Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 14, číslo 7-8/2012 **1. srpen**

7-8/2012

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1303 registrovaných odběratelů)

Obsah : str.

Příloha: dokument, který měl být odeslán pouze do interní skupiny NISTu pro výběr SHA-3 http://crypto-world.info/casop14/NIST_unikly_dokument.pdf
(více informací viz článek V.Klímy)

A. Andreas Figl – Nestor rakúskej školy kryptológie

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

Obr. 1: Andreas Figl

Meno Andreas Figl v histórii kryptológie doslova vyžaruje svetlo v temnotách každodennosti. Je známy tým, že založil roky pred vypuknutím I. svetovej vojny školu rakúskej kryptoanalýzy a voviedol ju počas tohto vojenského konfliktu k obrovským úspechom. Napísal štandardnú prácu o kryptografii, ktorá bola publikovaná v roku 1926, štúdiu o kryptoanalýze ktorej zverejneniu zabránil len mocensko-administratívny zásah rakúskej vlády a memoáre z pôsobenia počas I. svetovej vojny. Počas II. svetovej vojny bol najatý na prácu kryptoanalytika pre nacistické Nemecko, ale predtým než bol prepustený, Tretej ríši slúžil len 18 mesiacov.

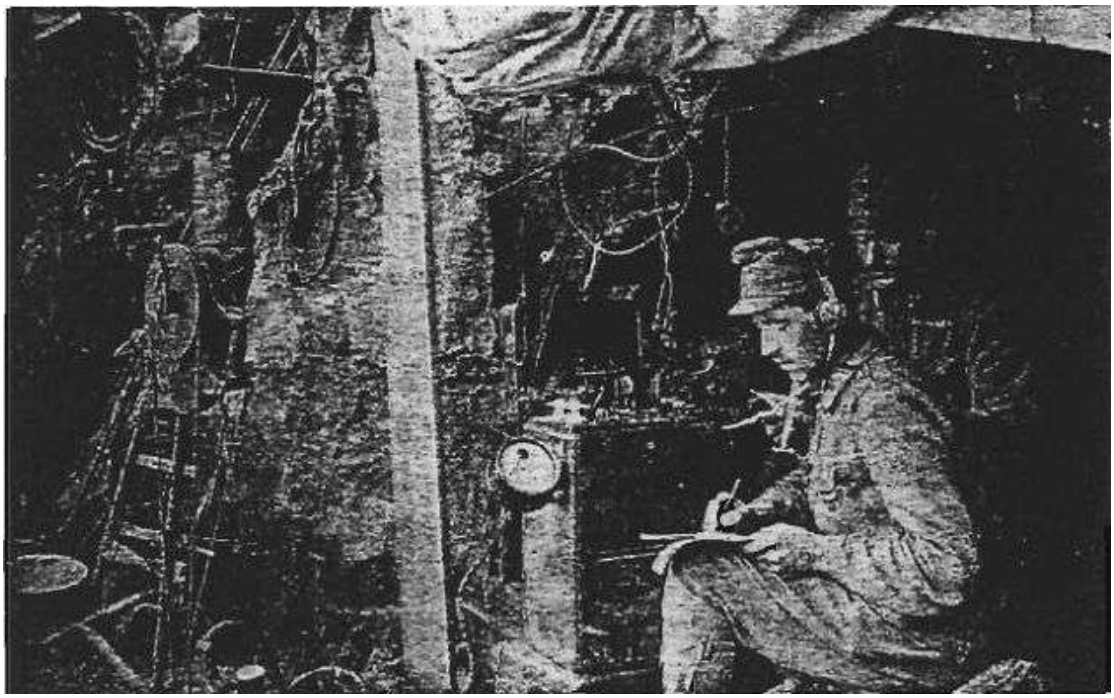
Celé desaťročia boli jedinými informáciami o jeho vynikajúcich úspechoch pokusy o stručný náčrt, nachádzajúce sa v knihe o histórii rakúskej spravodajskej služby v I. svetovej vojne napísanej plukovníkom **Maxom Rongem** a v nepublikovaných memoároch generála **Augusta Urbanskiho von Ostrymiec**. Bolo však isté, že si zaslúžil, aby o ňom bolo napísané podrobnejšie dielo. Narodil sa vo Viedni dňa 22. júna 1873. Svoje dôstojnícke vojenské vzdelanie získal v kadetnej škole v Terste, nachádzajúcom sa vtedy v rakúsko-uhorskej monarchii a v roku 1893 získal hodnosť poručíka. V mnohonárodnostnom rakúsko-uhorskom cisárstve, v ktorom sa hovorilo niekoľkými jazykmi, ako o ňom hovoria jeho služobné záznamy, dokonale ovládal nemčinu (jeho materinský jazyk) a srbochorvátštinu, taliančinu na celkom vyhovujúcej úrovni pre vojenskú službu a francúzštinu "dobre". V každoročne vydávaných správach sa o ňom píše pochvalne tým spôsobom, akým sa aj o všetkých dôstojníkoch pokým sa neosvedčili ako úplne nevyužiteľní: v roku 1908 sa o ňom písalo ako o "*pokojný, seriózny, čestný,...vojensky veľmi schopný,...znalý v tom ako hodnotiť svojich podriadených a inšpirovať v nich dôveru.*" Jeden pôvodný komentár je že "*vzbudzuje dojem že má jasnú hlavu.*" Ale potom odo dňa 23.mája 1909 bol zbavený vojenskej služby kvôli nehode, pri ktorej oslepol na jedno oko.

