Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 14, číslo 11-12/2012 **16. prosinec**

11-12/2012

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1316 registrovaných odběratelů)

Obsah :

Příloha: **Obrazová příloha** k části I. Mírka, J.: Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni
http://crypto-world.info/casop14/cast1.zip

A. SHA-3 a lehká kryptografie

RNDr. Vlastimil Klíma, nezávislý kryptolog – konzultant a KNZ s.r.o.,
v.klima@volny.cz

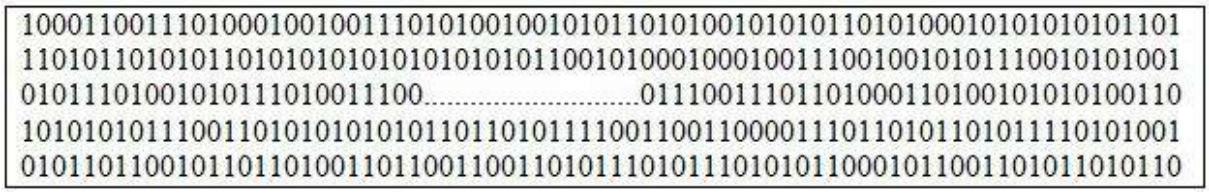
Abstrakt

Příspěvek se věnuje tématům SHA-3 a Lehké kryptografie. Lehká kryptografie (Lightweight Cryptography) je nové odvětví kryptografie, které se zabývá návrhem kryptoschémat pro velice limitovaná prostředí. Její vznik si vynutily nové technologie. Naproti tomu SHA-3 patří do skupiny obecných kryptoschémat, určených pro všechna prostředí a maximální bezpečnost. V příspěvku diskutujeme také nový pojem, a to "Kryptografie pro omezená rizika" (Limited Risc Cryptography) jako paralelu lehké kryptografie, avšak pro prostředí s omezenými riziky. Diskutujeme také návrh velmi rychlé blokové šifry pro tuto novou oblast.[1]

Klíčová slova: SHA-3, lehká kryptografie, kryptografie pro omezená rizika, Lightweight Cryptography, Limited Risc Cryptography .

1 Úvod

Kryptografické hašovací funkce jsou nejzákladnější nástroje informační bezpečnosti, protože zajišťují autentičnost a integritu digitálních dokumentů a souborů a dat, přenášených v nejrůznějších komunikačních protokolech. Proto jsou široce používány v praxi IT/IS. Kryptologové pomocí hašovací funkce realizovali v digitálním světě to, co v lidském světě znamená otisk prstu. Vynález hašovacích funkcí přinesl do té doby a úžasnou a mnohdy stále ještě nepředstavitelnou věc: každý digitální dokument, soubor, program nebo kousek přenesených dat má svůj digitální otisk, stejně jedinečný a stejně fungující jako otisk prstu u lidí.



Obr. 1: Digitální otisk.

To umožňuje se přesvědčit o neporušenosti přenesených dat i o tom (ve spojení s kryptografickými klíči), kdo je jejich původce. Dnes se jako super bezpečné používají 256bitové otisky nebo dokonce 512bitové, ale zcela běžně postačí 128bitové. Pomocí takového binárního řetězce jako vidíte na obrázku, lze identifikovat jakýkoli digitální soubor na světě. NIST garantuje, že není možné, aby někdo nalezl dva jakékoliv (krátké nebo dlouhé, smysluplné nebo nesmyslné) soubory, které by měly stejný digitální otisk. NIST dokonce garantuje, že když se změní byť jedno písmeno v knize, tak její nový digitální otisk bude naprosto náhodně odlišný od původního. To je síla kryptografie a její revoluční myšlenka digitálního otisku.

[1] Tento příspěvek byl ve zkrácené podobě určen pro konferenci MKB 2012. Tato rozšířená verze je určena širšímu okruhu čtenářů

2 SHA-3

Americký úřad pro standardy a technologie NIST oznámil 2. října t.r., že ukončil pětiletou soutěž na federální standard digitálního otisku (hašovací funkce).

Vítězem této mezinárodní soutěže (které se za Česko zúčastnil autor v týmech BMW a Edon-R a prof. Aleš Drápal z MFFUK v týmu Edon-R) se stala hašovací funkce KECCAK. Tato hašovací funkce byla navržena kryptografy z Belgie a Itálie, konkrétně těmito výzkumníky:

- Guido Bertoni (Itáliey) z firmy STMicroelectronics,
- Joan Daemen (Belgie) z firmy STMicroelectronics,
- Michaël Peeters (Belgie) z firmy NXP Semiconductors,
- Gilles Van Assche (Belgie) z firmy STMicroelectronics.

Čtenáři by mohli být překvapeni, že firmy, které velmi dobře znají jako čistě hardwarové, zaměstnávají kryptology. Je to tak, nejlepší kryptologové jsou rozebráni do tří oblastí – špičkové technologické firmy, tajné služby a akademický výzkum. Dokonce poprvé v historii tajné služby přímo přihlásily do této veřejné soutěže své kandidáty. Během pěti let se původních 64 návrhů zužovalo v druhém kole na 14, ve třetím na 5 a pak už zbyl jen vítěz. V každém kole se konala jedna mezinárodní konference a bylo odvedeno enormní množství kryptologické práce. Vše veřejně.
NIST vybral KECCAK jak oficiálně praví [1], z důvodu jeho elegantního návrhu, velké bezpečnostní rezervy, přizpůsobivosti, dobrého výkonu obecně a výborného výkonu v hardwéru.
KECCAK používá poměrně mladou „konstrukci houby", což je odlišná konstrukce, než mají nejpoužívanější hašovací funkce MD5, SHA-1 a platná rodina funkcí SHA-2. S odstupem času je stále zřejmější, že to je jeho největší výhoda, na níž se během pěti let soutěžení pozapomnělo. NIST měl obavy, že by se útoky na funkce MD5 (dokonaný) a na SHA-1 (teoretický, nedokonaný) mohly přelít i do rodiny SHA-2, což byla prapůvodní příčina vyhlášení soutěže. Teď je tedy splněn záměr, aby nový standard byl jakousi pojistkou pro tento krizový scénář. Co se nepovedlo, je rychlost, neboť všeobecná rychlost Keccaku je pouze „dobrá" jak konstatuje NIST. Takže Keccak bude zřejmě nasazován tam, kde bude rychlejší než stávající funkce z rodiny SHA-2, a to v softwaru asi vždy nebude.
Připomeňme, že NIST se „odklonil" od vyhlášených platných požadavků soutěže a uprostřed soutěže je změnil, což také veřejně (i když nepříliš hlasitě) konstatoval. Ustoupil z požadavku, že nový standard musí být podstatně rychlejší, než SHA-2. To NISTu jako jeden ze soutěžících (a spoluautor nejrychlejšího kandidáta v druhém kole) nikdy neodpustím. Trochu se u tohoto bodu zastavíme, protože je obecně zajímavý. Soutěž na hašovací funkci se dá přirovnat k soutěži na tanky. NIST požadoval, aby nový tank byl rychlejší i bezpečnější než stávající. Kdo by se odvážil přihlásit nový tank do soutěže, který nesplňuje tyto podmínky? Kupodivu takových týmů, včetně mocných průmyslových formací a včetně vítěze, bylo více. Důvod je prostý, tyto podmínky byly téměř nesplnitelné. Pouze několik týmů to dokázalo! Jak? Kde ušetřit, když pancíř musí být silnější, ale těžší tank nemůže být rychlejší? Motory (současné procesory) totiž měly všechny tanky dané a stejné! Pár týmů, které splnily zadání, použilo obrazně řečeno nový materiál, takže ochranný plášť mohl být přecejen odolnější a hmotnost se také snížila! Nový tank byl nakonec i rychlejší i bezpečnější! Jenže NIST (snad někde ve skrytu duše úřadu) chtěl použít osvědčený materiál, kterému věřil (což deklarováno nikde nebylo), a tím se zamotal do neřešitelné situace. Proto se vrátil k původnímu smyslu soutěže, tj. navrhnout nějakou alternativu pro případ kdyby byl současný standard SHA-2 prolomen a ustoupil z požadavku podstatně vyšší rychlosti. Je jasné, že kdyby ostatní týmy věděly, co vlastně NIST chce, a že má rád nějaký materiál nebo že bude ve skutečnosti

preferovat bezpečnost oproti rychlosti, tak by mohly navrhnout třeba lepší konstrukci než vítěz.
Po výběru vítěze vydal NIST závěrečnou zprávu [8], kde svůj výběr zdůvodnil. Z ní se dozvídáme, že Keccak není ani nejrychlejší, ani nejmenší (vyjádřeno "plochou křemíku"), ale má nejlepší poměr rychlosti k ploše křemíku. U našeho příměru s tankem by soutěž vyhrál tank, který není ani nejrychlejší, ani nejlevnější, ale který má nejlepší poměr rychlosti ku hmotnosti.
Podmínky soutěže i jejich nenaplnění dokladují následující oficiální dokumenty a výňatky z nich.

NIST expects SHA–3 to have a security strength that is at least as good as the hash algorithms currently specified in FIPS 180–2, and that this security strength will be achieved with significantly improved efficiency. NIST

Obr.2: Zahájení soutěže - podmínky na algoritmy, [6], str. 62213.

Performance was also important in choosing the finalists. In FRN-Nov07, NIST stated that it expected SHA-3 to have a security strength that is at least as good as the hash algorithms currently specified in FIPS 180-2[2], and that this security strength would be achieved with significantly improved efficiency. However, during the analysis of the second round candidates, it became apparent that significant improvement in efficiency while fulfilling the security requirements was not easily attainable. NIST chose finalists that could be implemented on as

Obr.3: Ze zprávy k druhému kolu (výběr 5 finalistů), [7], str. 5.

b. None of the five finalists is the best for every application, and none offers really compelling improvements over the SHA-2 algorithms.

Obr.4: Ze zprávy k třetímu kolu (výběr vítěze), [8], str. 6.

Contrary to the fears leading up to the SHA-3 Competition, SHA-2 has held up well in the face of continued cryptanalysis. The new SHA-3 will need to compete with an existing algorithm (SHA-2) that also offers very strong security and performance. Keccak was chosen, not just for its very strong overall security and performance, but because it offers exceptional performance in areas where SHA-2 does not, and because it relies on completely different architectural principles from those of SHA-2 for its security.

Obr.5: Ze zprávy k třetímu kolu (výběr vítěze), [8], str. 59.

Nyní, po skončení soutěže, je důležité, že NIST nové SHA-3 věří. Také obavy o bezpečnost SHA-2, panující před soutěží, se nenaplnily. Dokonce se ještě nepodařilo prakticky prolomit SHA-1! To je dobrá zpráva pro nás všechny, neboť průmysl IT se bez kvalitní kryptografie neobejde. **Přínosem soutěže bezesporu je, že dnes může průmysl IT na poli hašovacích**

funkcí být v klidu, neboť máme ve skutečnosti dva standardy SHA-2 a SHA-3 a není pravděpodobné, že by se někomu podařilo prolomit jak SHA-2, tak SHA-3. Vývojáři si dnes mohou vybrat ten algoritmus z rodin SHA-2 a SHA-3, který bude pro ně rychlejší, bezpečnější, méně náročný na paměť, výkon, apod. Nemusí přitom pospíchat, protože SHA-2 by mohla být v platnosti ještě cca 10 let a možná i déle.

Vítěz soutěže je vybrán, teď už se jen čeká na poslední etapu, a to je komentáře k vítězi, a na administrativní vydání nového standardu snad v příštím roce. Podrobné výkonnostní výsledky Keccaku v SW a HW je možné studovat na [2] a [3]. Zde pro přehlednost uvedeme zjednodušené výsledky. V první tabulce vidíme výsledky na 64-bitových procesorech, a to ve spotřebě hašovací funkce v cyklech na bajt. Takže pokud známe taktovací frekvenci daného čipu nebo procesoru, můžeme si snadno vypočítat rychlost hašování v bajtech. Uvádíme spotřebu cyklů na bajt jen pro dlouhé zprávy, pro krátké zprávy je toto číslo zavádějící, protože tato funkce musí v každém případě udělat jakýsi stejně náročný "rozjezd", nezávisle na tom, jestli má zpráva 1 bajt nebo 1 terabajt. Čas tohoto konstantního "rozjezdu" se u dlouhých zpráv rozpustí, ale u krátkých nikoli. Pro krátké zprávy jsou měření rychlosti například v [4]. V tabulce 1 vidíme, že u více než poloviny 64bitových procesorů není Keccak-256 rychlejší než SHA-256 a současně Keccak-512 rychlejší než SHA-512. Pro 32bitové procesory to teprve není žádná sláva, ale na druhé straně to není zase nějak devastující. U HW realizací se porovnání s SHA-256 nebo SHA-512 v tabulce neuvádí, ale NIST tvrdí, že Keccak je tam nejvýhodnější (ale jen v ukazateli rychlost ku ploše). Ostatně srovnání v HW (ASIC i FPGA) lze nalézt jak v závěrečné zprávě [8], tak v několika citovaných zdrojích, o něž se opírá.

