci, úradníci pre šifry (úrad tajomníka bol zavedený v r. 1555 a zastával ho prelát Trifón Bencio z Assisi, ktorý sa preslávil aj ako úspešný lúštiteľ tajnej korešpondencie španielskeho kráľa Filipa II. a šifrovaného listu tureckého agenta) opustili **jednoduché monoalfabetické šifry** (v ktorých každé písmeno malo jeden šifrový ekvivalent) a v bežnej korešpondencii s agentami a diplomatickými zástupcami sa postupne obracalo na utajovacie prostriedky poskytujúce zložitejšie homofónne substitúcie jednotlivých písmen otvoreného textu, pričom sa nakoniec dospelo až k tzv. **nomenklátorom**, kde sa ako šifrové jednotky používali tiež osobitné znaky alebo čísla pre slabiky spolu s hojným využitím tzv. **klamačov** a často sa vyskytujúcich kódových slov.



Obr. 5 Príklad jednoduchej substitúcie z vyššie zmienenej práce V. Hanku [2]

Rovnaké prostriedky na šifrovanie svojich vlastných správ zo zasadaní koncilu, jednaní s predstaviteľmi popredných európskych panovníckych dvorov a delegácií mestských štátov používal aj kardinál Morone. keď dňa 10. Apríla naňho dorazil, vzápätí však už cestoval 16. apríla k cisárovi, a potom sa natrvalo usídlil v Tridente, kde prebýval odo dňa 17. mája 1563 až skončenia koncilu v decembri 1563. A práve počas študijného pobytu v Ríme Josef Šusta nachádza vo tajnom Vatikánskom archíve sedemnásť doteraz neznámych šifrovaných listov, ktoré Morone odosielal pri svojich cestách z a do Ríma, presnejšie na polici č. LXII. v krabici pod označením T. 27, Č. 5, 18, 23, 23a, 32, 37, 46, 50, 66, 79, 81, a ďalšie v krabici T. 29 pod

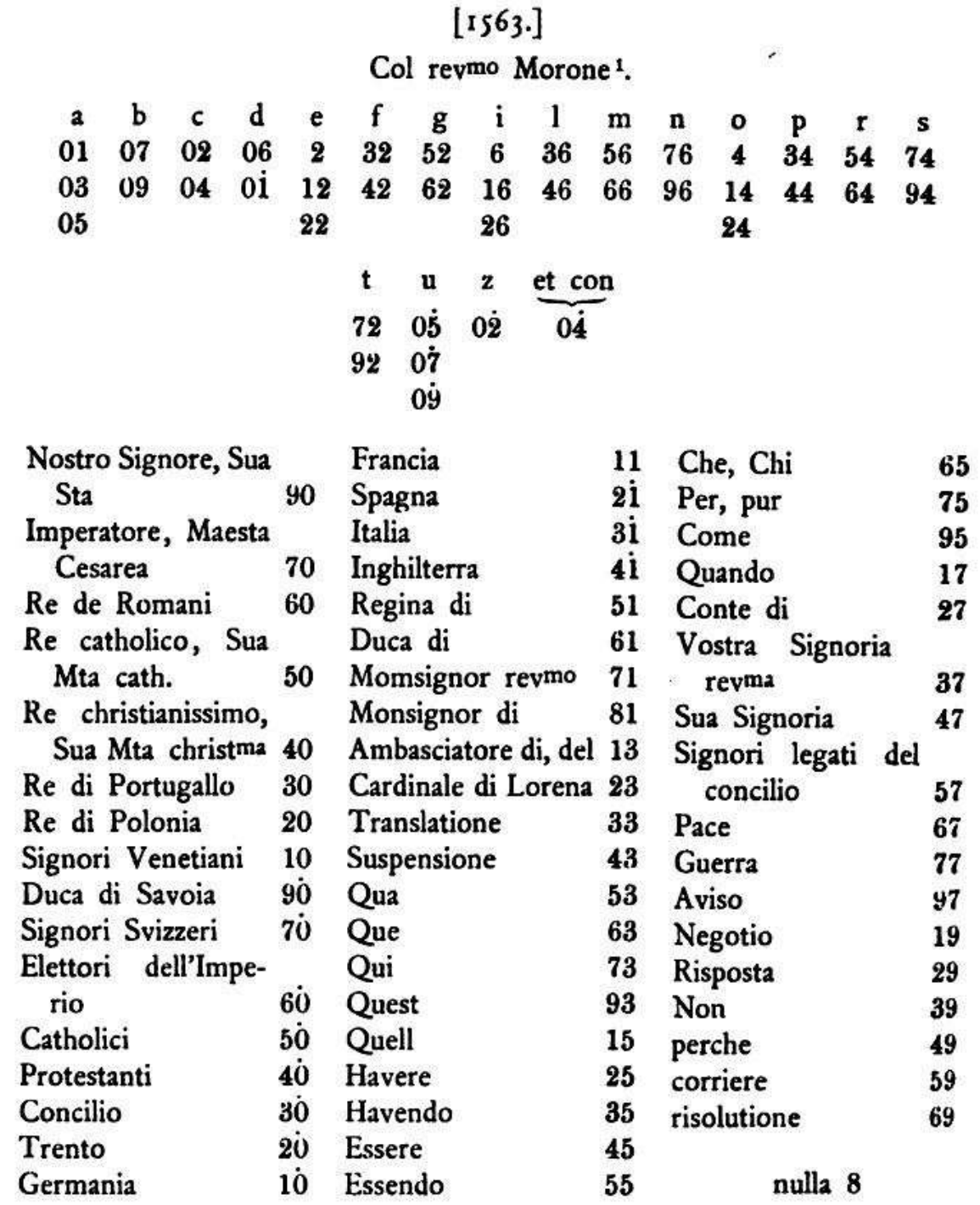
číselným ozn. 107, 108, 114, 115, 116 a v krabici č. 68 pod č. 134. Z týchto zachovaných archívnych dokumentov a menoslovov účastníkov Tridentu pán Josef Susta zrekonštruoval jednoduchý Moroneho nomenklátor v článku [8], podoba ktorého je uvedená aj v rozsiahlej práci padebornského profesora histórie a archivára Aloysa Meistera.