Ako sme už spomenuli, existujú dva rozličné príbehy o tom, aké boli začiatky rakúskej modernej kryptoanalýzy.

Prvý pochádza od plukovníka Maxa Rongeho, šéfa rakúskej spravodajskej služby v I. svetovej vojne a ktorý sa obzvlášť zaoberá lúštením kódov a šifier.

V rámci svojich spomienok píše, že v roku 1908 stáli Rakúsko-Uhorsko a Rusko vzájomne proti sebe z dôvodu panslavizmu na Balkáne a preto rakúske námorníctvo začalo zachycovať ruské správy ktoré vysielala a prijímala rádiová stanica v meste vtedy nazývanom po taliansky Antivari (resp. dnešnom Bare, ktorý je súčasťou Čiernej hory). Predstavitelia rakúskeho námorníctva prišli k Rongemu, ktorý bol vtedy kapitánom a veliteľom tzv. **Kundschaftsgruppe**, zbernej jednotky v rámci Evidenzburo, spravodajsko-analytickej agentúry generálneho štábu. Ronge našiel v spisoch svojej jednotky zahrabanú šifru ruského konzulátu, ktorá mu umožnila začať čítať ruské odposluchy.

Následne za pomoci špionáže rozšíril lúštiteľské schopnosti svojho oddelenia aj na kryptogramy zo susedného Srbska, ruského spojenca. Keď sa v roku 1911 dvaja zo susedov Rakúsko-Uhorska, Osmanská ríša a Taliansko, rozhodli ísť do vojny o Lýbiu, ‘‘*so zachytenými depešami sa priam roztrhlo vrece*’’, ako so značným pocitom hrdosti napísal Ronge. Kryptoanalytická práca čoskoro presiahla jeho možnosti, ale na pomoc dokázal získať istého nám dobre známeho dôstojníka: Figla. Ďalšie rozprávanie pochádza od neskoršieho Rongeho šéfa Urbanskiho, ktorý bol v tom čase vedúcim **Evidenzburo**. Urbanski tvrdil, že už dlho pred I. svetovou vojnou odhadol ako dôležitým by sa lúštenie kódov a šifier mohlo stať.



Obr. 2: Rakúsko-uhorská vojenská jednotka rádiového odposluchu v bojovom nasadení na fronte Isonzo, rok 1917

Hľadal pomoc u kryptoanalytikov Ministerstva zahraničia. Oni túto ponuku taktne odmietli. Keď zistil, že jeho jednotka by sa mohla kryptoanalýzu naučiť sama, spýtal sa svojich podriadených či by mu s tým nepomohli. Kapitán Hubka odporúčal jedného zo svojich bývalých spolubojovníkov z pluku, čuduj sa svete, rovnako ním bol Figl. Urbanski teda priviedol dôstojníka vo výslužbe naspäť, a tento v roku 1911 zaútočil na talianské odposluchy. Urbanski potom túto jednotku rozšíril tým, že do nej angažoval rusky hovoriaceho dôstojníka.

Figlov vlastný rukopis z roku 1924 s názvom ‘‘*Vojnové pamäti z I. svetovej vojny – nem. Kryptographische Erinnerungen aus dem Weltkrieg*’’ nedáva zásluhy za začiatky modernej rakúskej vojenskej kryptoanalýzy ani jednému či druhému. Avšak stále platí to, že úspešný začiatok nezabezpečí aj budúcnosť rakúskej vojenskej kryptoanalýzy. Mnohí dôstojníci pri oceňovaní hodnoty lúštenia kódov a šifier ostávali skeptickí. V polovici júna roku 1914, ako píše Figl, vedúci Evidenzburo, plukovník Oskar von Hranilovic, si povolal Figla do svojej kancelárie. Podal mu zväzok okolo 40 zachytených správ pochádzajúcich z rozličných krajín a povedal mu: ‘‘Ak tieto správy nedokážete rozlúštiť do 20. septembra, od toho dňa budem musieť ukončiť vaše pôsobenie v tejto jednotke.’’ Dňa 28. júna bol v Sarajeve zavraždený rakúsky korunný princ, vďaka čomu vypukla I. svetová vojna.

Figl vo svojich pamätiach pripomína skvelý príklad toho, čo vtedy vojenská spravodajská služba dokázala zistiť z na prvý pohľad nevinne vyzerajúcej a vlastne zbytočnej správy.

Rakúšania zachytili 15. júla 1915 rádiovú správu, ktorá obsahovala blahoželania od dôstojníkov zo štábu XII. zboru (zóna Carnia) náčelníkovi generálneho štábu generálovi Luigi Cadornovi pri príležitosti jeho menín:

éu da év == li 21 ore 2 r 20 == Comando presidio Udine per Sua Eccellenza generale C A D O R N A. A nome mio e tutti gli ufficiali della zona Carnia prego Vostre Eccellenza accogliere voti augurali pel Suo onomastico che si identificano con quelli per la grandezza della patria. Generale LEQUIO == éu da év--

Figl jasne ukázal, čo Rakúšania dokázali odvodiť z tohto bezstarostného rádiového vysielania:

1. éu je volací znak Comando supremo, vrchného velenia;
2. év je volací znak stanice zo zóny Koruta, identickej s XII. armádnym zborom;
3. Veliteľom spomínanej Korutánskej zóny je generál Lequio;
4. Cadorna priezvisko najvyššieho veliteľa;
5. Nachádza sa v Udine;

6. Tolmezzo, čo je poloha stanice év podľa adresára volacích znakov patriacich talianskému štábu je taktiež poloha veliteľstva zóny Koruta - Comando della zona Carnia.