Procesor	Keccak-256 (c/b)	SHA-256 (c/b)	Keccak-512 (c/b)	SHA-512 (c/b)
AMD Athlon 64 X2	9,94	14.88	12,28	9.93
AMD Phenom 9550	9,90	15.06	12,23	9.92
AMD Phenom II X4 955	9,96	15.04	12,30	11.83
AMD Phenom II X6 1090T	9,89	15.05	12,22	11.51
HP Itanium II	4,78	20.47	5,91	9.30
IBM POWER4	15,94	25.34	19,69	15.37
IBM POWER5	12,88	22.19	15,92	13.52
IBM PowerPC G5 970	14,83	22.28	18,32	13.32
ICT Loongson-2 V0.3	18,83	35.03	23,27	24.27
Intel Core 2 Duo	9,63	15.34	11,90	11.73
Intel Core 2 Duo E4600	9,62	15.55	11,89	10.27
Intel Core 2 Duo E8400	9,65	15.28	11,92	10.22
Intel Core 2 Quad Q9550	9,63	15.26	11,90	10.26
Intel Core i5 750	8,37	14.08	10,33	10.61
Intel Core i5 M 520	8,28	13.90	10,23	10.48
Intel Core i7 920	9,97	16.94	12,32	11.45
Intel Xeon E5420	9,63	15.16	11,90	11.79
Intel Xeon E5530	10,00	16.92	12,35	11.82
Sun UltraSPARC IIIi	28,87	27.71	35,66	20.50

Procesor	Keccak-256 (c/b)	SHA-256 (c/b)	Keccak-512 (c/b)	SHA-512 (c/b)
Sun UltraSPARC T1	62,45	75.00	77,14	131.26

Tab.1: Průchodnost Keccaku na různých 64bitových procesorech

Procesor	Keccak-256 (c/b)	SHA-256 (c/b)	Keccak-512 (c/b)	SHA-512 (c/b)
AMD Athlon	28,93	19,53	35,74	70,65
Atmel AT91RM9200	87,62	47,37	108,24	122,51
Freescale i.MX515	47,91	22,31	59,18	89,50
Intel Pentium 3	31,13	24,80	38,46	67,47
Intel Pentium 4	37,25	35,88	46,01	37,44
Intel Pentium M	25,77	21,62	31,83	29,96
Luminary Micro LM3S811	78,62	40,64	97,12	172,77
Motorola PowerPC 750CXe	35,67	21,08	44,07	54,38
Motorola PowerPC G4 7410	35,60	21,17	43,97	54,10
Motorola PowerPC G4 7447a	40,07	16,59	49,50	44,99
TI OMAP 2420	74,19	47,11	91,64	117,95
TI AR7 (4KEc)	113,01	84,00	139,60	140,48

Tab.2: Průchodnost Keccaku na různých 32bitových procesorech

Hlavní autor realizace	Technologie	Syntéza	Plocha (kGE)	Kmitočet (MHz)	Rychlost (Gbit/s)
Sugawara	STM 90nm	Gate level	55.9	1030	44
Sugawara	STM 90nm	Gate level	26.5	553	24
Henzen	UMC 90nm	Place and route	50.0	949	40
Henzen	UMC 90nm	Place and route	27.5	149	6
AIST	STM 90nm	Gate level	50.6	781	33
AIST	STM 90nm	Gate level	33.6	541	23
AIST	STM 90nm	Gate level	29.5	355	15
Tillich	UMC 0.18µm	Gate level	56.3	488	20
Tillich	UMC 0.18µm	Place and route	56.7	267	11
Guo	UMC 130nm	Place and route	47.4	377	15
Guo	UMC 130nm	Place and route	34.9	161	7
Tým Keccaku	STM 130nm	Gate level	48.0	526	22
Tým Keccaku	STM 130nm	Gate level	9.3	200	39 Mbit/s
Kavun	130nm	Gate level	20.0	100 kHz	85 kbit/s

Tab.3: Průchodnost Keccaku v různých realizacích ASIC

Hlavní autor realizace	Typ	Plocha	Kmitočet (MHz)	Rychlost (Mbit/s)

Hlavní autor realizace	Typ	Plocha	Kmitočet (MHz)	Rychlost (Mbit/s)
Strömbergson	Cyclone III	2670 reg., 5842 LE	123	7000
Strömbergson	Cyclone III	242 reg., 1769 LE	85	22
Tým Keccaku	Cyclone III	2670 reg., 5770 LE	145	6100
Tým Keccaku	Cyclone III	242 reg., 1570 LE	183	39
Strömbergson	Spartan 3A	2780 reg., 3393 slices	85	4800
Gai	Spartan III	3339 CLB	83	3161
Gai	Stratix III	4458 ALUT	296	13000
Strömbergson	Stratix III	2670 reg., 4550 ALUT	176	10000
Tým Keccaku	Stratix III	2641 reg., 4684 ALUT	206	8700
Tým Keccaku	Stratix III	242 reg., 855 ALUT	359	70
Strömbergson	Stratix III	242 reg., 1026 ALUT	133	35
Gai et al.	Virtex V	1229 CLB	238	10000
AIST	Virtex V	2666 reg., 1433 slices	205	8397
Gai et al.	Virtex V	1412 CLB	195	7840
Strömbergson	Virtex V	2669 reg., 1483 slices	118	6700
Guo et al.	Virtex V	1556 slices	154	6570
Baldwin	Virtex V	1117 slices	189	5895
Tým Keccaku	Virtex V	2640 reg., 1330 slices	122	5200
Tým Keccaku	Virtex V	244 reg., 448 slices	265	5

Tab.4: Průchodnost Keccaku v různých realizacích FPGA

Technické detaily, kompletní popis, celou dokumentaci, testovací příklady a množství realizací v různých jazycích a spoustu dalších informací naleznete na webu Keccaku [5]. Vše je veřejně dostupné, bez poplatků a často jako freeware nebo s podobnou licencí. Na závěr připomeňme ještě pěknou vlastnost přizpůsobivosti Keccaku. Jeho varianty (mimo standard) lze totiž s úspěchem využít v embedded systémech, také o tom jsou další informace v [5].

3 Keccak

Varianty Keccaku

Keccak má poměrně suchý a špatně čitelný popis. Navíc jsou dvě verze Keccaku, oficiální, která má čtyři požadované varianty (SHA-3-n, kde n = 224, 256, 384 a 512) podle požadované délky výstupního kódu n =224, 256, 384 a 512 bitů, a verze neoficiální (teoreticky slabší), která se skládá z jedné funkce, jejíž 1600bitový výstup se prostě krátí na požadovanou délku hašovacího kódu n bitů. Neoficiální verze je sice jednodušší na programování a výklad, ale o něco pomalejší než oficiální varianty a nemá žádnou garanci ani podporu NIST, protože není standardizovaná.

Parametry

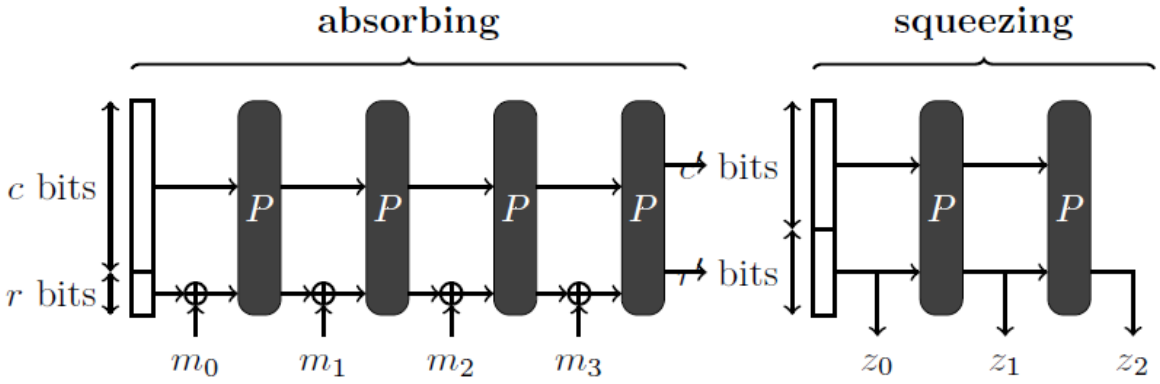
Kousněme do kyselého jablka popisu parametrů. Keccak pracuje s jednou kompresní funkcí f, která má 1600 bitový vstup a stejně tak dlouhý výstup, proto se jí také říká permutace. Hodnota 1600 je rozdělena na bitovou rychlost r a na kapacitu c: 1600 = r + c. Velikost r je důležitá v tom, že hašovaná zpráva se zpracovává po blocích délky r bitů, odkud také pramení

název bitová rychlost. Číslo r zároveň říká, kolik bitů se nakonec, po zpracování celé zprávy, může odebrat z výstupu funkce f jako výsledek hašování. Vývojáři Keccaku definovali jednu funkci f, ale pro různé varianty SHA-3-n (kde n = 224, 256, 384 a 512) se definuje jiné r. Definuje se:
1. SHA3-224: r = 1152; c = 448;
2. SHA3-256: r = 1088; c = 512;
3. SHA3-384: r = 832; c = 768;
4. SHA3-512: r = 576; c = 1024;

Pro neoficiální verzi se použije poslední varianta parametrů r = 576; c = 1024 a z výsledných 576 bitů se prostě jen odebere prvních n bitů pro kde n = 224, 256, 384 a 512. Nejrychlejší oficiální verze je pochopitelně SHA3-224, protože během jedné funkce f zpracuje 1152 bitů zprávy. Nejpomalejší je SHA3-512, zpracovávající zprávu po blocích o délce 576 bitů (72 bajtů).

Princip houby

Zůstaňme teď už jen u oficiální verze. Na následujícím obrázku vidíme, jak se zpráva postupně zpracovává po blocích délky r bitů.



Obr.5: Princip houby (sponge construction)

Doplňování zprávy

D1oplňování zprávy do celistvého počtu r-bitových bloků se dělá jinak, než jsme byli dosud zvyklí. Je definováno symbolicky jako "10*1", což znamená, že povinně se za zprávu doplní bit 1 a potom nejmenší počet nulových bitů tak, aby závěrečný bit 1 dokončoval úplný blok o r-bitech. Nejméně se doplní dva bity a nejvíce r+1 bitů.

Výstup hašovací funkce

Z obrázku je vidět, že jakmile se zpracuje poslední blok zprávy s doplněním, z funkce P (v Keccaku je to permutace f) se odebere n bitů (kde n = 224, 256, 384 a 512), takže fáze vymačkávání (squeezing) vlastně odpadá. Nyní zbývá dodefinovat funkci f. Prvopočáteční stav funkce f je 1600 nulových bitů.

Funkce f

Funkce f, jak už víme, nezávisí na žádných parametrech, a autoři ji oprávněně považují za nejdůležitější (a nejmilejší, stejně jako autor) část Keccaku. Jediná věc, která by se dala uvažovat za parametr, je počet rund funkce f, který je ale stanoven jako konstanta na 24.

Počet 1600 bitů vznikl tak, že je to 25 slov o 64 bitech. To je proto, že se pracuje se slovy o délce 64 bitů, stejně jako to dělají moderní "velké" procesory. Takže máme 25 slov, které jsou srovnány do matice 5x5. Pokud převezmeme popis návrhářů Keccaku, máme tady stavové pole a[x][y], které obsahuje 5x5 slov, kde x a y jsou indexy od nuly do čtyř, přičemž pokud se v nich objevují výrazy, jsou počítány vždy modulo 5. Pokud budeme dělat bitovou rotaci

64bitového slova a[x][y], hodí se nám třetí index, z, který označuje bity 64bitového slova a[x][y]. Třetí index má hodnotu 0 až 63 a výrazy v něm se počítají modulo 64. Stavové pole můžeme tedy zapsat také jako pole bitů a[x][y][z]. Slovo a[x][y] rotované o jeden bit doleva můžeme symbolicky zapsat jako b[x][y][z] = a[x][y][z-1]. K popisu funkce f už nepotřebujeme nic jiného. Autoři funkci f popisují matematicky tak, jak ukazuje obrázek 6. Poznamenejme, že znaménko plus zde znamená binární sčítání, tj. operaci XOR nikoli ADD.

$$R = \iota \circ \chi \circ \pi \circ \rho \circ \theta, \text{ with}$$

$$\theta: \quad a[x][y][z] \leftarrow a[x][y][z] + \sum_{y'=0}^{4} a[x-1][y'][z] + \sum_{y'=0}^{4} a[x+1][y'][z-1],$$

$$\rho: \quad a[x][y][z] \leftarrow a[x][y][z-(t+1)(t+2)/2],$$

$$\text{with } t \text{ satisfying } 0 \le t < 24 \text{ and } \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}^t \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \text{ in } \mathrm{GF}(5)^{2\times 2},$$

$$\text{or } t = -1 \text{ if } x = y = 0,$$

$$\pi: \quad a[x][y] \leftarrow a[x'][y'], \text{ with } \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix},$$

$$\chi: \quad a[x] \leftarrow a[x] + (a[x+1]+1)a[x+2],$$

$$\iota: \quad a \leftarrow a + \mathrm{RC}[i_r].$$

Obr.6: Funkce f - jádro Keccaku

Na obrázku 6 je popsána jedna runda (R) funkce f, ta jich má 24.