Chiffre chiffrant.

Buchstaben		Nomenclator			
a	01, 03, 05	S. Stà, N. Sre	90	avviso	97
b	07, 09	imperatore	70	havere	25
c	02, 04	re Catholico	50	havendo	35
d	06, 0i	cardinale Lorena	23	essere	45
e	2, 12, 22	concilio	30	essendo	55
f	32, 42	Trento	20	quì	73
g	52, 62	Germania	10	questo	93
i	6, 16, 26	Francia	11	quello	15
l	36, 46	Spagna	21	che	65
m	56, 66	vescovo	71	per	75
n	76, 96	monsignore	91	quà	53
o	4, 14, 24	duca	61	que	63
p	34, 44	V. Sria Illma	37	come	95
r	54, 64	S. Sria Illma	47	non	39
s	74, 94	legati	57	quando	17
t	72, 92	negocio	19	et	04
u	05, 07, 09	risposta	29	con	
z	02	corriere	59		
Chiffre non-valeur					8

Obr. 6: Nomenklátor kardinála Moroneho – časť šifrant

Avšak porovnaním s ním uvedeným nomenklátorom sa ukáže na jednej strane, že Šustom odhalený šifrovací kľúč, ktorý bol v dôsledku ním odhaleného malého množstva archívneho materiálu obmedzený len na abecedu a základné numerické kódy, na druhej strane sa však u neho vyskytli malé chyby pretože podľa správnosti mali byť nad čísla pri kódových výrazoch vytlačené bodky a to napr. pri slove **concilio** = 30, **Trento** = 20, **Germania** =10, **Spagna** = 21 atď. Bádanie v tajných archívoch Vatikánu umožnil pápež Lev XIII. ich otvorením v r. 1881, a týmto nečakaným ťahom umožnil aj historikom a študentom cisárskeho rakúskeho inštitútu (ktorého členom bol Šusta) nahliadnuť od zaprášených zväzkov a poodhaliť tak niekoľko storočí prehliadané informácie o zaujímavých udalostiach cirkevnej histórie.



[1563.]