Takže dokonca úplne bežné detaily môžu znamenať zisk hodnotných informácií, najmä ako poukazuje Figl, že otvorená zrada bola u Talianov takmer vylúčená. Môžeme spomenúť aj ďalšie príklady úplne neuveriteľnej bezstarostnosti Talianov. Tak napríklad Taliani používali aktuálne kľúče (zvyčajne už Rakúšanom známe) na zašifrovanie nových kľúčov pre ďalšie obdobie a následne ich poslali vzduchom pomocou rádiového vysielania. Dennodenne sa na lekársky štáb posielali lekárske správy využitím presne rovnakého slovosledu a identických slov, neustále sa menili iba počty rôznych úmrtí.

a. Cifrario tascabile.

•	a b c d e f g h i	•	j k l m n o p q r	•	s t u v w x y z	•	0 1 2 3 4 5 6 7 8 9	•
a	10 11 12 13 14 15 16 17 18	a	19 20 21 22 23 24 25 26 27	a	28 29 30 31 32 33 34 35	a	36 37 38 39 40 41 42 43 44 45	a
b	11 12 13 14 15 16 17 18 19	b	20 21 22 23 24 25 26 27 28	b	29 30 31 32 33 34 35 36	b	37 38 39 40 41 42 43 44 45 10	b
c	12 13 14 15 16 17 18 19 20	c	21 22 23 24 25 26 27 28 29	c	30 31 32 33 34 35 36 37	c	38 39 40 41 42 43 44 45 10 11	c
d	13 14 15 16 17 18 19 20 21	d	22 23 24 25 26 27 28 29 30	d	31 32 33 34 35 36 37 38	d	39 40 41 42 43 44 45 10 11 12	d
e	14 15 16 17 18 19 20 21 22	e	23 24 25 26 27 28 29 30 31	e	32 33 34 35 36 37 38 39	e	40 41 42 43 44 45 10 11 12 13	e
f	15 16 17 18 19 20 21 22 23	f	24 25 26 27 28 29 30 31 32	f	33 34 35 36 37 38 39 40	f	41 42 43 44 45 10 11 12 13 14	f
g	16 17 18 19 20 21 22 23 24	g	25 26 27 28 29 30 31 32 33	g	34 35 36 37 38 39 40 41	g	42 43 44 45 10 11 12 13 14 15	g
h	17 18 19 20 21 22 23 24 25	h	26 27 28 29 30 31 32 33 34	h	35 36 37 38 39 40 41 42	h	43 44 45 10 11 12 13 14 15 16	h
i	18 19 20 21 22 23 24 25 26	i	27 28 29 30 31 32 33 34 35	i	36 37 38 39 40 41 42 43	i	44 45 10 11 12 13 14 15 16 17	i
j	19 20 21 22 23 24 25 26 27	j	28 29 30 31 32 33 34 35 36	j	37 38 39 40 41 42 43 44	j	45 10 11 12 13 14 15 16 17 18	j
k	20 21 22 23 24 25 26 27 28	k	29 30 31 32 33 34 35 36 37	k	38 39 40 41 42 43 44 45	k	10 11 12 13 14 15 16 17 18 19	k
l	21 22 23 24 25 26 27 28 29	l	30 31 32 33 34 35 36 37 38	l	39 40 41 42 43 44 45 10	l	11 12 13 14 15 16 17 18 19 20	l
m	22 23 24 25 26 27 28 29 30	m	31 32 33 34 35 36 37 38 39	m	40 41 42 43 44 45 10 11	m	12 13 14 15 16 17 18 19 20 21	m
n	23 24 25 26 27 28 29 30 31	n	32 33 34 35 36 37 38 39 40	n	41 42 43 44 45 10 11 12	n	13 14 15 16 17 18 19 20 21 22	n
o	24 25 26 27 28 29 30 31 32	o	33 34 35 36 37 38 39 40 41	o	42 43 44 45 10 11 12 13	o	14 15 16 17 18 19 20 21 22 23	o
p	25 26 27 28 29 30 31 32 33	p	34 35 36 37 38 39 40 41 42	p	43 44 45 10 11 12 13 14	p	15 16 17 18 19 20 21 22 23 24	p
q	26 27 28 29 30 31 32 33 34	q	35 36 37 38 39 40 41 42 43	q	44 45 10 11 12 13 14 15	q	16 17 18 19 20 21 22 23 24 25	q
r	27 28 29 30 31 32 33 34 35	r	36 37 38 39 40 41 42 43 44	r	45 10 11 12 13 14 15 16	r	17 18 19 20 21 22 23 24 25 26	r
s	28 29 30 31 32 33 34 35 36	s	37 38 39 40 41 42 43 44 45	s	10 11 12 13 14 15 16 17	s	18 19 20 21 22 23 24 25 26 27	s
t	29 30 31 32 33 34 35 36 37	t	38 39 40 41 42 43 44 45 10	t	11 12 13 14 15 16 17 18	t	19 20 21 22 23 24 25 26 27 28	t
u	30 31 32 33 34 35 36 37 38	u	39 40 41 42 43 44 45 10 11	u	12 13 14 15 16 17 18 19	u	20 21 22 23 24 25 26 27 28 29	u
v	31 32 33 34 35 36 37 38 39	v	40 41 42 43 44 45 10 11 12	v	13 14 15 16 17 18 19 20	v	21 22 23 24 25 26 27 28 29 30	v
w	32 33 34 35 36 37 38 39 40	w	41 42 43 44 45 10 11 12 13	w	14 15 16 17 18 19 20 21	w	22 23 24 25 26 27 28 29 30 31	w
x	33 34 35 36 37 38 39 40 41	x	42 43 44 45 10 11 12 13 14	x	15 16 17 18 19 20 21 22	x	23 24 25 26 27 28 29 30 31 32	x
y	34 35 36 37 38 39 40 41 42	y	43 44 45 10 11 12 13 14 15	y	16 17 18 19 20 21 22 23	y	24 25 26 27 28 29 30 31 32 33	y
z	35 36 37 38 39 40 41 42 43	z	44 45 10 11 12 13 14 15 16	z	17 18 19 20 21 22 23 24	z	25 26 27 28 29 30 31 32 33 34	z
•	a b c d e f g h i	•	j k l m n o p q r	•	s t u v w x y z	•	0 1 2 3 4 5 6 7 8 9	•