Operace theta

První operace theta je na první pohled složitá operace, ve skutečnosti je to velice úsporná realizace lineární transformace stavového pole. Vzorec říká, že slovo na pozici [x][y] aktualizujeme tak, že na něj načteme slova ze sloupce nalevo a ze sloupce napravo (ty předtím ještě rotujeme o jeden bit doleva). "Načtení" chápeme binárně, jak jsme už poznamenali. Operace theta tedy prostě lineárně promíchá stavové bity. Jistě bychom se mohli ptát, proč zrovna takto, ale uvědomme si, že návrháři jsou z firem, které navrhují čipy, a operace theta je v hardwaru velice úsporná, stejně tak je rotace o jeden bit hardwarově skousnutelná, neboť jen jeden vodič překřižuje ostatní (nejvyšší bit, když se dostává na nejnižší místo). Operaci theta také můžeme realizovat tak, že v poli 5x5 slov vypočteme sloupcové součty a uložíme do pěti proměnných (je to levá část přídavku z rovnice pro ró), z nich vytvoříme rotací o jeden bit doleva dalších pět proměnných (to je pravá část přídavku z rovnice pro ró), poté sečteme vždy jednu proměnnou z první pětice a jednu z druhé pětice a máme celý „přídavek“ z rovnice pro ró. Tímto přídavkem modifikujeme původní slova stavového pole. Zajímavé je, že máme pouze pět přídavků (pro x = 0, x = 1, x= 2, x = 3, x= 4), nikoli 25, neboť jak je vidět z rovnice pro ró, přídavky jsou nezávislé na indexu y, tj. jsou pro všechna slova ve sloupci y stejné. Celou transformaci tak tvoří 5x součet (XOR) pěti slov a 5x rotace slova doleva o jeden bit, 5x součet dvou slov, 25x součet dvou slov.

Operace ró

Druhá operace ró neznamená nic jiného než rotaci každého 64bitového stavového slova o určitý počet bitů doleva. Tento posun je definován složitě vzorci, ale v hardwéru i softwéru bude zcela jistě realizován tabulkou o 25 položkách, přímo definující bitovou rotaci, viz obrázek 7.

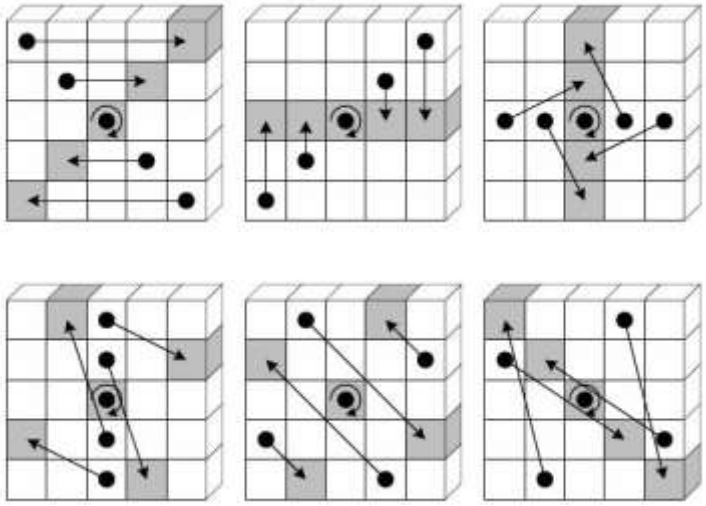
	$x=3$	$x=4$	$x=0$	$x=1$	$x=2$
$y=2$	153	231	3	10	171
$y=1$	55	276	36	300	6
$y=0$	28	91	0	1	190
$y=4$	120	78	210	66	253
$y=3$	21	136	105	45	15

Obr.7: Bitová rotace.

Bitové posuny, definované v tabulce na obr. 7 pochopitelně znormalizujeme v našem případě modulo 64. Celá transformace je tak tvořena 25 (resp. 24) rotacemi slova doleva o specifikovaný počet bitů.

Operace pí

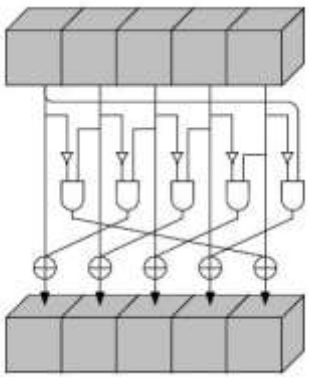
Operace pí je pouhá permutace slov ve stavovém poli. Graficky to vypadá efektně na obrázku 8.



Obr.8: Permutace slov ve stavovém poli.

Operace chí

Operace chí je jediná nelineární operace a schématicky je pro každý řádek stavové matice znázorněna na obrázku 9.



Obr.9: Operace chí na řádku stavové matice.

Ve vzorci pro chí je vynechán index y, neboť výpočet nového stavu stavové matice je stejný pro každý řádek, takže si tam index y můžeme u každého a[x] klidně připsat.

Operace jota

Operace jota přixoruje na stavovou matici konstantní matici typu 5x5, lišící se rundu od rundy. Tato matice je však redukována na jeden nenulový prvek, a to ten s indexy [0][0]. Přičtení dané rundovní konstanty se tedy děje jen prostým přičtením definované konstanty (jiné v každé rundě) na slovo a[0][0].

Na závěr popisu

Vidíme, že operace Keccaku jsou jednoduché, složitosti se dosahuje tím, že je jich mnoho, a to poměrně vysokým počtem rund (24). Všimli jsme si, že funkce f je realizována tak, že jeden bit výstupu připadá pouze 24 bitových operací typu AND a množství bitových operací typu XOR, aplikovaných na bity vstupu. To se autorovi zdá velice velice málo a mělo by to podnítit výzkum v této oblasti. Ideální by bylo zjistit preimage k nulovému výstupu Keccaku, viz dále.

(1. část přednášky pro MKB, pokračování příště)

References

[1] Domácí stránka soutěže SHA-3: www.nist.gov/hash-competition

[2] Výkon v SW: http://keccak.noekeon.org/sw_performance.html

[3] Výkon v HW: http://keccak.noekeon.org/hw_performance.html

[4] Obsáhlá měření: http://ehash.iaik.tugraz.at/wiki/SHA-3_Hardware_Implementations a http://bench.cr.yp.to/results-sha3.html

[5] Domácí stránka Keccaku: http://keccak.noekeon.org/

[6] "Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family", Federal Register/ Vol. 72, No. 212 / Friday, November 2, 2007 / Notices 62212, http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf, str. 62213.

[7] "Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition, str. 5", NIST Interagency Report 7764, http://csrc.nist.gov/publications/nistir/ir7764/nistir-7764.pdf , str. 5.

[8] NISTIR 7896, Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition, http://dx.doi.org/10.6028/NIST.IR.7896 , str. 6.

Poznámka: V textu použity též výňatky z článků autora ve Sdělovací technice, č. 12/2012 a 11/2011.

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

Jakub MÍRKA, SOA Plzeň, mirka@soaplzen.cz

Článek, který si budete moci přečíst na následujících řádkách, byl v tomto roce již uveřejněn v letošním vydání Západočeských archivů, periodiku vydávaném Státním oblastním archivem v Plzni. Vzhledem k tomu, že Západočeské archivy jsou specializovaným archivním časopisem, který není dostupný v běžné obchodní distribuci, dohodli jsme se s Pavlem Vondruškou na uveřejnění článku také na stránkách Crypto-Worldu, který je pro zájemce o historii kryptologie dostupnější. Vzhledem k rozsahu článku bude jeho text rozdělen do tří částí, které vyjdou ve třech po sobě následujících číslech Crypto-Worldu. Text byl oproti prvnímu vydání jen nepatrně korigován a především byla o něco málo zkrácena jeho teoretická část pojednávající o šifrovacích systémech.

Obrazové přílohy, které jsou umístěny přímo v textu, lze nalézt v lepší kvalitě v příloze Crypto-Worldu (Obrazová příloha k části I. http://crypto-world.info/casop14/cast1.zip). Ve všech případech jde o kopie archiválií uložených ve Státním oblastním archivu v Plzni.

Cílem článku je seznámit veřejnost s raně novověkou šifrovanou korespondencí[1] nacházející se ve fondech šlechtických rodinných archivů SOA v Plzni, které jsou ve správě 5. oddělení sídlícího v Kláštěře u Nepomuka. Lze říci, že právě tyto fondy jsou v rámci sítě státních oblastních archivů téměř výlučným zdrojem tohoto typu korespondence. Šifrování bylo v minulosti užíváno v naprosté většině případů u zpráv mimořádného významu, zejména pak ve sféře vojenské a diplomatické. Šifrované dopisy tedy nacházíme nejčastěji v archivech ústředních politických a vojenských úřadů, jejichž fondy také bývají obvykle uloženy v centrálních národních nebo státních archivech, a dále v písemných pozůstalostech významných představitelů těchto úřadů. V období raného novověku totiž nebyla dána pevná hranice mezi archivem úřadu a osobním archivem jeho vrcholného představitele, a proto jsou písemnosti čistě úředního rázu a mnohdy velkého státního významu často uloženy právě v písemných pozůstalostech jednotlivých šlechticů v rámci rodinných archivů.

[1] Pod souhrnný název „šifrovaná korespondence“ zahrnuji i dobové šifrovací klíče. Ty sice nelze považovat přímo za korespondenci, ale jejich vznik je podmíněn tím, že je někdo hodlá užívat pro šifrování a dešifrování zpráv a mezi korespondencí také bývají v archivech obvykle uloženy. Podobně do šifrované korespondence zahrnuji i kódy. Pro užívání kódů se v současnosti užívá spíše termínu kódování. V raném novověku však byly kódy často kombinovány se substitučními šiframi a do určité míry je možné je považovat za jistou variantu substituce. Důsledné odlišení šifrování a kódování tedy není pro účely tohoto článku možné.

Podobně je tomu i v případě záležitostí vojenských. Ještě v průběhu třicetileté války, ze které pochází patrně největší množství raně novověké šifrované korespondence uložené v českých archivech, fungovala armáda spíše na podnikatelské bázi.[2] Jednotlivé pluky byly najímány soukromníky, většinou přímo samotnými vojevůdci pocházejícími zpravidla z významných šlechtických rodů, kteří opět všechnu svou korespondenci s panovníkem, centrálními úřady, dalšími vojevůdci, zpravodaji aj. obvykle ukládali do svých vlastních archivů. To platí nejen o majitelích jednotlivých pluků, ale i o císařských vojevůdcích, členech válečné rady a jiných vojenských činitelích.

Samozřejmě ne všechna šifrovaná korespondence musí být vojenského nebo diplomatického rázu a ne vždy v ní musí být obsaženy v danou chvíli zásadní informace pro vývoj války nebo státu. Jsou známy i zcela soukromé dopisy psané šifrovanou abecedou, které sice také většinou obsahují důležité informace, ale převážně pouze pro velmi úzký okruh osob a bez významu pro veřejnou sféru.[3]

Ovšem ani ve fondech šlechtických rodinných archivů se nenachází výrazně velké množství šifrovaných dopisů. Významnější soubory šifrované korespondence se v SOA v Plzni vyskytují pouze ve dvou fondech (Rodinný archiv Trauttmansdorffů a Rodinný archiv Windischgrätzů), a to v písemných pozůstalostech těch členů rodu, kteří zastávali důležité dvorské úřady. Ovšem i v jejich písemných pozůstalostech tvoří šifrované dopisy jen malé procento, nebo spíše promile, veškeré korespondence.[4] Přitom je však nutné říci, že v některých fondech šlechtických rodinných archivů uložených v jiných státních oblastních archivech se nachází výrazně větší množství šifrované korespondence. Jde především o fondy obsahující písemné pozůstalosti významných vojevůdců třicetileté války.[5] Ale i zde platí, že šifrovány byly zejména dopisy obsahující informace nejvyššího významu a naprostá většina korespondence šifrována nebyla.

V tomto článku si autor neklade za cíl pouze přiblížit čtenáři šifrovanou korespondenci uloženou ve fondech SOA v Plzni. Zároveň se pokouší na jejím příkladě alespoň částečně zodpovědět otázky, jaké způsoby šifrování byly v příslušné době užívány a v jakém prostředí, jaký typ zpráv byl nejčastěji šifrován a jaká byla míra bezpečnosti jejich utajení. Na některých případech bude také ukázáno, jakým způsobem probíhalo šifrování a dešifrování dopisů.

---

[2] K tomuto způsobu fungování armády více viz např. MAŤA, Petr. *Svět české aristokracie (1500–1700)*. Praha : Nakladatelství Lidové noviny 2004, s. 443.

[3] Nelze vyloučit ani to, že šifrování mohlo být užíváno i v úřední korespondenci nižších regionálních úřadů, ale patrně pouze v malé míře a autorovi článku není dosud žádný takový případ znám. Šifrované dopisy se tedy ve státních oblastních a okresních archivech samozřejmě mohou nacházet i v jiných fondech, ale pravděpodobně půjde pouze o nepříliš četné jednotlivosti.

[4] Zajímavé je např. Roubíkovo vyčíslení poměru mezi šifrovanou a nešifrovanou korespondencí ve vojenské registratuře Albrechta z Valdštejna. Mezi cca 25 000 dopisů mu bylo známo jen 65 šifrovaných. Nutno však podotknout, že Roubík předpokládá, že se nedochovaly všechny šifrované dopisy. 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.

[5] Větší soubory šifrované korespondence se nacházejí např. ve fondech Historická sbírka Clam–Gallasů, Frýdlant (SOA v Litoměřicích, pobočka Děčín – Podmokly) a RA Piccolominiů, Náchod (SOA v Zámrsku).

Pouze letmo bude dotknuto téma luštění raně novověkých šifer, které nelze pro jeho složitost do článku komplexněji zahrnout a které by si zasloužilo samostatné zpracování.