Col revmo Morone[1].

a	b	c	d	e	f	g	i	l	m	n	o	p	r	s
01	07	02	06	2	32	52	6	36	56	76	4	34	54	74
03	09	04	0i	12	42	62	16	46	66	96	14	44	64	94
05				22			26				24			

t	u	z	et con
72	05	02	04
92	07		
	09		

Nostro Signore, Sua Sta	90	Francia	11	Che, Chi	65
Imperatore, Maesta Cesarea	70	Spagna	21	Per, pur	75
Re de Romani	60	Italia	31	Come	95
Re catholico, Sua Mta cath.	50	Inghilterra	41	Quando	17
Re christianissimo, Sua Mta christma	40	Regina di	51	Conte di	27
Re di Portugallo	30	Duca di	61	Vostra Signoria revma	37
Re di Polonia	20	Momsignor revmo	71	Sua Signoria	47
Signori Venetiani	10	Monsignor di	81	Signori legati del concilio	57
Duca di Savoia	90	Ambasciatore di, del	13	Pace	67
Signori Svizzeri	70	Cardinale di Lorena	23	Guerra	77
Elettori dell'Imperio	60	Translatione	33	Aviso	97
Catholici	50	Suspensione	43	Negotio	19
Protestanti	40	Qua	53	Risposta	29
Concilio	30	Que	63	Non	39
Trento	20	Qui	73	perche	49
Germania	10	Quest	93	corriere	59
		Quell	15	risolutione	69
		Havere	25		
		Havendo	35	nulla 8	
		Essere	45		
		Essendo	55		

Obr. 7: Verzia doplnená o kódové výrazy a opravená A. Meisterom v práci [9]

Význam historického diela

Ucelené Šustovo dielo na poli histórie netreba snáď ani spomínať. Prípadných záujemcov odkážme len na výstižné zhodnotenie v knihe[7]. Možno len s ľutosťou konštatovať, že nikdy nevyšiel už pripravený zborník k Šustovým sedemdesiatinám, obsahujúci okrem iných príspevkov a bibliografie tiež stručný životopis od dr. Josefa Hobzka (jeho rukopis sa bohužiaľ stratil po autorovej smrti v roku 1989).

Josef Šusta bol profesorom všeobecných dejín na Karlovej univerzite a v dvadsiatych rokoch tiež zastával funkciu ministra školstva a národnej osvety. Jednalo sa o jeho jediný priamy vstup do politiky, i keď politický život ovplyvňoval tiež v nasledujúcich rokoch napr. ako

člen tzv. Pátečníků. Na sklonku života sa stal predstaviteľom českej vedy ako prezident Českej akadémie vied a umení. V tejto funkcií v ťažkých dobách nemeckej okupácie usiloval o udržanie kontinuity českého vedeckého a kultúrneho života. Podľa svedectva pamätníkov chcel zabrániť zneužitiu svojho diela nacistickými okupantami a preto odmietol vydanie uvedeného jubilejného zborníka. Očakával jeho následné vydanie v svobodných časoch. Bohužiaľ sa tak už nestalo. Prof. Šusta bol nespravodlivo obvinený z kolaborácie a napadnutú česť vedca a Čecha doviedol obhájiť aj dobrovoľným odchodom zo života v máji 1945 (F. Kutnar). Telesné pozostatky prof. Šusty boli uložené neďaleko jeho dlhoročného sídla - vily v Prahe na Hanspaulce, na neďaleký cintorín u kostola sv. Mateja presne pri západnom priečelí kostola, kde je od cintorínovej rampy nádherný výhľad do Šáreckého údolia. A práve tu bývalo Šustovo obľúbené miesto prechádzok. Z finančným príspením ČSAV bola na vybranom mieste postavená v polovici päťdesiatych rokov Šustova hrobka vo forme sarkofágu, podľa návrhu architekta prof. Jana Sokola. Na jej zadnej strane je nápis: **Prezidentovi Českej akadémie vied a umenia - Čs. akadémie vied.**

Literatúra:

[1] Maloch, Antonín V., *Rozluštění chiffrovaného písma v češtině*, Lumír, Roč. VIII, č. 9, 4.3.1858, s. 205-206,

[2] 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 in Betreff des passauischen Kriegsvolkes*** (*Aus den Abhandlungen der königl. böhm. Gesellschaft der Wissenschaften*. V. Folge, Band 4.), Druck der k. k. Hofbuchdruckerei von Gottlieb Haase Söhne, Prag, 1845 - 84s. Šifrovaný list je vložený medzi strany 42 a 43 a ozn. ako strana 48(?).