b. Schlüsseln.

Klarschrift: D a s v i e r t e B a t a i l l o n h a t v o n s e i n e r S t e l l u n g a m . . .
Schlüssel: i n m i t t e n m e i n e s l e b e n s w e g
Sigel: 39 31 26 35 12 33 15 23 41 14 26 34 25 42 34 32 30 18 34 39 16 27 22

c. Sigelschrift.

Das 3931 2635 1233 1523 4114 2634 2542 34 hat von seiner 3230 1834 3916 2722 am . . .

Tab. 1: Názorný príklad tabuľky a šifrovania pomocou tzv. *cifrario tascabile*, „vreckovej šifry“

Z dochovaných útržkov historickej dokumentácie je známe, že Taliani používali tri základné skupiny šifrovacích systémov v niekoľkých variant ách:

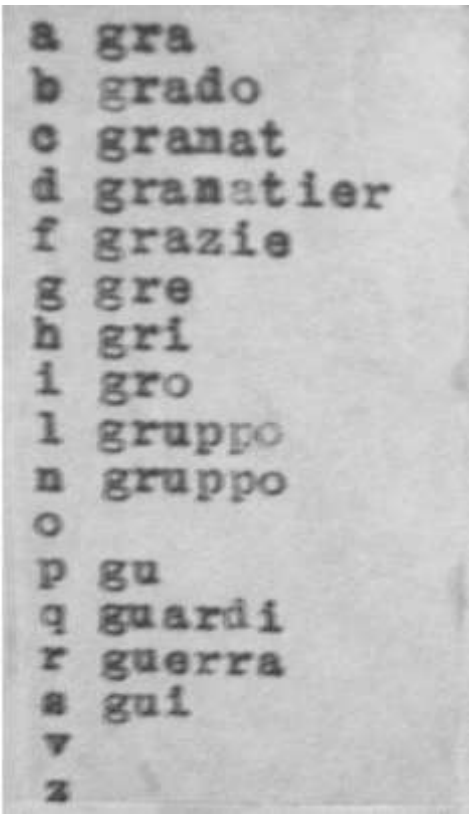
cifrario servizio: ‘‘služobná šifra’’, používaná pri komunikácii medzi veliteľskými štábmi
cifrario tascabile: ‘‘vrecková šifra’’ určená pre komunikáciu na frontových líniách
cifrario rosso: ‘‘červená šifra’’, používaná pri komunikácií na úrovni prísne tajné v rámci generálneho štábu.

Tzv. **cifrario tascabile** nebola v rámci vtedajších vojenských kryptosystémov nič zvláštne, jednalo sa o šifru typu Vigenére v ktorej boli k abecede otvoreného textu pripojené číslice 0 až 9 a ktorej šifrová abeceda pozostávala z čísel 10 až 45 v normálnom poradí, preto jej rozlúštenie bolo hračkou a rakúsko-uhorským kryptoanalytikom trvalo zvyčajne nie menej než tri až štyri hodiny, aby identifikovali a úspešne prelomili jednu či dve správy zašifrované týmto systémom.

Cifrario rosso - červená šifra bola vlastne kódová kniha o približne 240 stranách, kódové slová usporiadané abecedne ale (úmyselne) nie tematicky s dodatočným zoznamom mien osôb a názvov miest.