Ke zkoumání výše uvedených otázek byly pro srovnání využity i některé fondy z jiných státních oblastních archivů.[6] U těchto fondů však nešlo o systematické vyhledávání. V nich uložená korespondence byla zkoumána pouze výběrově a komplexnější zpracování ji teprve čeká. Skutečnost, že jsou dopisy psané šifrovou abecedou, bývá totiž v archivních pomůckách uvedena jen zřídka, a proto je vyhledávání šifer časově náročná práce. Zároveň není vyloučeno, že šifrovanou korespondenci mohou obsahovat i fondy dosud nezpracované. Z toho důvodu lze očekávat další nálezy i ve fondech SOA v Plzni, i když se nedá předpokládat, že půjde o velké množství archiválií. Proto si autor neklade za cíl v článku komplexně řešit výše uvedené otázky. Jde spíše o jejich načrtnutí a předložení možných řešení a odpovědí. Ty však bude možné potvrdit, korigovat či vyvrátit až po systematičtějším studiu většího množství tohoto typu pramenů i v jiných archivech. Předmětem článku není samotný obsah šifrovaných zpráv. V několika případech však byla učiněna výjimka sloužící k ilustraci toho, jak závažná sdělení byla v mnohých případech pomocí šifrování utajována.

Vzhledem k atraktivitě tématu bylo o šifrování napsáno mnoho prací, které není možné uvést vyčerpávajícím způsobem. Zmíněny proto budou alespoň ty nejvýznamnější. Větší pozornost bude věnována článkům a publikacím českých autorů, vycházejícím z našeho prostředí, a pracím vztahujícím se ke střední Evropě.

Publikace o kryptologii vycházely již v době raného novověku. Vesměs nešlo o práce historické, ale teoretické, i když obsahují také pasáže věnované starším šifrovacím systémům. Tyto práce tvořili většinou vynikající učenci a kryptologové své doby. Zabývali se v nich především základními principy a zdokonalováním stávajících šifrovacích systémů, vynalézáním nových a někdy také luštěním šifer.[7] Novější literaturu o historii kryptologie lze velmi zhruba rozdělit do dvou kategorií. Do první patří knihy kryptologů a matematiků zabývajících se šifrovacími systémy minulosti. Jejich zájem je přitom soustředěn zejména na vývoj kryptologie od nejstarších dob až po současnost a na matematické popsání jednotlivých šifrovacích systémů, případně na možné způsoby jejich luštění. Jejich práce přitom bývají často psány z velké části matematickým jazykem, který je asi pro většinu humanitně vzdělaných historiků a archivářů obtížně srozumitelný. Ovšem i v této první kategorii nalezneme díla, která neobsahují žádné matematické vzorce a jsou lehce pochopitelná i pro laiky. Jde zejména o popularizační knihy o kryptologii pro širokou veřejnost. I ty jsou však obvykle psány vynikajícími vědci nebo popularizátory vědy a absence vzorců jim rozhodně

[6] Korespondence z jiných archivů byla vybírána z převážné části na základě údajů uvedených v edici ČECHOVÁ, Gabriela – JANÁČEK, Josef – KOČÍ, Josef – POLIŠENSKÝ, Josef (edd). *Documenta Bohemica belli tricennale illustrantia, Tomus I–VII*. Praha : Academia 1971–1981. Jednotlivé fondy a archiválie budou uvedeny vždy u konkrétních příkladů.

[7] Komentovaný přehled nejvýznamnějších prací z doby pozdního středověku a raného novověku viz např. VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha : Albatros 2006, s. 210–237.

neubírá na odbornosti. Práce tohoto druhu také obsahují mnoho zajímavých případů z minulosti, většinou ale z románské a anglosaské kulturní oblasti.[8]

Odlišnou skupinou jsou práce psané historiky a archiváři. Některé z nich se šifrováním zabývají jen okrajově. Jejich autoři se většinou zaměřují na obsah vzájemné korespondence dvou významných osob a jejímu šifrování věnují často jen kratičkou část. Záleží především na tom, jak velké množství dopisů bylo šifrováno, a také, jak velký význam této skutečnosti přikládal sám autor.[9] I v této kategorii ale nalezneme práce, v nichž je šifrování ústředním tématem.[10] Mezi nimi si samostatnou zmínku zaslouží dvě knihy Aloyse Meystera, zabývající se počátky moderní kryptologie a šifrováním v papežské kanceláři do konce 16. století,[11] a dva články Hildegardy Ernst o šifrách užívaných při diplomatickém styku říšské kanceláře v letech 1635–1642, které poskytují velké množství poznatků do značné míry korespondujících se závěry tohoto článku, pro nějž byly využity jako srovnávací materiál.[12]

Česká historiografie se tomuto tématu zatím příliš nevěnovala, ale i u nás můžeme nalézt několik prací, zabývajících se popisem nebo luštěním souborů raně novověké šifrované korespondence, jejichž autory jsou nejčastěji archiváři.[13] Nejvíce se u nás tímto tématem

---

[8] Např. KAHN, David. *The Codebreakers. The Story of Secret Writing*. New York: Macmillan 1967; SINGH, Simon. *Kniha kódů a šifer.* Praha : Dokořán a Argo 2003; JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti.* Praha : Naše vojsko, 1994; VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma.* Praha : Albatros 2006.

[9] Např. EDELMAYER, Friedrich (ed.). *Die Korrespondenz der Kaiser mit ihren Gesandten in Spanien. Band 1. Briefwechsel 1563–1565.* Oldenbourg : Verlag für Geschichte und Politik 1997; VERŽOVSKIJ, Fedor. *Dve kandidatury na polskij prestol Vilgelma iz Rozenberga i ercgercoga Ferdinanda 1574–1575 po neizdannym istočnikam.* Varšava : Tipografija K. Kovalevskago 1889; PRIBRAM, Alfred Francis (edd.). *Privatbriefe Kaiser Leopold I. an den Grafen F. E. Pötting 1662–1673.* Wien : Carl Gerold´s Sohn 1903.

[10] Např. BISCHOFF, Bernhard. Übersicht über die nichtdiplomatischen Geheimschriften des Mittelalters. *Mitteilungen des Instituts für österreichische Geschichtsforschung*, 62, 1954, . 1–27; GERLICH, Wilhelm. Die Entzifferung von historischen Geheimschrifetn. *Mitteilungen des Österreichischen Staatsarchivs*, 1, 1992, s. 445–469; HÜTTENHAIN, Erich. *Die Geheimschriften des Fürstbistums Münster unter Christoph Bernhard von Galen 1650–1678.* Münster : Aschendorff 1974; STIX, Franz. Geheimschriftenkunde als Hilfswissenschaft. *Mitteilungen des Instituts für österreichische Geschichtsforschung*, Erg.–Bd. 14, 1939, s. 453–459; TÝŽ. Zur Geschichte und Organisation der Wiener Geheimen Ziffernkanzlei von ihren Anfängen bis zum Jahre 1848. *Mitteilungen des Österreichischen Instituts für Geschichtsforschung* 51, 1937, s. 131–160.

[11] MEYSTER, Aloys. *Die Anfänge der modernen diplomatischen Geheimschrift.* Paderborn : Schöningh Verlag 1902; Týž. *Die Geheimschrift im Dienste der päpstlichen Kurie. Von ihren Anfängen bis zum des XI. Jahrhunderts.* Paderborn : Schöningh Verlag 1906.

[12] ERNST, Hildegard. Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel, 1635–1642. *Mitteilungen des Österreichischen Staatsarchivs,* 42, 1992, s. 102–127; TÁŽ. Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel, 1635–1642. Teil II. *Mitteilungen des Österreichischen Staatsarchivs,* 45, 1997, s. 207–247. Tyto práce jsou cenné mimo jiné tím, že Hildegard Ernst se zabývala i obsahem dopisů a také listovní praxí říšské kanceláře. Jejím původním tématem byla totiž samotná korespondence a jejím šifrováním se zabývala až následně. ERNST, Hildegard. *Madrid und Wien 1632–1637. Politik und Finanzen in den Beziehungen zwischen Philipp IV. und Ferdinand II.* Münster : Aschendorff 1991.

[13] MALOCH, Antonín V. Rozluštění chiffrovaného písma v češtině. *Lumír* 1858, s. 205–206; 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; Viz VAVROUŠKOVÁ, Anna. *Šifrované dopisy Fridricha Falckého. In: Sborník prací věnovaných Janu Bedřichu Novákovi k šedesátým narozeninám*. Praha : Československá archivní

zabýval Jaroslav Kašpar, který se zčásti zamýšlel i nad obecnějšími otázkami šifrování a předložil první ucelenější bibliografii české a rakouské odborné literatury věnované dějinám kryptologie.[14]

ZÁKLADNÍ KRYPTOLOGICKÉ POJMY

Ačkoli není předmětem tohoto článku šifrování jako takové, ale jen některé jeho aspekty a způsoby využití, bude vhodné na začátku krátce zmínit základní kryptologické pojmy, aby se mohl orientovat i čtenář, který se s nimi dosud nesetkal.[15] *Kryptologie* je věda o utajení obsahu zpráv. Jejími hlavními podobory jsou *kryptografie* a *kryptoanalýza*.[16] Zjednodušeně řečeno kryptografie zkoumá metody pro utajení obsahu zprávy. Zvláště v současné informační společnosti, kdy potřeba ochrany dat stále stoupá, řeší tato vědní disciplína mnohé aspekty utajování informací. V minulosti byla její náplní především tvorba a používání šifrovacích systémů. Naopak kryptoanalýza se zabývá luštěním těchto šifrovacích systémů, resp. šifrovaných zpráv. Mezi kryptografií a kryptoanalýzou však existuje velmi silný vztah, protože oba obory jsou zákonitě propojeny a každý z nich musí využívat poznatky toho druhého. Chceme-li vytvářet bezpečný šifrovací systém, musíme znát jeho slabiny, vžít se do role luštitele, kryptoanalytika. A naopak, chceme-li šifrované zprávy luštit, musíme vědět, na jakých principech jsou založené. V souvislosti s kryptoanalýzou je třeba odlišovat dva pojmy, které bývají zvláště v archivní literatuře z historických důvodů často zaměňovány. Současná kryptologie rozlišuje *dešifrování* a *luštění* textu. Dešifrování je pouze mechanickou činností, při níž je šifrovaná zpráva převáděna zpět na původní text s pomocí klíče, zatímco snaha o zjištění obsahu zprávy bez znalosti klíče se nazývá *luštění*. Toto odlišení však zavedla až moderní kryptologie a v minulosti se obvykle používal pouze termín dešifrování, který zpravidla označoval i samotné luštění.[17]

Velice důležitými pojmy kryptologie, které budou prostupovat celým článkem, jsou *otevřený text* a *šifrový text.* Jako otevřený text se označuje text zprávy psaný běžnými a pro

společnost 1932, s. 486–494; HULEC, Otakar. Konspirativní charakter předbělohorské protistavovské opozice. *Jihočeský sborník historický* 30, 1961, s. 97–102.

[14] KAŠPAR, Jaroslav. Příspěvek k řešení tajného písma ze 17. století. Acta Universitatis Carolinae, Philosophica et Historica 5, 1963, s. 95–107; TÝŽ, *Soubor statí o novověkém písmu.* Praha : Univerzita Karlova 1993, s. 177–209.

[15] Ještě roku 2002 si přední český kryptolog Vlastimil Klíma v předmluvě k prvnímu českému vydání knihy Simona Singha posteskl nad absencí úplné české kryptologické terminologie. SINGH, Simon. *Kniha kódů a šifer.* Praha : Dokořán a Argo 2003, s. 10. V následujících odstavcích, týkajících se české kryptologické terminologie, čerpám především z mladší knihy dalšího vynikajícího kryptologa Pavla Vondrušky. VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha : Albatros 2006, s. 8–35.

[16] Trochu stranou dvou výše uvedených oborů stojí *steganografie*, která někdy bývá označována jako třetí podobor kryptologie. Ta se nezabývá tím, jak utajit obsah zprávy, ale tím, jak utajit skutečnost, že vůbec nějaká zpráva existuje. Sem patří tajné schránky, neviditelné inkousty, mikrotečky apod. Steganografické metody však nebudou předmětem tohoto článku.

[17] Viz např. BREITHAUPT, Christian. *Ars decifratoria, sive Scientia occultas scripturas solvendi et legendi.* Helmstadt : Christian Friedrich Weygand 1738. Také např. v němčině se dodnes pro *luštění* užívá pojmu *Entzifferung*, zatímco pro *dešifrování* pojmu *Entschlüsselung*.

okruh možných čtenářů (ať zamýšlených nebo nezamýšlených) srozumitelnými znaky, obvykle znaky abecedy příslušného jazyka. Právě proto, aby tento text nebyl běžně srozumitelný a jeho obsah mohla číst pouze omezená skupina vybraných osob, bývá otevřený text převeden na šifrový text, který vzniká buď tak, že jsou znaky otevřeného textu přeskupeny, anebo zaměněny za znaky jiné.

V prvním případě jde o *transpozici*, při níž dochází ke změně pozice znaků otevřeného textu se záměrem, aby zprávu mohl číst pouze ten, kdo zná způsob, jakým byly znaky přeskupeny. Jde o případy, kdy se text čte např. odzadu nebo jen jeho každé druhé písmeno. Do tohoto okruhu utajení zpráv patří i užívaní šifrovacích mřížek. Nezdá se však, že by se tento způsob šifrování zpráv v raném novověku nějak výrazně užíval, a ani mezi korespondencí uloženou v SOA v Plzni jsem žádnou takovou zprávu nenalezl. Transpozici proto nebudu nadále věnovat pozornost.