[3] Maloch, A. V.: Riegrův slovník naučný, 1863, II. díl, Heslo: Dechiffrování, s. 103: http://katkryptolog.blogspot.sk/2013/02/heslo-dechiffrovani-z-riegrova-slovniku.html

[4] A. V. Maloch a Jičín :: Symbolické usmíření Antonína Vánkomila Malocha s městem Jičínem: http://www.jicinskabeseda.cz/projekty/symbolicke-usmireni-a-v-malocha-s-mestem-jicinem/

[5] Z přednášky o Antonímu Vánkomilu Malochovi - Jičínský deník, 18.2.2013: http://jicinsky.denik.cz/kultura_region/jicin-prednaska-maloch20100615.html

[6] Šusta, Josef, *Die römische Kurie und das Konzil von Trient unter Pius IV*. Wien, 1904–1914

[7] Kutnar, František, *Přehledné dějiny českého a slovenského dějepisectví II*, Praha, 1977

[8] Šusta, Josef. *Eine päpstliche Geheimschrift aus dem 16. Jahrhundert*. Mitteilungen des Instituts für Österreichische Geschichtsforschung, XVIII. Band, 1897, pp. 367-371

[9] Meister, Aloys, *Die geheimschrift im dienste der Päpstlichen kurie von ihren anfängen bis zum ende des XVI jahrhunderts, Padeborn,* 1906, S. 260-261

[10] Francek, Jindřich , *Jičínský historiograf Antonín Vánkomil Maloch*, in: **Zpravodaj Krajského muzea východních Čech** 8, 1981/2-3, s. 25-47

C. Elektronický podpis v praxi

Seminář, termín: 5. - 6. března 2013
Přednášející: P.Vondruška a J.Peterka
http://www.konference.cz/photos_files/akce_2717_3_C1317_pre_program.pdf

Program semináře IIR: **Elektronický podpis v praxi**

ÚTERÝ 5. BŘEZNA 2013

Základní pojmy asymetrické kryptografie

- Základy asymetrické kryptografie (veřejný, soukromý, klíč, algoritmy, požadavky na velikost modulu - klíče)
- Hashovací funkce (kolize prvního a druhého řádu, vlastnosti, vhodné algoritmy, užití)
- Technologie digitálního podpisu, šifrování s využitím asymetrické kryptografie, SSL protokol, autentizace

Právní změny, které upravují elektronický podpis

- Zákon 227/2000 Sb. O elektronickém podpisu
- Certifikační autorita (CA), základní činnost, druhy CA
- Typy elektronických podpisů (elektronický podpis, zaručený elektronický podpis, uznávaný podpis, „kvalifikovaný podpis", elektronická značka)
- Druhy certifikátů (kvalifikovaný, komerční, systémový kvalifikovaný certifikát)
- Položky certifikátu (taxativní, význam položek, identifikátor vlastníka), životní cyklus, CRL
- Časová razítka (význam, protokol) x časová značka
- Přehled CA v ČR, SR a v EU

Důvěra v certifikáty a způsoby ověření

- Ověření platnosti certifikátu - sestavení certifikační cesty, CRL, důvěra v certifikát poskytovatele
- Různá úskalí při sestavování cesty - metody sestavení cesty včetně metody AKID-SKID, výměna kořenového certifikátu
- Zajištění důvěry v kořenový certifikát akreditovaného poskytovatele (v ČR a SR)
- Ověření, že certifikát byl vydán jako kvalifikovaný v EU, uznávání
- Důvěra v kořenové certifikáty v běžné praxi (úložiště v MS CAPI, Mozilla, VeriSign, Thawte, ČR)
- Způsob „hlídání" chování poskytovatelů certifikačních služeb - Valicert. org., akreditační schéma, cross - certifikace, bridge
- Jak zajistit implementaci důvěryhodných certifikátů v úložišti - uživatel vs. centrální politika, samoinstalační balíčky, bezpečnostní záplaty

MGR. PAVEL VONDRUŠKA, KRYPTOLOG, PRAHA

STŘEDA 6. BŘEZNA 2013

Podepisování a ověřování elektronických podpisů na PDF dokumentech

S jakými druhy podpisů a razítek se lze setkat u PDF dokumentů?