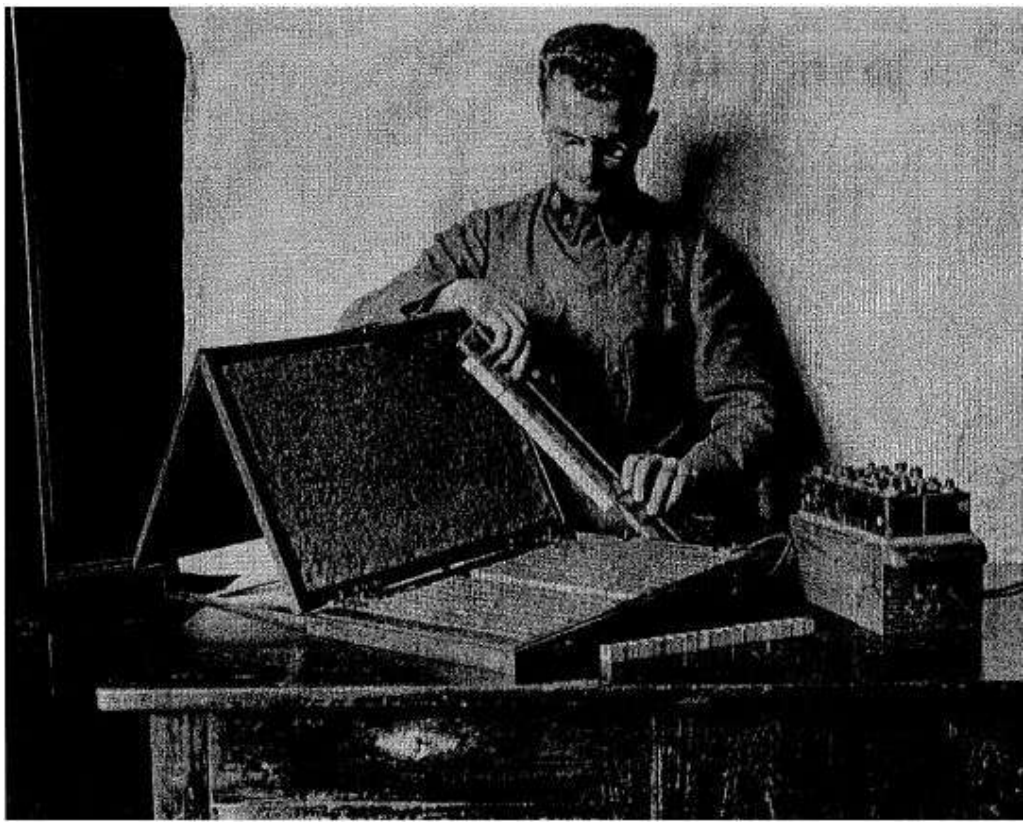
Svoj názov si požičala od červenej farby jej dosiek, v ktorých bola zviazaná. Kód, poprvýkrát publikovaný v roku 1898, bol na tie časy moderným, ušitým na mieru pre potreby organizácie v talianskej armáde. Jeho užitočnosť sa ukázala počas tzv.**Tripoliskej vojny** v rokoch 1911–1912. Kuriozitou tejto šifry bolo, že ako kódový výraz sa v nej nachádzala aj táto veta: „*uši a nosy odrezané líbyjským vojakom*„. Po niekoľkých vylepšeniach v roku 1915 sa často používala aj v I. svetovej vojne. Figl ju však charakterizoval ako zastaranú a nebezpečnú.

Tzv. **cifrario servizio**, služobná šifra, bola v zásade niečo medzi kódom a šifrou, pretože ponúkala šifrantom obe metódy ako správne zašifrovať správu. Bola zostavená na princípe dvojrozmernej tabuľky typu 17x17, pričom jej súradnice boli označené tzv. skrátenou talianskou abecedou, bez písmen E, J, K, M, T, U, W, X a Y (Tab. 2).



Tab. 2: Príklad políčka tzv. cifrario servizio, pozostávajúceho zo 17 podriadkov. Podriadky *o, v* a *z* sa nepoužívajú.

Kľúčom bolo aktuálne poradie tých označujúcich znaky a pravidelne sa menil. Každé políčko na súradnicovej pozícii sa nazývalo ‘‘*položka tabuľky*’’ resp. krátko ‘‘*položka*’’. Táto obsahovala na ďalších riadkoch (‘‘*podriadkoch*’’) otvorený text, ktorých bolo najmenej dva a nanajvýš sedemnásť, v závislosti na použitej verzii. Pre uľahčenie procesu lúštenia tohto kryptosystému bol vymyslený tzv. **Scheubleho aparát,** čo bola vlastne mechanicky jednoduchá kryptoanalytická pomôcka (predpokladá sa, že jeho názov pochádza, i keď sa nedochoval žiadny dokument, ktorý by sa dal použiť ako definitívny dôkaz, že zariadenie, bolo vynájdené jedným z najúspešnejších a najtvorivejších lúštiteľov a žiakov majora Figla poručíkom (neskôr kapitánom) Hugom Scheublem pôsobiacim v rámci veliteľstva 10. Armády na stanici vo Villachu, Korutánsku).



Obr. 3: Dobová fotografia zariadenia (okolo r. 1915) na ktorej je znázornené že bloky sa dali rozoberať postupne po riadkoch. Pravdepodobne je na nej aj sám Scheuble. Výložky na golieri patria poručíkovi telegrafného pluku, čo môže byť nepriamy dôkaz

Kryptoanalýza sa teda mala stať jedným z hlavných zdrojov rakúsko-uhorskej vojenskej rozviedky a od apríla 1917 sa organizácia, ktorá produkovala takéto cenné informácie, rozrástla do viacerých sekcií. K tzv.**Evidenzgruppe** pri Generálnom štábe bola pripojená tzv. **Chiffrengruppe I.**, pod vedením kapitána de Carla a **Chiffrengruppe II.**, spadajúcej pod kapitána Richarda Immeho. Teoreticky ale, podľa plukovníka Rongeho (ktorý velil obom)