Ve druhém případě jde o *substituci*. Při ní jsou znaky otevřeného textu nahrazeny znaky *šifrové abecedy*, které obvykle mají podobu běžné latinské abecedy (ovšem se změněným významem) nebo znakových systémů jiných jazyků, dále číslic, astrologických symbolů, geometrických tvarů aj. Někdy bývají samostatným znakem šifrové abecedy nahrazována i delší spojení znaků otevřeného textu – většinou bigramy (tj. spojení dvou sousedních znaků - ba, be, bi, ... atd.), případně trigramy (pra, pro, ...) nebo slabiky. Substituce může být monoalfabetická, při níž je užíváno pouze jedné šifrové abecedy, a polyalfabetická, při níž je pro převod znaků otevřeného textu užíváno více šifrových abeced. Podobně jako u transpozice nebude v dalším textu věnována pozornost ani polyalfabetické substituci, protože mi zatím pro toto období není znám jediný případ jejího dochování v našich archivech.

Zvláštním druhem substituce jsou kódy, i když někdy bývá kódování považováno za samostatný způsob šifrování. Kódy jsou obvykle znaky nebo jejich spojení (případně i slova), která nahrazují celá slova otevřeného textu. Vzhledem k tomu, že při kódování nejsou nahrazovány pouze znaky, ale celá slova, může být počet kódů značně velký, takže často jsou vytvářeny dlouhé seznamy kódů – *kódové knihy*.

Jednotlivé způsoby šifrování je samozřejmě možné libovolně kombinovat, k čemuž hojně docházelo i v minulosti.

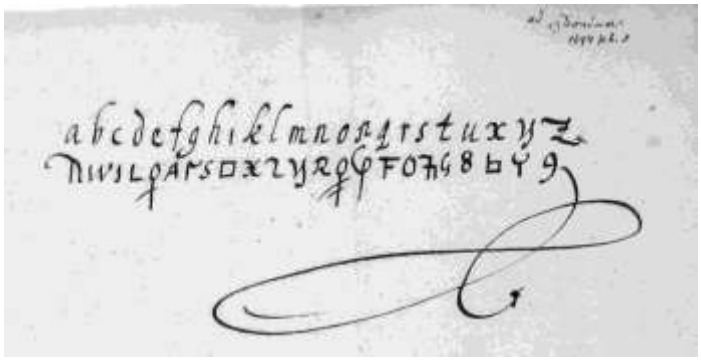
Z výše uvedených šifrovacích systémů byla v období raného novověku nejrozšířenější substituce. Doklady o jejím používání máme již ve starověku. Známá je např. Caesarova šifra.[18] Při jejím užití bylo každé písmeno otevřeného textu zaměněno za písmeno, které se nachází o tři pozice dále v abecedě. Komplikovanější variantou je vyloučení pravidelnosti

[18] Pasáže zabývající se historií kryptologie, které prostupují text o české kryptologické terminologii, čerpají především z těchto prací: KLÍMA, Vladimír. Utajené komunikace, 1.–4. díl. *Chip*, květen 1994, str. 194–197, červen 1994, str. 184–188, červenec 1994, str. 138–141, srpen 1994, str. 118–121; SINGH, Simon. *Kniha kódů a šifer*. Praha : Dokořán a Argo 2003, s. 17–70; VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha : Albatros 2006, s. 201–240. Pavel Vondruška dále přednesl sérii přednášek o historii kryptologie na každoročních Mikulášských kryptobesídkách. Prezentace dostupné z URL: http://crypto–world.info/vondruska/index.php?id=prednasky. Další sérii článků na stejné téma publikoval v internetovém e–zinu Crypto–world. Dostupné z URL: http://crypto–world.info/index2.php.

(např. posunu o tři písmena v případě Caesarovy šifry) a přiřazení znaků šifrové abecedy znakům otevřené abecedy náhodně. V tom případě si už adresát nevystačí se zapamatováním jednoduché poučky, ale musí mít k dispozici *šifrovací klíč*, s jehož pomocí provede dešifrování. Systém, v němž je každý znak otevřené abecedy nahrazen jedním znakem šifrové abecedy, se nazývá *jednoduchá substituce* (viz *příklad 1* a *obr. 1*).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Q	Y	Z
Q	W	E	R	T	Z	U	I	O	P	A	S	D	F	G	H	J	K	L	Y	X	C	V	B	N	M

SEJDEME SE V SEDM V LESE = LTPRTDT LT C LTRD C STLT



Obrázek 1 – klíč pro šifrování pomocí jednoduché substituce, [1. polovina 17. století]. Ve fondu uložen u dopisu purkrabího z Donína Maxmiliánovi z Trauttmansdorffu z 8. února 1644.

Ve starověku byl tento systém považován za nevyluštitelný, ale středověcí arabští učenci dokázali přijít na řešení v podobě *frekvenční analýzy* šifrového textu, založené na zkoumání rozdílné četnosti hlásek a jejich spojení v jednotlivých jazycích a tomu odpovídající frekvenci znaků šifrové abecedy v textu. Například nejčastěji užívanou hláskou v českém jazyce je E, které v česky psaných textech statisticky zaujímá zhruba 11 % celého textu. Objeví-li se v textu šifrovaném jednoduchou substitucí šifrový znak, který se v textu vyskytuje zhruba v 11 %, je poměrně pravděpodobné, že tento šifrový znak skutečně nahrazuje písmeno E. U velmi krátkých textů však může být frekvenční analýza neúčinná. Obecně platí, že čím delší je text, který je k dispozici, tím je tato metoda spolehlivější. Kromě četnosti samostatných znaků se zkoumá i četnost bigramů (v češtině patří mezi nejčastější např. ST, PR, PO, CH), trigramů (v češtině nejčastější např. STR nebo PRO) a polygramů.[19]

V Evropě se jednoduchá substituce užívala i ve středověku. Někdy docházelo dokonce pouze k záměně samohlásek a souhlásky zůstávaly v původní podobě.[20] Spolehlivější šifrovací systémy se v Evropě začaly prosazovat až v období renesance, především v

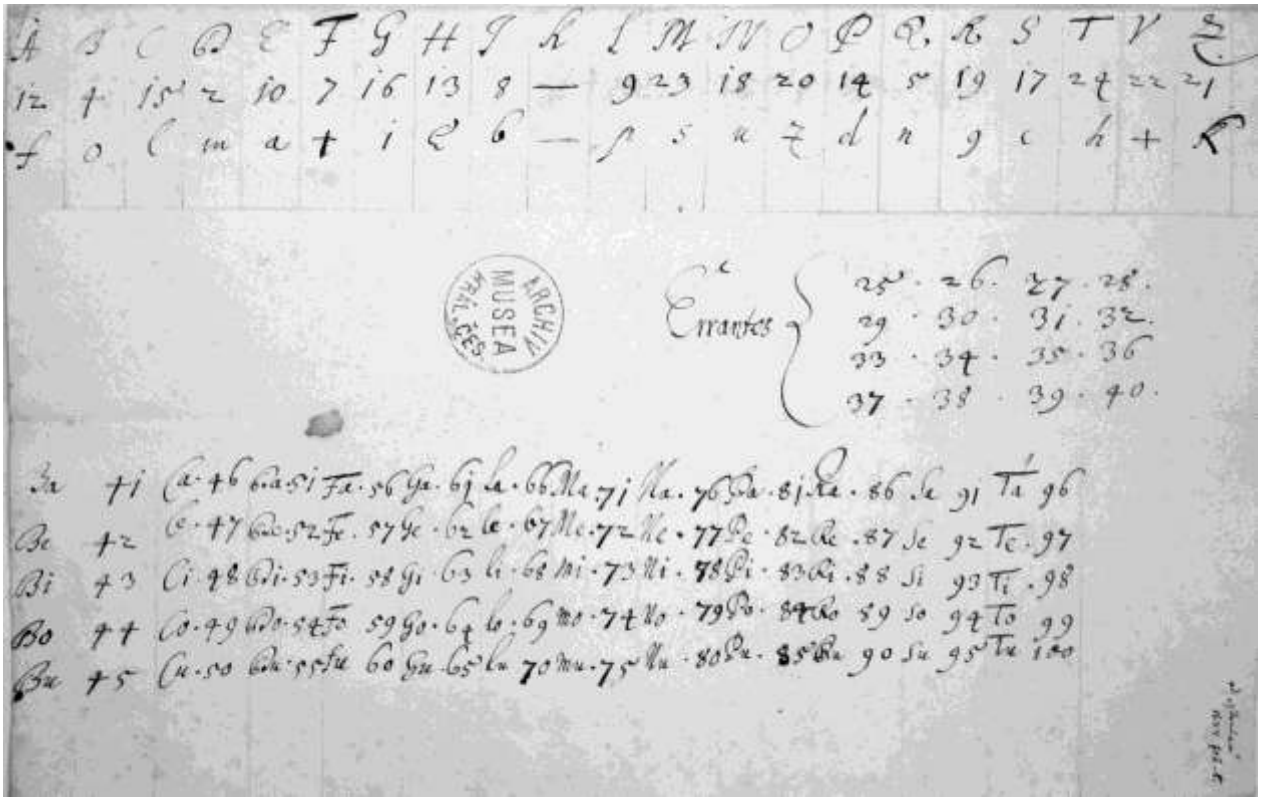
[19] Tabulky četnosti výskytu hlásek a jejich spojení v češtině, angličtině, francouzštině, němčině, španělštině a italštině viz JANEČEK, Jiří. *Odhalená tajemství šifrovacích klíčů minulosti.* Praha : Naše vojsko, 1994, s. 17–24.

[20] Viz např. RYBA, Bohumil. K tajnému písmu v listech Husových. *Sborník historický* 1, 1953, s. 46–52.

italském prostředí. Nejjednodušší, ale rozhodně ne nepřemožitelnou obranou proti frekvenční analýze bylo užívání *homofonní substituce*, které spočívalo v tom, že pro nejčastěji užívané hlásky bylo alternativně užíváno více znaků, čímž se snížila četnost jejich výskytu v šifrovém textu (viz *příklad 2* a *obr. 2* na následující straně). První jednoduché homofonní šifry se začaly objevovat již koncem 14. století.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Q	Y	Z
Q	W	E	R	T	Z	U	I	O	P	A	S	D	F	G	H	J	K	L	Y	X	C	V	B	N	M
ξ				β				φ			μ		δ	π			ζ	θ	ν	ε	λ			ω	
8				3				2						7						5				9	

SEJDEME SE V SEDM V LESE = LβPR3DT θβ C L3RD λ STθβ



Obrázek 2 – nomenklátor s klíčem pro homofonní substituci (nahoře), klamači (uprostřed) a bigramy (dole), [1. polovina 17. století]. Ve fondu uložen u dopisu purkrabího z Donína Maxmiliánovi z Trauttmansdorffu z 8. února 1644.

Další obranou proti frekvenční analýze bylo jednolité psaní šifrového textu bez oddělování slov a také používání *klamačů*, v dobové terminologii nejčastěji označovaných latinskými termíny *errantes* nebo *nullae* (viz např. *obr. 2*). Klamače byly znaky šifrové abecedy, které nezastupovaly žádný znak otevřené abecedy a do textu byly vkládány jen pro zmatení případného luštitele. Při dešifrování se klamače jednoduše přeskakovaly. Pokud bychom

stanovili, e klamači jsou číslice 1, 4 a 6, a rozhodli se pro neoddělování jednotlivých slov, mohla by výše uvedená zašifrovaná zpráva vypadat např. takto:

SEJDEME SE V SEDM V LESE = L1βPR34DTθβCL31RDλS6T4θβ

V době raného novověku byly zprávy šifrovány převážně prostřednictvím tzv. *nomenklátoru*, který byl kombinací šifrování pomocí substituce a kódování. Nejjednodušší nomenklátory se skládaly z jednoduché nebo homofonní šifrové abecedy a pár kódů, nahrazujících několik pro danou korespondenci nejobvyklejších slov. Ve složitějších nomenklátorech se kromě většinou homofonní šifrové abecedy objevovaly znaky pro bigramy či nejpoužívanější slabiky, klamače, zdvojené souhlásky a také obvykle mnohem větší počet kódů pro celá slova (viz např. *obr. 3*). Vzhledem k tomu, že počet potřebných znaků šifrové abecedy takto stále vzrůstal, začalo převažovat zapisování šifrového textu pomocí číslic. Některé nomenklátory obsahovaly tolik kódů, že už se nevešly na jeden list papíru a byly zapisovány do sešitu. Tím byl dán základ pro vznik kódové knihy.

Obrázek 3 – nomenklátor pro italsky psanou korespondenci s Juanem Álvarem kardinálem Cienfuegos Villazón. [cca 1720–1730]. Kromě klíče pro homofonní substituci, bigramů, klamačů aj. obsahuje téměř 200 abecedně řazených kódů.