- Viditelné, neviditelné, tisknutelné a netisknutelné podpisy
- Schvalující a certifikační podpisy
- Prázdné podpisy
- Ruční podpisy
- Podpisová a archivní časová razítka

Co je potřeba vědět o elektronických podpisech?

- Jaké jsou podmínky pro platnost a neplatnost podpisu?
- Co znamená, když výsledek ověření zní: nevím?
- Jak se pozná, zda je elektronický podpis kvalifikovaný nebo jen zaručený
- Jakou roli hraje faktor času? Jakou roli hraje časové razítko?
- Jakou roli hrají revokační informace a jejich (ne)dostupnost
- Možnost vkládání revokačních informací do elektronických podpisů
- Koncepce dlouhodobých elektronických podpisů

Nastavení Adobe Readeru pro ověřování podpisů

- Volba úložiště důvěryhodných certifikátů
- Instalace certifikátů autorit
- Volba posuzovaného okamžiku
- Nastavení způsobu vyhodnocování revokačních informací

Praktické ověřování podpisů na PDF dokumentech – na příkladech

- Podpis, založený na již expirovaném certifikátu
- Podpis, založený na revokovaném certifikátu
- Podpis s vloženými revokačními informacemi
- Nastavení Adobe Readeru pro podepisování
- Možnosti podepisování a připojování časových razítek v Adobe Readeru
- PDF dokumenty odemknuté pro změny v Adobe Readeru
- Volba úložiště a umístění soukromého klíče a certifikátů
- Nastavení autority časového razítka
- Vkládání revokačních informací
- Konkrétní příklady podepisování PDF dokumentů

RNDR. ING. JIŘÍ PETERKA, NEZÁVISLÝ PUBLICISTA, PRAHA

5. – 6. března 2013, Jurys Inn Prague Hotel, Praha **www.konference.cz**

D. SOOM.cz - Hacking & Security konference #2
Roman Kümmel

Server SOOM.cz si Vás dovoluje pozvat na druhý ročník odborné konference věnované hackingu a informační bezpečnosti, která se uskuteční 15.března 2013 v Praze. Návštěvníky čeká den plný zajímavých přednášek v příjemném prostředí konferenčního centra Green Point.

Se svým příspěvkem vystoupí známá kontroverzní umělecká skupina **Ztohoven** nebo **Asociace českých lockpickerů**, která šokujícím způsobem předvede návštěvníkům různé způsoby otevírání mnoha typů zámků. Dokonce i těch, jejichž majitelé věří, že dokonale ochrání jejich majetek.

Igor Hák, provozovatel webového portálu viry.cz věnuje svou prezentaci doplněnou mnoha praktickými ukázkami novým trendům v oblasti malware a virovým hrozbám. **Jan Šeda** se zaměří na fenomén dnešní doby, kterým není nic menšího než cloud. Jeho poznatky z praxe upozorní zájemce o tuto technologii na některá rizika a úskalí, která jsou s ní spojena. **Roman Kümmel** nastíní možnosti klamání uživatelů, kteří dnes již jen stěží dokáží odhalit rozdíl mezi instalovaným softwarem, součástmi operačního systému nebo webovou aplikací, která je pod kontrolou útočníka.