bola "skutočnou" rakúsko-uhorskou spravodajskou službou tzv. **Nachrichtenabteilung** pri generálnom štábe, sídliaca v Badene. Jedna z jej piatich divízií bola tzv. **Kriegschiffregruppe** ("Vojnová šifrová skupina"), ktorú viedol vtedajší nadporučík **Hermann Pokorny**, skvelý kryptoanalytik, ktorý ako sme písali v predošlom článku, dokázal rozlúštiť krátko po vypuknutí vojny prvý ruský šifrovaný telegram a ktorý sa neskôr stal vedúcim Evidenzgruppe. **Kriegchiffregruppe** bola rozdelená do troch sekcií: Talianskej sekcie, ktorej velil vtedajší major **Andreas Figl** (ktorý bol neskôr povýšený na plukovníka), Rumunskej pod velením kapitána **Kornelia Savu** a Ruskej, pod kapitánom **Viktorom von Marchesetti**. Zásobovanie zachytenými telegramami zaobstarávali tri hlavné stanice rádiového odposluchu, prezývané Rongem tzv. **Penkala** (označované podľa obchodnej značky firmy, ktorú založil rodák zo slovenského Liptovského Mikuláša, vynálezca Eduard S. Penkala, vlastniacej továreň na ceruzky, na ktorej bola vyobrazená hlava s ceruzkou za obrovským uchom): Rakúsko-Západ, pokrývajúca talianský sektor; Rakúsko-Sud, rumunský a Rakúsko-Nord, ruský. Celý komplex sa neoficiálne označoval názvom "***Dechiffrierdienst***".

Obr. 4: Reklamný leták firmy Penkala na ceruzky a plniace perá

(http://elacd.carnet.hr/index.php/Datoteka:Penkala.jpg**)**

A týmito skvelými úspechmi rakúsko-uhorskí kryptoanalytici, doplnení ešte o spojencov z Nemecka, pomohli armádam Ústredných mocností zastaviť obrovskú ruskú útočnú vojnovú mašinériu. A na južnom fronte rakusko-uhorskí vojaci porazili Talianov v rozhodujúcej 12.tej bitke o Isonzo, všeobecne známej pod názvom Caporetto. Figl považoval za jedno z pre neho najväčších zadosťučinení neúmyselný kompliment pochádzajúci zo správy povojnovej talianskej vyšetrovacej komisie o spôsobených stratách:‘‘*nepriateľ poznal všetky naše šifry, a to aj tie najtajnejšie a najdôležitejšie.*’’

Po porážke Rakúska-Uhorska Figl získal prácu u národnej polície, pracujúc v alebo v spolupráci s Kriminalistickým inštitútom, pravdepodobne preto, že jeho vedecký riaditeľ, Dr.

Siegfried Turkel, sa zaujímal o kryptológiu: neskôr bol autorom solídnej, dobre ilustrovanej knihy o šifrovacích strojoch. V roku 1924 Figl spísal svoje memoáre pod názvom ‘‘**Kryptographische Erinnerungen aus dem Weltkrieg**’’ (‘‘*Kryptografické pamäti zo svetovej vojny*’’) a ktoré vyšli len prednedávnom (v roku 2011) aj tlačou. V týchto sa popisovali hlavné rakúsko-uhorské úspechy pri rozlúštení šifier nepriateľa—hoci bez kryptoanalytických detailov—a ich dopad na vojnové udalosti. Nikdy však neboli publikované. V roku 1926 samozrejme Figl uverejnil prvú z dvoch resp. troch plánovaných kníh o kryptológii pod záštitou Kriminalistického inštitútu. Jej názov bol „*Systeme des Chiffrierens“* a celkovo na 243 stranách popisovala kryptosystémy a ich použitie. Jej 46 technických dodatkov, vytlačených separátne a zasunutých do obálky prilepenej k zadnému obalu, poskytlo viacej informácií, obzvlášť detaily o šifrách používaných počas vojny, než jej často rozvláčny samotný text. Kniha pomáhala poukázať na úspechy Rakúsko-Uhorska v kryptoanalýze, ale neposkytovala detaily o tom, aké to boli resp. akým spôsobom k nim došlo. Toto, ako sa zdá, bolo naplánované do budúceho zväzku pod názvom ‘‘*Systeme des Dechiffrierens.*’’


Wissenschaftliche Veröffentlichungen des Kriminalistischen Laboratoriums der Polizeidirektion Wien

SYSTEME
DES CHIFFRIERENS

von

A. FIGL
Oberst und Regierungsrat

GRAZ 1926

Verlag von Ulr. Mosers Buchhandlung (J. Meyerhoff)

Obr. 5: Predná strana prvého zväzku *Systeme des Chiffrierens*

Je zrejmé, že sa rozhodol pre napísanie novej obsiahlej knihy hlavne z dôvodov hlbokého presvedčenia o jej nutnosti, pretože všetka dostupná literatúra bola už niekoľko desaťročí zastaralá, neúplná a napísaná nesystematicky. Takže jeho zámerom bolo zozbierať všetky svoje znalosti a praktické skúsenosti získané počas mnohých rokov svojej kariéry kryptológa a pretaviť ich v rámci silnej systematickej a vedecky štruktúrovanej schémy do značne erudovane vybavenej knihy.

Členenie jeho knihy vyzerá nasledovne:

Úvod

- viditeľné a neviditeľné tajné písma,

- Hranice a štruktúra odboru

- Špeciálne odborné výrazy,

- Literatúra,

I. časť: Písmenové metódy

- Transpozície,

- Substitúcie,

- Mechanické metódy,

- Screening, Testovanie,

- Skrývanie písiem, Steganografia,

II. časť: Slabičné a Slovné metódy

- Špeciálne metódy,

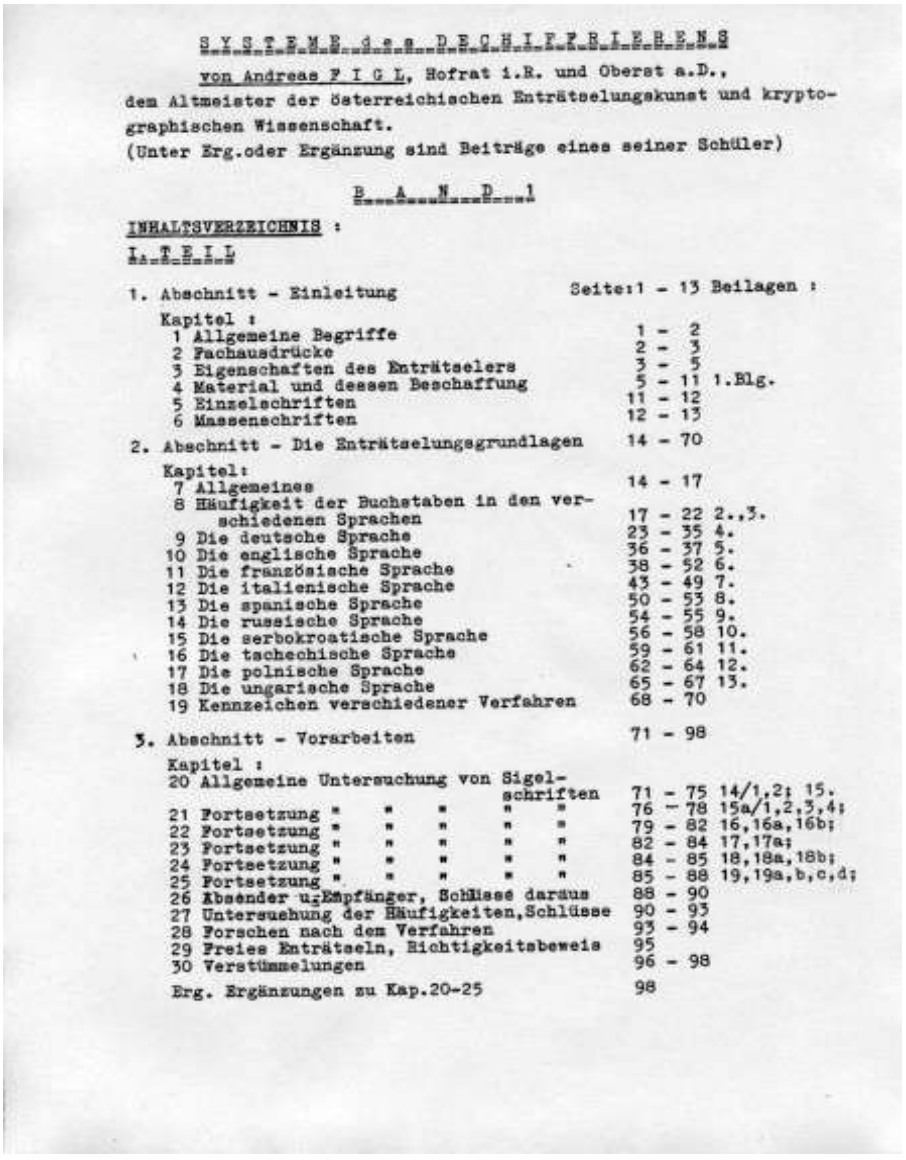
- Heslové tabuľky (povelové, veliteľské, hláskovacie tabuľky)

- Knižné metódy, Kódové knihy.

Dá sa povedať, že Figl nielenže štruktúroval obsah veľmi silne ale taktiež do hĺbky a systematicky rozpracoval všetky detaily. Mnohé staroveké a v jeho dobe viac-menej dobre známe metódy sú popísané s vedeckou presnosťou spolu s ich výhodami, nevýhodami a slabými miestami. Figl už vtedy napríklad popísal šifrovací stroj Enigma a v tomto kontexte prehlásil, že skutočným kryptografickým tajomstvom nie je šifrovacie zariadenie ale iba šifrovací kľúč, čiže malo by sa dodržiavať 2. pravidlo známeho **Kerckhoffsovho princípu**.

Čo sa týka plánovaného druhého zväzku: vydavateľ mal jej rukopis dať do tlače, keď tu zrazu v roku 1927 rakúske ministerstvo obrany vydavateľský proces zastavilo na základe možného ohrozenia národnej bezpečnosti. Figlovi však nevyplatilo ani pfennig a uspokojilo finančné straty vydavateľa iba do výšky nákladov za vysádzanie. Niekoľko neoficiálnych výtlačkov bolo počas II. svetovej vojny dostupných v kryptoanalytickej agentúre nemeckého ministerstva zahraničných vecí, ale nedochovalo sa. V tomto prípade je dôvod zrejmý a dobre

zdokumentovaný. Vydanie druhého zväzku bolo oficiálne zakázané tým samým úradom, v ktorom Figl pracoval ako vládny zamestnanec. V roku 1926, keď bol prvý zväzok jeho knihy zverejnený, pracoval v šifrovacej skupine oddelenia zahraničných vecí Úradu federálneho kancelára a venoval jednu kópiu svojej knihy šéfovi S. Turkelovi, tejto šifrovacej skupiny s osobným venovaním. Reakcia bola strašná. Dôvod pre ňu sa dá nájsť v spôsobe myslenia v rámci štátnej politiky utajovania v tej dobe. Niektoré z popisovaných metód s ich nevýhodami a slabinami boli zrejme stále používané vládnymi zložkami. Preto vtedy reagovali ako ostrieži: skôr hľadeli nechať v utajení slabú metódu dúfajúc tak, že nikdo túto slabinu neodhalí, než hľadať novú bezpečnejšiu metódu. Tak boli značne šokovaní, keď bola teraz táto slabá stránka verejne známa. Avšak nebolo možné vrátiť sa späť, tj. eliminovať už publikovaný prvý zväzok.