Jak již bylo řečeno výše, vývoj středověké evropské kryptologie byl spojen především s Itálií a konkrétně zejména s Benátkami. Toto postavení si Itálie udržela i v raném novověku, především pak v 16. století, kdy byla patrně nejvyspělejším kryptologickým pracovištěm papežská kancelář. Z Itálie se šířily nové metody do dalších románských zemí – Španělska a

Francie, kde v průběhu 16. a 17. století docházelo i k jejich dalšímu zdokonalování. Ve druhé polovině 17. století se kryptologie dále rozvíjela i v Anglii. Střední Evropa zpočátku nehrála ve vývoji kryptologie výraznější roli. To se změnilo v 18. století v souvislosti se vznikem špičkového kryptologického pracoviště, tzv. černé komnaty, u vídeňského dvora pod vedením Ignáce svobodného pána von Koch.[21]

Nelze si však představovat, že pisatelé šifrovaných dopisů vždy užívali těch nejmodernějších a nejbezpečnějších šifrovacích systémů. Samozřejmě vždy záviselo na schopnostech a kryptografických znalostech jejich konkrétních tvůrců či uživatelů. Volbu šifrovacího systému však ovlivňovaly i jiné faktory. Kromě bezpečnosti šifry hrála významnou roli i obtížnost a časová náročnost vyhotovení šifrového textu a jeho následného dešifrování. Mnoho situací, zvláště ve válečných dobách, totiž obvykle vyžadovalo velmi rychlé jednání. V takových případech by nebylo efektivní využívat takovou šifru, která by sice byla velmi bezpečná, ale zároveň by při jejím použití trvalo sestavení a dešifrování zprávy neúměrně dlouhou dobu. Z toho důvodu se v raném novověku např. téměř nevyužívalo polyalfabetické substituce, ačkoli byla vynalezena již v 16. století. Faktor bezpečnosti šifry a faktor náročnosti její aplikace jsou hlavními hledisky pro volbu šifrovacího systému prakticky dodnes. Velkou roli hrálo např. i to, jak důležitá byla samotná šifrovaná zpráva, z jakého prostředí pocházel její pisatel nebo jak schopný byl v jeho očích její potenciální luštitel.

ŠIFROVANÁ KORESPONDENCE V SOA V PLZNI A V NĚKTERÝCH DALŠÍCH ČESKÝCH ARCHIVECH

K tomu, abychom získali přesnější obrázek o tom, jakým způsobem byla korespondence šifrována v konkrétní době a prostředí, je především nezbytné studovat dobové archivní prameny. V českých archivech se nachází relativně velké množství šifrované korespondence z období třicetileté války. Řada šifrovaných dopisů je uvedena v edici *Documenta Bohemica bellum tricennale illustrantia*.[22] Tato edice pramenů je však pouze výběrová, a tak s její pomocí nelze získat vyčerpávající přehled o veškeré šifrované korespondenci té doby, uložené v našich archivech, ale velice dobře poslouží pro získání základní orientace a k vytipování příslušných fondů. Mezi ty nejbohatší patří především rodinné archivy rodů, z jejichž řad pocházeli významní císařští vojevůdci a které se v Čechách většinou usadily v důsledku pobělohorských konfiskací. K nejvýznamnějším z nich patří Historická sbírka (rodinný archiv) Clam-Gallasů, Frýdlant (SOA v Litoměřicích – pobočka Děčín); Rodinný archiv Piccolominiů, Náchod (SOA v Zámrsku); Rodinný archiv Buquoyů a Rodinný archiv Schwarzenberků, Hluboká nad Vltavou (SOA v Třeboni); Valdštejniana, Jičín (Národní archiv) nebo Rodinný archiv Ditrichštejnů (MZA v Brně).[23]

---

[21] STIX, Franz. Zur Geschichte und Organisation der Wiener Geheimen Ziffernkanzlei von ihren Anfängen bis zum Jahre 1848. *Mitteilungen des Österreichischen Instituts für Geschichtsforschung* 51, 1937, s. 131–160.

[22] ČECHOVÁ, Gabriela – JANÁČEK, Josef – KOČÍ, Josef – POLIŠENSKÝ, Josef (edd). *Documenta Bohemica belli tricennale illustrantia, Tomus I–VII*. Praha : Academia 1971–1981.

[23] Některé z těchto fondů mi poskytly materiál pro srovnání s archiváliemi SOA v Plzni. Více k tomu viz níže.

Pro období před třicetiletou válkou je autorovi článku zatím známo pouze několik příkladů šifrované korespondence uložené v českých archivech. Velké množství šifrovaných dopisů z doby před Bílou Horou by se mělo nacházet ve Sbírce fotonegativů MZA v Brně. Negativy byly pořízeny za první republiky při bohemikálních výzkumech konaných převážně ve Vatikánu a ve španělském Generálním archivu v Simancas. Ale již v roce 1979 prý byla většina snímků vinou rozkladu emulze nečitelná.[24] Dalším zajímavým pramenem z předbělohorských Čech je částečně šifrovaná korespondence Viléma z Rožmberka s jeho agenty v době jeho kandidatury na polský trůn v letech 1574–1575, uložená v SOA v Třeboni.[25] V Národním archivu se v opisech dochovala korespondence některých významných domácích i zahraničních představitelů protestantské opozice vůči císaři, mimo jiné např. Petra Voka z Rožmberka[26] a v Archivu Národního muzea soubor šifrované korespondence z let 1608–1612, o které se zmíním ještě níže.[27] Pro období po třicetileté válce jsou autorovi článku zatím známy pouze šifrované dopisy a klíče uložené v SOA v Plzni, o kterých bude pojednáno níže. Je ale nanejvýš pravděpodobné, že se nacházejí i v jiných archivech.[28]

Jak již bylo řečeno v úvodu, v SOA v Plzni se raně novověká šifrovaná korespondence nachází především ve fondech šlechtických rodinných archivů, uložených na pracovišti v Klášteře. Nejvýznamnější soubory šifrovaných dopisů a šifrových klíčů se nacházejí ve fondech Rodinný archiv Trauttmansdorffů a Rodinný archiv Windischgrätzů. Malé množství šifrovaných dokumentů je uloženo ještě ve fondech Rodinný archiv Verdugů, Doupov; Rodinný archiv Nostitz-Rienecků, Sokolov a Rodinný archiv Nostitzů, Planá.

V případě Rodinného archivu Trauttmansdorffů jde výhradně o korespondenci Maxmiliána z Trauttmansdorffu z doby třicetileté války. Maxmilián z Trauttmansdorffu (1584–1650) měl

---

Na tomto místě bych rád poděkoval za vstřícné přijetí a pomoc se zpřístupněním fondů a obtížněji dostupné literatury svým váženým a milým kolegyním a kolegům Heleně Smíškové, Otto Chmelíkovi (oba SOA v Litoměřicích – pobočka Děčín), Laděně Plucarové, Jaromíru Hřebeckému (oba SOA v Třeboni), Jiřímu Kubovi, Milanu Novotnému (SOA v Zámrsku) a Janu Kahudovi (Národní archiv).

[24] Viz CULKOVÁ, Dagmar. Výzkum bohemik v zahraničí do roku 1939 organizovaný našimi archivy. In: *Sborník archivních prací*. Praha 1979, roč. 29, s. 173.

[25] SOA v Třeboni, Historica Třeboň, sign. 4834/36. Pod touto signaturou se nachází 26 dopisů, z nichž tři jsou šifrované. Vilém z Rožmberka užíval k šifrování jednoduchou substituci a asi třicet kódů. Edice dopisů a klíč ke korespondenci viz 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). Za tyto informace vděčím Kateřině Pražákové z Filozofické fakulty Jihočeské univerzity v Českých Budějovicích. Veržovskij se ve své práci zabývá také kandidaturou na polský trůn arcivévody Ferdinanda, který při té příležitosti také užíval šifrované korespondence. Zajímavé je, že arcivévodův šifrovací systém byl složitější než Vilémův. Pro každý znak abecedy používal dva znaky šifrové abecedy (homofonní substituce) a stejně jako Vilém také kódy.

[26] HULEC, Otakar. Konspirativní charakter předbělohorské protistavovské opozice. *Jihočeský sborník historický* 30, 1961, s. 97–102.

[27] Archiv Národního muzea, Sbírka D, karton č. 9, korespondence z let 1606-1611.

[28] Vzhledem k absenci podobné pomůcky jako je edice *Documenta Bohemica bellum tricennale illustrantia* je badatel pro období před třicetiletou válkou a po ní odkázán především na archivní pomůcky, v nichž ale nebývá pravidlem uvádět, zda je korespondence šifrovaná, anebo na literaturu, která je však k tomuto tématu velice skrovná. Má–li štěstí, podaří se mu získat tip od archiváře nebo jiného badatele.

rozhodující vliv na pozvednutí Trauttmansdorffů mezi nejmocnější šlechtické rody habsburské monarchie. Za vlády císařů Matyáše a zejména Ferdinanda II. a Ferdinanda III. dovedl dobře uplatnit svůj diplomatický talent a získat tak jejich přízeň. Jako nejvyšší hofmistr císaře Ferdinanda III. se stal nejvlivnějším mužem na jeho dvoře. Proslul především jako císařský hlavní vyslanec při jednáních o vestfálském míru, na kterých houževnatě hájil císařovy zájmy. V příhodné politické konstelaci Maxmilián obratně využil možnosti zajistit pro své potomky rozsáhlý pozemkový majetek v Čechách.[29]

Většina písemné pozůstalosti Maxmiliána z Trauttmansdorffu se dnes nachází ve fondu *Familienarchiv Trauttmansdorff*, který je uložen v Rakouském státním archivu ve Vídni a je stále ve vlastnictví rodiny Trauttmansdorffů.[30] I v tomto fondu se nachází mnoho šifrovaných dopisů (pravděpodobně mnohem více než v SOA v Plzni) a především klíčů, které se ve fondu Rodinný archiv Trauttmansdorffů dochovaly jen vzácně. Pro hlubší zkoumání šifrované korespondence Maxmiliána z Trauttmansdorffu bude tedy v budoucnu nutné využít obou uvedených fondů.

Nejrozsáhlejší a pravděpodobně nejvýznamnější je soubor šifrovaných dopisů zaslaných Maxmiliánovi říšským vicekancléřem Ferdinandem Zikmundem Kurtzem von Senftenau.

Obrázek 4 – dopis Ferdinanda Zikmunda Kurtze von Senftenau Maxmiliánovi z Trauttmansdorffu ze 17. ledna 1639 z Hamburku (první strana). Většina šifrovaného textu je dešifrována mezi řádky

[29] Srov. MÍRKOVÁ, Marie. Řád zlatého rouna a rodová prestiž v představách Adama Matyáše z Trauttmansdorffu, in: Václav Bůžek – Jaroslav Dibelka (edd.), *Utváření identity ve vrstvách paměti.* České Budějovice 2011 (= Opera historica 15), s. 249–282, zde s. 256–257; LERNET, Brigitte. *Maximilian von Trauttmansdorff. Hofmann und Patron im 17. Jahrhundert (dizertační práce).* Wien 2004.

[30] Österreichisches Staatsarchiv Wien, Allgemeines Verwaltungsarchiv, Familienarchiv Trauttmansdorff. K fondu srov. MÍRKOVÁ, Marie. *Bádání v Rakouském státním archivu ve Vídni*. Západočeské archivy 2, 2011, s. 10–12. Fond byl Marií Mírkovou také popsán pro účely *Průvodce po Rakouském státním archivu ve Vídni pro českého návštěvníka*, který by měl koncem roku 2012 vydat Národní archiv. Jeho autorem je kolektiv autorů pod redakčním vedením Jana Kahudy.

Nejvíce dopisů pochází z let 1638–1639. Kurtz von Senftenau je zasílal Trauttmansdorffovi do Vídně z Hamburku, kde se v té době účastnil diplomatických jednání. Většinou jde o poměrně dlouhé a dosud nedešifrované dopisy, které jsou psány německy, ovšem s mnoha cizojazyčnými diplomatickými termíny.[31] Na první straně dopisu ze 17. ledna 1639 byl naštěstí mezi řádky vepsán dešifrovaný otevřený text (viz *obr. 4*).

Díky tomu jsem porovnáním šifrového a otevřeného textu mohl sestavit šifrovací klíč, který lze aplikovat na všechny dopisy těchto dvou osob z této doby. Klíčem je nomenklátor obsahující šifrové znaky pro jednotlivá písmena abecedy (jde o homofonní substituci), pro bigramy (ba, be, bi, bo, bu; ca, ce, ci, co cu; da, de, di, … atd.) a klamače. Neobsahuje žádné kódy. Vzhledem ke značné délce dopisů jsem jako vzorek pomocí získaného klíče zatím dešifroval pouze psaní ze 17. ledna 1639.

Jeho text obsahuje velké množství poměrně heslovitě podávaných informací. Kurz von Senftenau informoval Trauttmansdorffa mimo jiné o nátlaku, který bude zřejmě činit koalice Švédů, Francouzů a Holanďanů na polského krále, o problémech se zásobováním, o nutnosti vybudovat z pěších vojáků kavalerii, nebo o tom, že sasko-lauenburský vévoda má zřejmě v úmyslu vydat se pod ochranu Dánska.

Nejzajímavější je zřejmě nejdelší pasáž, týkající se významného braniborského vojevůdce Hanse Georga von Arnim, který se do třicetileté války zapojil nejdříve na katolické a později na protestantské straně, když stanul v čele saských vojsk. Po pražském míru se Arnim stáhl do ústraní, ale roku 1637 byl zajat a odvlečen do Švédska, odkud se mu roku 1638 podařilo uprchnout a dostat do Hamburku.[32] Dopis byl tedy napsán poměrně krátce po jeho útěku. Kurtz v něm sděluje, že s Arnimem jednal a ten ho ujišťoval, že neměl žádný podíl na „frýdlantské zradě“ (rozuměj Valdštejnově zradě), jak se o něm soudí. Naopak ji prý pomohl odhalit. Je zjevné, že uvažoval o opětném přejití na katolickou stranu a žádal o milost u císaře. Kurtz zřejmě opatrně doporučoval mu vyhovět. Jak známo, Arnim brzy na to skutečně opět začal bojovat na straně císařských, při níž setrval až do své smrti roku 1641.