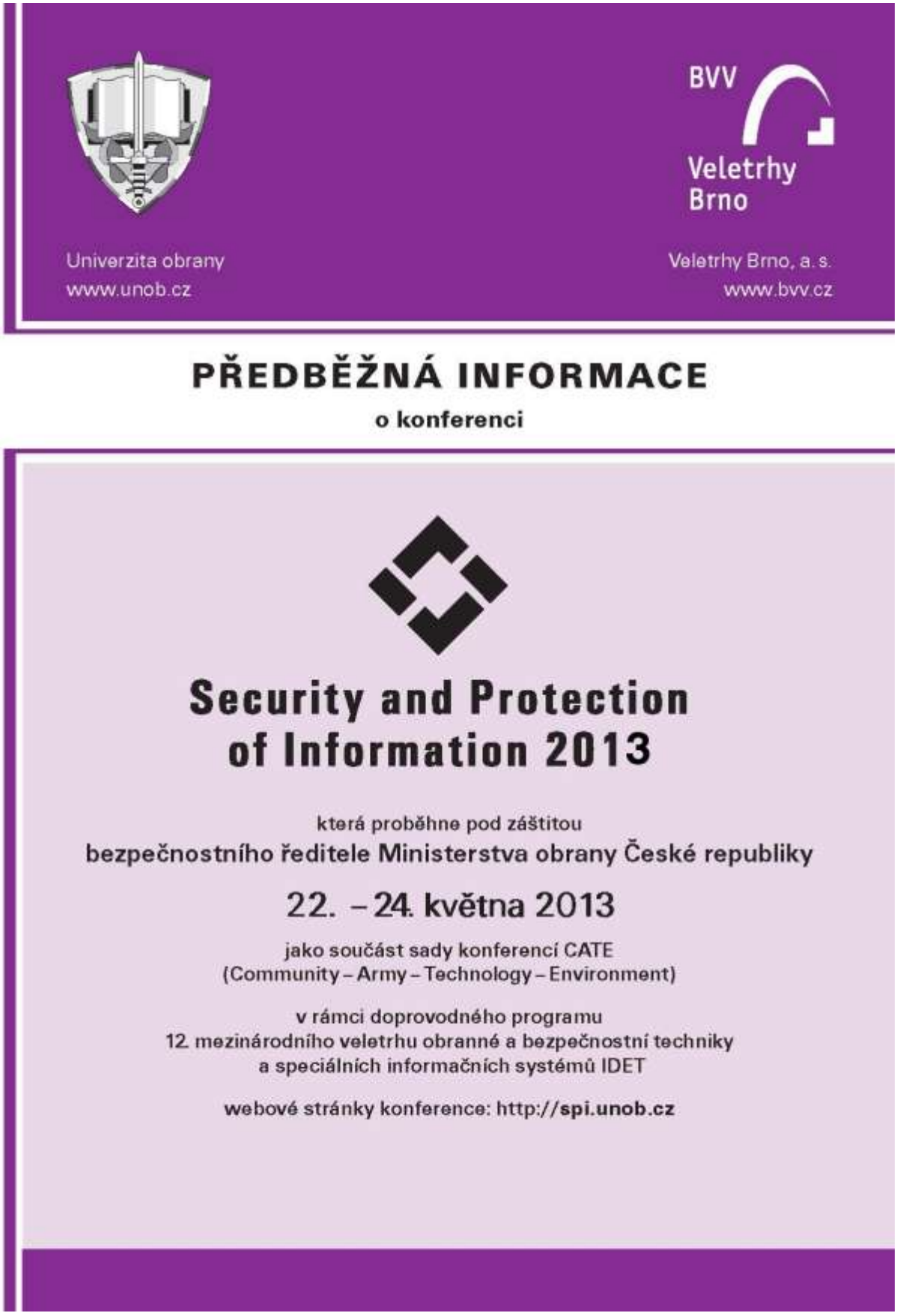
Martin Dráb poodhalí tajemství rootkitů, které získávají kontrolu nad napadeným počítačem ještě dříve, než je zaveden samotný operační systém. **Martin Klubal** předvede vytvoření botnetu z volně dostupných zdrojů, kterými se mohou stát například free hostingové servery.

Petr Subber P. upozorní na slabé zabezpečení plzeňského systému a informačních kiosků plzeňské karty. **Mjr. Mgr. Václav Písecký** následně v rámci možností zodpoví dotazy návštěvníků konference ze své pozice zástupce oddělení informační kriminality MVČR.

Podrobnější informace o jednotlivých prezentacích a registrační formulář jsou dostupné na webové stránce http://www.soom.cz/konference

Zdroj: http://www.soom.cz/konference

E. Security and Protection of Information 2013



Témata konference nabídnutá autorům

Ochrana utajovaných informací:

- bezpečnostní politiky
- vývoj a aplikace bezpečnostních standardů
- slabiny IT systémů, management rizik, řešení rizik
- management bezpečnostních oprav
- bezpečnost mobilních zařízení
- forénzní analýza výpočetních systémů a sítí
- ekonomické otázky bezpečnosti
- bezpečnost cloud computingu, bezpečnost v oblasti big data
- plánování kontinuity byznysu, obnova po havárii
- management identit, přístupu a autorizace
- prevence ztráty dat
- aplikace elektronického podpisu a PKI
- personální bezpečnost a ochrana programů
- virtualizace datových center a jejich bezpečnost