Součástí fondu je také dopis Kurtze Trauttmansdorffovi z 19. září 1646, kdy se oba vyskytli prakticky v opačné situaci. Tentokrát byl Trauttmansdorff na mírových jednáních v Münsteru a Kurtz mu psal z Vídně. Klíč ke korespondenci z let 1638–1639 nelze v tomto případě aplikovat. Text dopisu je ale dešifrován hned na následující straně, a tak bylo opět možné klíč rekonstruovat. Jde znovu o nomenklátor, ovšem tentokrát bez znaků pro bigramy. Naopak oproti staršímu nomenklátoru se zde vyskytují kódy a je posílena homofonie tím, že jednotlivá písmena abecedy jsou střídavě nahrazována 3–5 různými znaky šifrové abecedy.[33]

---

[31] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 10, i. č. 200. Tato korespondence je zmíněna i v edici ČECHOVÁ, Gabriela – JANÁČEK, Josef – KOČÍ, Josef (edd). *Documenta Bohemica bellum tricennale illustrantia. Tomus VI.* Praha : Academia 1978, s. 53.

[32] Viz např. GOLLWITZER, Heinz. Hans Georg Arnim v. Boitzenburg. In: *Neue Deutsche Biographie. Band 1*. Berlin : Duncker & Humblot 1953, s. 372–373.

[33] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 10, i. č. 200.

Ke korespondenci Maxmiliána z Trauttmansdorffu s Kurtzem von Senftenau je také přiložen koncept latinsky psaného a pomocí jednoduché substituce šifrovaného dopisu z 11. září 1635, jehož adresát není určen,[34] a nomenklátor k italské korespondenci. Nepodařilo se mi zjistit žádnou spojitost těchto archiválií s Kurtzem von Senftenau. I když to nemohu říci s jistotou, zdá se mi pravděpodobné, že obě byly k jeho dopisům zařazeny až při některém ze starších archivních pořádání, a to především z toho důvodu, že jde také o šifry.[35] Tuto domněnku posiluje především fakt, že přiložený nomenklátor vznikl pravděpodobně již někdy mezi lety 1616–1621.[36]

Za samostatnou zmínku také určitě stojí opis dopisu českého a uherského krále a budoucího císaře Ferdinanda III. ze 13. listopadu 1634.[37] Jde o jediný z celého souboru kopií Ferdinandových dopisů Trauttmansdorffovi, který byl šifrován. O významu jeho obsahu svědčí i nešifrovaná zpráva v jeho závěru, v níž Ferdinand výslovně sděluje, že dopis šifruje a posílá jej po svém vlastním poslu. Text není dešifrován a klíč se mi zatím nepodařilo rozluštit.[38] Podle velkého počtu znaků šifrové abecedy a jejich podoby[39] se zdá, že jde o složitější nomenklátor s homofonií, bigramy a pravděpodobně i kódy.

Počet dalších pisatelů šifrované korespondence adresované Maxmiliánovi z Trauttmansdorffu je poměrně značný a nelze se každým zabývat dopodrobna. Níže sice uvedu jejich úplný výčet (resp. výčet těch, jejichž šifrované dopisy jsou mi známy), ale krátce se zastavím jen u několika nejdůležitějších.

Významný okruh Trauttmansdorffových korespondentů tvořili císařští vyslanci, případně agenti či rezidenti v cizích zemích.[40] Mezi ně patřili císařský rezident v Konstantinopoli Sebastian Lustrier von Liebenstein[41] (dopis ze 7. dubna 1625 – viz *obr. 5*);[42] Johann Karl hrabě von Schönburg,[43] císařský vyslanec v Madridu (dopis z 20. června 1637);[44] František Pavel de Li-

[34] Podoba jména uvedeného v konceptu je pravděpodobně [B. Fopio].

[35] Tento postup nebyl neobvyklý a setkal jsem se s ním i v jiných případech.

[36] Nomenklátor uvádí mimo jiné kódy pro kardinála Klesla (tj. Melchiora Klesla, který byl kardinálem jmenován roku 1616) a kardinála Aldobrandiniho (s největší pravděpodobností jde o Pietra Aldobrandiniho, který zemřel roku 1621). Viz RAINER, Johann. Klesl, Melchior. In: *Neue Deutsche Biographie. Band 12*. Berlin : Duncker & Humblot 1980, s. 51–52; *Ottův slovník naučný. První díl.* Praha : J. Otto 1888, s. 757. Nomenklátor se tedy svým časovým zařazením vymyká z řady Kurtzových dopisů. Od ostatních nomenklátorů, které používal Maxmilián z Trauttmansdorffu, se liší také tím, že pro některé znaky šifrové abecedy jsou užita písmena hebrejské alefbety.

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

[38] Není vyloučeno, že by se odpovídající nomenklátor pro korespondenci Maxmiliána z Trauttmansdorffu a Ferdinanda III. mohl nacházet ve Vídni ve fondu FA Trauttmansdorff nebo v Haus–, Hof– und Staatsarchiv.

[39] Šifrová abeceda je tvořena výhradně dvojcifernými a trojcifernými číslicemi.

[40] Vzhledem k tématu tohoto článku by pojmy „agent“ a „rezident“ mohly svádět představě tajného agenta či špiona. Agenty byli v raném novověku, ale i v dobách mladších, nazýváni lidé, kteří pro osobu či instituci, která je najímala, obvykle zcela otevřeně obstarávali různou agendu na vzdáleném místě. To ovšem nevylučuje, že do popisu jejich činnosti mohlo patřit i obstarávání tajných zpráv.

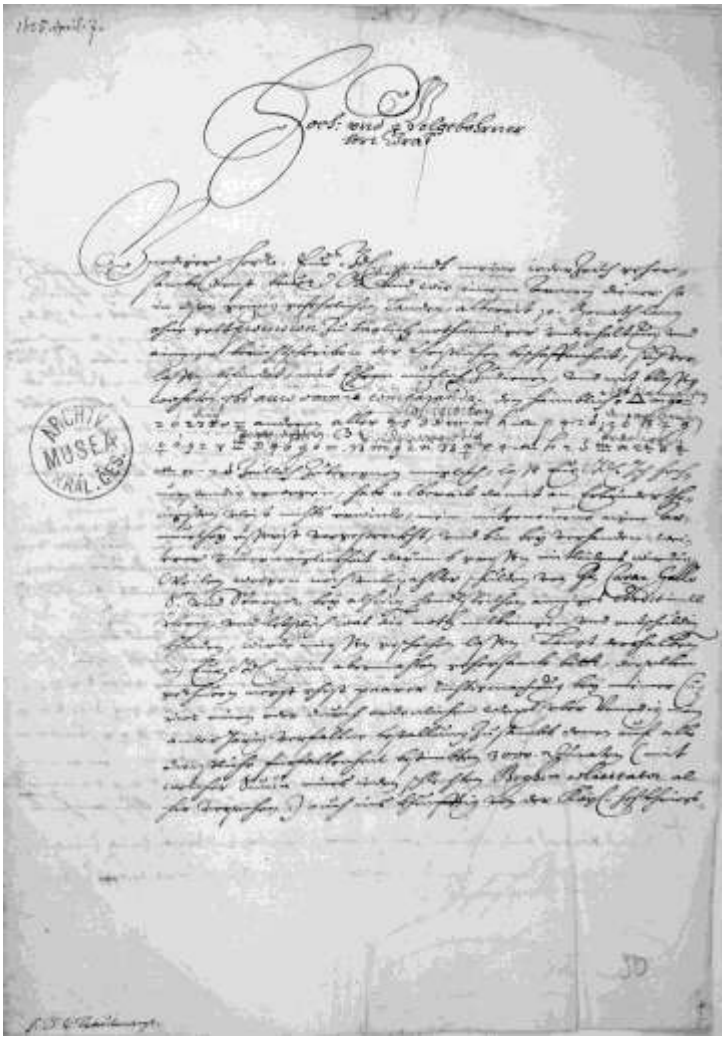
[41] Sebastiana Lustriera von Liebenstein jako rezidenta v Konstantinopoli zmiňuje např. HAMMER, Joseph von. *Geschichte des Osmanischen Reiches. Neunter Band.* Pest : C. A. Hartleben´s Verlage, 1933, s. 312.

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

[43] Schönburgovým působením v Madridu se obsáhle zabývala např. ERNST, Hildegard. Madrid und Wien *1632–1637. Politik und Finanzen in den Beziehungen zwischen Philipp IV. und Ferdinand II.* Münster : Aschendorff 1991.

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

sola,[45] který v první polovině čtyřicátých let 17. století působil jako vyslanec v Londýně a v červnu a počátkem července roku 1645 napsal sérii šifrovaných dopisů z Bruselu;[46]Johann Tasselt,[47] agent Ferdinanda III. v Londýně, jehož dopisy z ledna a března roku 1645[48] jsou psány stejnou šifrou jako ty od de Lisoly;[49] a Johann Sieber,[50] císařský rezident v Hamburku (dopis ze 6. prosince 1639).[51]



List od Sebastiana Lustriera ze 7. dubna 1625 z Konstantinopole[52] je nejstarším šifrovaným dopisem v pozůstalosti Maxmiliána z Trauttmansdorffu. Značnou část textu věnoval Lustrier von Liebenstein svým finančním potížím, které mu ztěžovaly jeho poslání a nutily jej půjčovat si peníze. Žádal o zaslání značné finanční hotovosti 3000 dukátů přes Benátky. Většina textu je psána otevřenou abecedou, jen některé pasáže jsou utajeny pomocí homofonní šifry bez kódů.

Obrázek 5 – dopis Sebastiana Lustriera von Liebenstein Maxmiliánovi z Trauttmansdorffu ze 7. dubna 1625 z Konstantinopole (první strana). Text dešifrován mezi řádky.

[45] Této osobnosti a jejím diplomatickým službám (včetně období, z nějž pocházejí šifrované dopisy) je věnována kniha PRIBRAM, Alfred F. *Franz Paul Freiherr von Lisola (1613–1674) und die Politik seiner Zeit.* Leipzig : Veit & Comp., 1894.

[46] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 10, i. č. 209.

[47] O Tasseltově působení se rovněž zmiňuje PRIBRAM, Alfred F. *Franz Paul Freiherr von Lisola (1613–1674) und die Politik seiner Zeit*. Leipzig : Veit & Comp., 1894, s. 16, 18.

[48] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 12, i. č. 289.

[49] Shoda panuje i v jazyce dopisů. Všechny byly psány latinsky.

[50] Johann Sieber byl prvním poštmistrem saského kurfiřství. Roku 1636 vstoupil do služeb císaře v hodnosti nejvyššího zásobovacího komisaře (*Oberproviantkomissar*). Více k jeho osobě viz Geschichte des sächsischen Postwesens bis zur Zeit des Erscheines der Post–Ordnung vom Jahre 1713. In: HÜTTNER, Gottlieb F. *Beiträge zur Kenntniß des Postwesens.* Leipzig : Verlag von Gustav Brauns 1848, s. 269–272.

[51] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 12, i. č. 274.

[52] Tamtéž, karton č. 12, i. č. 330.

Žádal o zaslání značné finanční hotovosti 3000 dukátů přes Benátky. Většina textu je psána otevřenou abecedou, jen některé pasáže jsou utajeny pomocí homofonní šifry bez kódů. Důsledně je např. šifrováno jméno odbojného uherského magnáta Gabora Bethlena. Píše o jeho verbování posil a také o činnosti jeho poselstva v Konstantinopoli. Kromě toho uvádí, že vezír z Budy udržuje v pohotovosti řecké a bosenské jednotky.

Za zmínku stojí také dopis hraběte von Schönburga z 20. června 1637 z nejvzdálenější destinace – Madridu.[53] Je k němu totiž přiložena kopie šifrovaného dopisu adresovaného Schönburgovi španělským státním sekretářem Andrésem de Rocas.[54] Dopis je zároveň ukázkou velké chyby šifranta, o které se zmíním níže.

V menší míře se dochovaly šifrované dopisy od vojenských osob. V červenci roku 1646 Trauttmansdorff obdržel dopisy od císařského generálního válečného komisaře Joachima Fridricha svobodného pána von Blumenthal a od polního maršála Petra hraběte von Holzappel, který do roku 1642 bojoval na straně protestantů (viz obr. 6, na následující stránce). Oba dopisy byly šifrovány pomocí stejného silně homofonního klíče bez bigramů a kódů.[55] Z léta roku 1646 pocházejí také dopisy od francouzského vojevůdce ve službách Habsburků Alexandra hraběte de Bournonville. Tato korespondence není šifrována, ale jsou k ní přiloženy opisy dvou dopisů (jeden z nich je šifrovaný) českého pobělohorského exulanta Karla svobodného pána Robmhapa ze Suché, adresovaných hesenské landkraběnce Amálii Alžbětě von Hanau-Münzenberg ze stejné doby. Bournonville Trauttmansdorffovi sděloval, že tyto dopisy nepřátel byly zachyceny u Arnsbergu a že se nepodařilo šifru vyluštit.[56]

Dva klíče jsou přiloženy k nešifrovanému dopisu purkrabího z Donína,[57] datovanému 8. února 1644 ve Vratislavi.[58] Jeden je pro šifrování pomocí jednoduché substituce a ve druhém případě jde o složitější nomenklátor s homofonií, bigramy a klamači (viz obr. 1 a 2). Je ale pravděpodobné, že klíče ve skutečnosti ke korespondenci nepatří a byly k ní přidány až v pozdější době. Tento předpoklad podporuje i skutečnost, že jsou vzhledem k absenci písmene „W“ pravděpodobně určeny pro korespondenci v některém z románských jazyků, zatímco dopis purkrabího z Donína je psán německy.[59]

---

[53] Tamtéž, karton č. 12, i. č. 271.