Bezpečnost počítačových sítí:

- bezpečnostní hrozby, hackerské aktivity, řešení incidentů
- bezpečnost protokolové sady TCP/IP, bezpečnost směrování
- bezpečnost VoIP, IT telefonie a WiFi sítí
- bezpečnost adresářů, elektronické pošty, DNS, a webu
- firewally, VPN, detekce a prevence průniku
- bezpečné programování a antivirové programy

Aplikovaná kryptografie:

- kryptografické aplikace
- bezpečnostní aplikace kryptografie a kryptoanalýza
- kryptografické algoritmy, jejich návrh a implementace
- modularita a opakované použití ověřených kritických komponent
- elektronický podpis
- přijatelná rizika kryptografické bezpečnosti
- standardizace a kryptografie
- legislativa související s kryptografií
- technologie posilující soukromí
- dokazatelnost bezpečnosti
- RFID – bezpečnostní a kryptografické aspekty
- další oblasti kryptografie

Bezpečnost informací ve vojenském prostředí:

- víceúrovňové bezpečnostní systémy
- bezpečnostní politiky, procedury a regulace
- bezpečné nastavení operačních a databázových systémů
- technologické otázky počítačové bezpečnosti
- bezpečnost dokumentů
- bezpečnost videokonferencí
- scénáře řešení bezpečnostních problémů, bezpečnostní vzdělávání

F. O čem jsme psali za posledních 12 měsíců

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

Crypto-World 1/2012

A.	Informace redakce, PF 2012	2
B.	Soutěž 2011 – Kompletní příběh včetně úloh, nápověd a jejich správného řešení	3-29
C.	Soutěž 2011 - Statistika soutěže, úspěšnost, řešitelé	30-31
D.	Soutěž 2011 - Ceny a loga sponzorů	31
E.	Pozvánka na SOOM Hacking & Security konferenci	32
F.	O čem jsme psali v lednu 2000 – 2011	33-34
G.	Závěrečné informace	35

Crypto-World 2/2012

A.	Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 10., Šifra „Utility“ (J.Kollár)	2 - 10
B.	Lehká kryptografie a pár slov k hackingu (V.Klíma)	11 - 24
C.	Pozvánka na SCIENCE Cafe v Hradci Králové	25
D.	O čem jsme psali v únoru 2000 – 2011	26 – 27
E.	Závěrečné informace	28

Crypto-World 3-4/2012

A.	Ceskoslovenské šifry z obdobia 2. svetovej vojny Diel 11., Šifra „Palacký“ (J.Kollár)	2 - 12
B.	Má zmysel používať autokľúč? (J.Kollár)	12 - 17
C.	Slabý generátor náhodných čísel umožňuje faktorizovať RSA moduly (O.Mikle, předmluva P.Vondruška)	18 – 21
D.	Call for Papers - Mikulášská kryptobesídka 2012	22
E.	Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška)	23
F.	O čem jsme psali v březnu 2000 – 2011	24 – 25
G.	Závěrečné informace	26

Crypto-World 5-6/2012

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

Crypto-World 7-8/2012

A. Andreas Figl – Nestor rakúskej školy kryptológie 2 – 13
B. Kryptologické perličky 1 (K.Šklíba) 14 – 24
C. Z NISTu unikl interní dokument k SHA-3 (V.Klíma) 25 - 30
D. Kniha Kryptologie, šifrování a tajná písma rozebrána (P.Vondruška) 31
E. Problematika infrastruktury veřejných klíčů (PKI), kurz Akademie CZ.NIC (P.Vondruška) 32 – 23
F. ZPRÁVA - Nechcete být odposloucháváni? (L.Stejskalová) 34
G. O čem jsme psali v létě 2000 – 2011 35 – 37
H. Závěrečné informace 38

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

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

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

Crypto-World 11-12/2012

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

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

D. Závěrečné informace

1. Sešit

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

2. Registrace / zrušení registrace

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

3. Redakce

E-zin Crypto-World

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

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Dušan Drábik	Dusan.Drabik@o2bs.com ,	
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška, jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info