[54] Z kopie dopisu nelze s jistotou určit, zda byl originál také šifrovaný. Pokud byl, tak pravděpodobně jinou šifrou než samotná kopie, která je vyhotovena podle klíče užívaného Schönburgem a Trauttmansdorffem. Praxi šifrování přeposílaných dopisů potvrzuje ERNST, Hildegard. Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel, 1635–1642. *Mitteilungen des Österreichischen Staatsarchivs*, 42, 1992, s. 102.

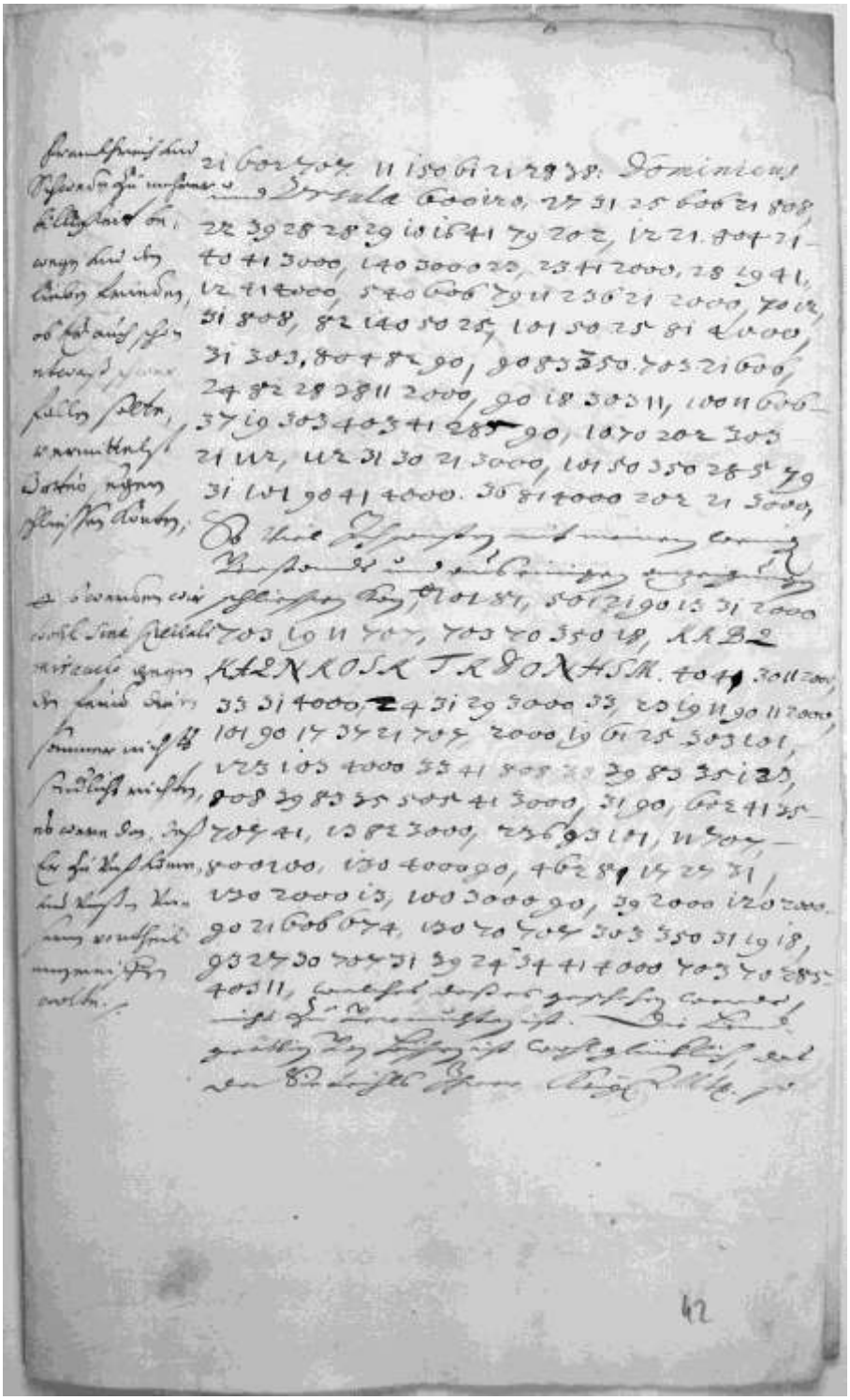
[55] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 8, i. č. 122; Tamtéž, karton č. 9, i. č. 184.

[56] Tamtéž, karton č. 8, i. č. 125.

[57] Nepodařilo se mi zjistit, o kterého člena rodu purkrabích z Donína přesně jde.

[58] SOA v Plzni, pracoviště Klášter, RA Trauttmansdorffů, karton č. 8, i. č. 148.

[59] Ovšem pouze na základě tohoto faktu nelze stoprocentně vyvrátit souvislost mezi dopisy purkrabího z Donína



Obrázek 6 – dopis Joachima Friedricha von Blumenthal Maxmiliánovi z Trauttmansdorffu ze 14. července 1646 z ležení u Hombergu (třetí strana). Text dešifrován na kraji stránky.

(pokračování v příštím čísle)

C. Tip na vánoční dárek: Enigma - bitva o kód

Mgr. Pavel Vondruška (pavel.vondruska@crypto-world.info)

Dovoluji si upozornit na český překlad jedné z nejvíce oceňovaných knih o Enigmě. Pokud se o problematiku šifrování nebo dějin druhé světové války zajímáte, pak by vám určitě neměla ve vaší knihovničce chybět.

Kniha vyjde těsně před vánocemi (17. 12. 2012), a tak může být současně i vhodným dárkem pod stromeček.

Enigma
bitva o kód
Hugh Sebag-Montefiore
Překlad: Jan Krejčí
Odborný korektor: Pavel Vondruška
Odpovědný redaktor: Andrea Brázdová, Silvie Sanža
Vnitřní úprava: Veronika Kopečková
Sazba a DTP: Veronika Kopečková, Alena Sigmundová
Jazyková korektura: Eva Stejskalová

První vydání
ISBN 978-80-87222-09-6
B4U Publishing s.r.o., Minská 13, 616 00 Brno
www.b4upublishing.com

www.knihyprovas.cz

http://www.b4upublishing.com/M02/fBook_Detail.aspx?BokID=96&Lang=CZ&CatID=4

Text na obalu knihy:

Jedna z nejzajímavějších kapitol druhé světové války – špionážní bitva o kód německého šifrovacího stroje Enigma – přichází v doposud nejlepší a nejkomplexnější knize, která na toto téma byla napsána. Kniha čtenáře provede kompletním sledem všech historických událostí, jež se kolem šifrovacího stroje rozpoutaly. Kniha podává velmi podrobný a souvislý popis historických událostí, které se vztahují k prolomení šifrátoru Enigma, a doplňuje ho o vyprávění životních příběhů protagonistů tohoto fascinujícího příběhu, který patřil mezi rozhodující okamžiky druhé světové války. Velmi podrobně a plasticky popisuje příběhy námořníků, kteří s nasazením vlastních životů získali důležitý šifrový materiál z německých ponorek. Publikaci ocení i odborník, protože v dodatcích ke knize jsou detailně shrnuty postupy, jichž bylo využíváno pro zisk nastavení šifrátoru, a to včetně některých méně známých (jako například metoda charakteristik, řádkování, puntíkování, banburismus).

Pavel Vondruška, kryptolog

Ukázka z knihy - Dodatek 4

Cillis

Chyby Němců známé jako cillis, zmíněné v kapitole 8, umožnily kryptologům v Bletchley Parku číst leteckou Enigmu počínaje 22. květnem 1940 včetně. Říká se, že si jich všiml Dilly Knox v lednu 1940 v době, kdy již zprávy šifrované Enigmou byly prolamovány. Tyto chyby byly využívány před výpadkem v dešifrování 1. května 1940, aby se urychlilo dešifrování pomocí perforovaných listů.

Podstata cillis se dá nejlépe vysvětlit na dlouhých německých zprávách, které byly rozděleny na několik částí. Německé předpisy nepřipouštěly zprávy delší než 250 znaků. Knox si všiml, že je-li nastavení rotorů řekněme ABC, operátor končící šifrování první části své zprávy použije stejné nastavení jako výchozí polohu (definována v dodatku 1) pro další část zprávy. V takovém případě, kryptologům stačilo, aby se podívali, jaká byla nešifrovaná poloha rotorů pro druhou část zprávy, a věděli, která písmena byla v okénkách nad rotory, když bylo zašifrováno poslední písmeno první části. Tato skutečnost spolu s tím, co je řečeno v následujícím odstavci, umožnila kryptologům dopracovat se písmen, která se ukazovala v okénkách nad rotory, když bylo zašifrováno první písmeno první části zprávy. Pro zjednodušení budu tato písmena nazývat nastavení zprávy, přestože jak bylo uvedeno v dodatku 1, části 2, kryptologové neznali nastavení samotných rotorů, dokud se nepropracovali k nastavení kroužků na rotorech například s použitím Herivelova tipu popsaného v kapitole 8.

Při určování nastavení první části zprávy uvažovali kryptologové následovně: Znali písmena, která se objevila v okénkách nad rotory při zašifrování posledního písmena první části zprávy. Dejme tomu, že šlo o písmena ABC. Věděli také, kolik písmen tvoří první část zprávy, protože Němci tuto informaci uváděli na jejím začátku. Mohlo to být například 240 písmen. Na základě těchto údajů pak kryptologové jednoduše zjistili nastavení první části zprávy tak, že otočili rotory o 240 míst zpět od ABC.

Byla zde nicméně jistá komplikace. Ironií osudu právě tato komplikace, jež měla prolomení šifry ztížit, pomohla kryptologům při využívání cillis a odkrývání pořadí rotorů pro daný den. Poloha, ve které se rotory po otočení o 240 pozic zpět, závisela na tom, které rotory byly v Enigmě nasazeny. Každý z pěti rotorů, které měla k dispozici obsluha letecké a armádní Enigmy, měl jiné „krokové polohy“. Krokovou polohu udávalo písmeno abecedy, které se objevilo v okénku nad rotorem, když byla dalším stisknutím klávesnice aktivována kroková poloha rotoru. Při dosažení krokové polohy určitého rotoru zářez na jeho obvodu zajistil, aby se rotor v poloze vlevo od něj při dalším stisknutí klávesy pootočil o 1/26 plné otočky. Kroková poloha rotoru 1 mohla být například písmeno Q a rotoru 2 písmeno E. Pokud kryptologové při použití postupu popsaného v předešlém odstavci nevěděli, které rotory jsou uvnitř stroje Enigma, nemohli určit přesné nastavení první části zprávy. Mohli pouze předpokládat, že jde o jedno z omezeného počtu s možných nastavení. Atd…….

Poznámka:

Tyto německé chyby vešly ve známost jako cillis, protože jedno z prvních nastavení zprávy zjištěné tímto způsobem bylo CIL. Slovo cilli vzniklo zkřížením CIL a „Silly“ (hloupý), čímž kryptologové v Bletchley Parku vyjádřili, co si o operátorech Enigmy, kteří dělají takové chyby, myslí. Operátoři je navíc neustále opakovali, přestože obě zmíněné chyby v tomto dodatku jmenovitě zakazovaly německé manuály k Enigmě…..

D. Pracovní příležitost (World Startup Project)

Zbynek Loebl, zbynek@odrexchange.com

Hledáte zajímavou pracovní příležitost?

My zase hledáme schopné programátory / vedoucího týmu, kteří mají zkušenosti s rozsáhlými web aplikacemi. Jde o trvalý pracovní poměr s dlouhodobou perspektivou.

Nabízíme účast na nově připravovaném „stratup projektu se světovou působností“, který se dostal po důkladné přípravě do stádia realizace. Místa budou nadstandardně placena.

O projektu se lze více dozvědět zde:
http://www.odrexchange.com/

Těšíme se na spolupráci!

Kontakt pro zájemce je Zbynek Loebl, zbynek@odrexchange.com

E. O čem jsme psali v listopadu a prosinci 1999 – 2011

Crypto-World 11/2005

Crypto-World 11/2006

Crypto-World 11/2007

Crypto-World 11/2008

Crypto-World 11/2009

Crypto-World 11/2010

Crypto-World 12/1999

Crypto-World 12/2000

Příloha : teze.zip - zkrácené verze prezentací ÚOOÚ použité při předložení tezí k Zákonu o elektronickém podpisu (§6, §17) dne 4.12.2000 a teze příslušné vyhlášky.

Crypto-World Vánoce/2000

Crypto-World 12/2001

Příloha: uloha7.wav

Crypto-World 12/2002

Příloha : EAL4.jpg (certifikát operačního systému W2k podle CC na EAL4)

Crypto-World 12/2003

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