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

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

B A N D 1

INHALTSVERZEICHNIS :

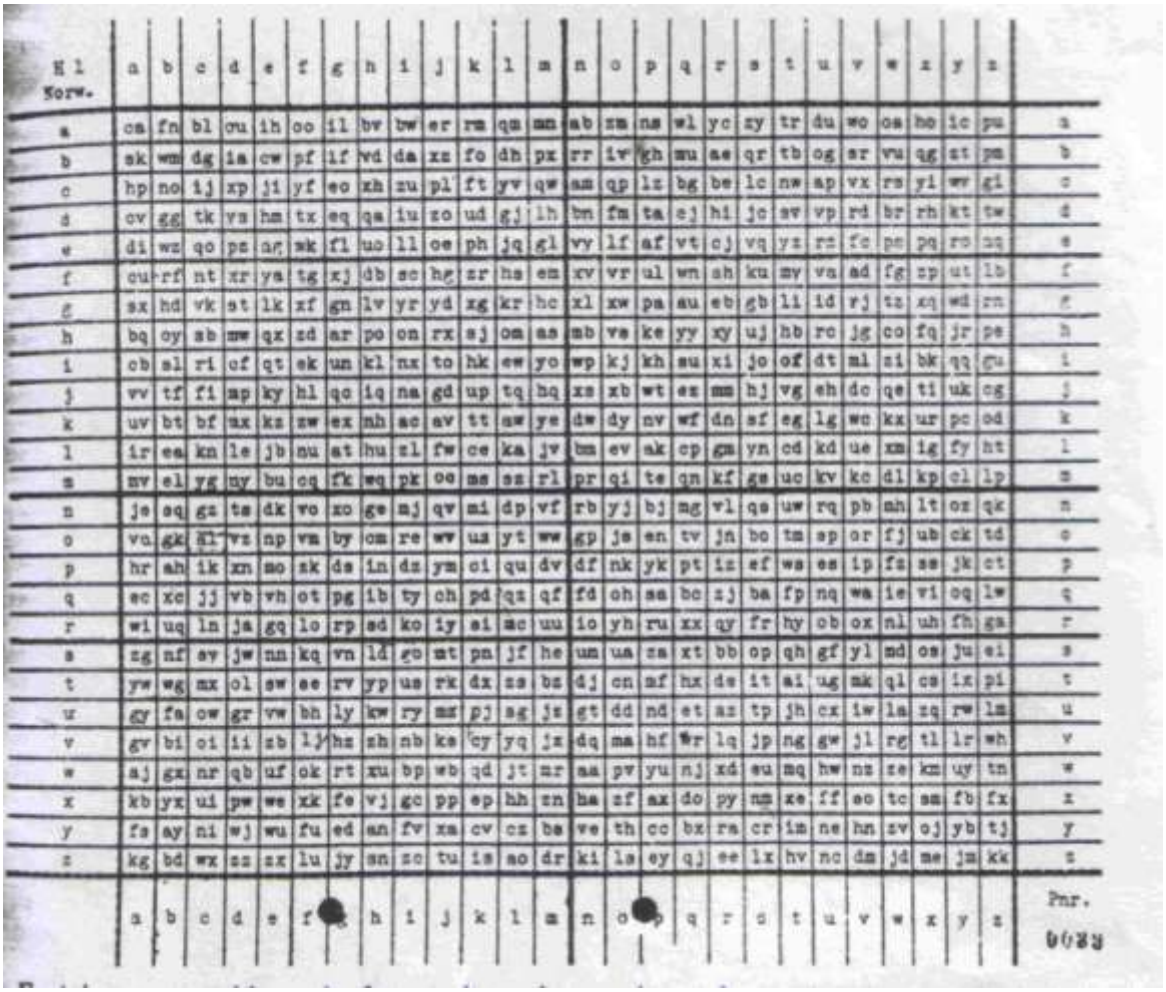
I. T E I L

Obr. 6: Prvá stránka strojopisu Figlovej zakázanej práce *Systeme des Deschiffrierens*

Preto po rýchlej konzultácii s Federálnym ministerstvom pre záležitosti ozbrojených síl (**Bundesministerium fur Heerwesen**) bolo rozhodnuté prinajmenšom zabrániť publikovaniu predtým ohláseného druhého zväzku pod titulom "*Systeme des Deschiffrierens*" (Kryptoanalýza systémov). Je známe, že druhý zväzok už bol pripravený do tlače a že vydavateľ bol pre stratu autorských práv náležite finančne odškodnený.

Rukopis zhotovený na písacom stroji, založený na vlastnoručných Figlových poznámkach, spísaný, znovuzostavený a doplnený v niektorých bodoch žiakom A. Figla je dnes uložený v rukopisnom oddelení Bavorskej štátnej knižnice v Mníchove pod. archívnym označením **Cgm 9304**.

Neskôr keď odišiel do výslužby v kryptológii už nenapísal nič významné. Ku kryptoanalýze sa vrátil v roku 1941, keď rakúsky kryptoanalytik **Albert Langer** navrhol jeho meno oddeleniu zahraničného spravodajstva Nacististickej strany tzv. **Amt VI RSHA** (*Reichssicherheitshauptamt*).



H 1 Korw.	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
a	ca	fn	bl	cu	ih	oo	il	bv	bw	er	rm	qm	mn	ab	zm	ns	wl	yc	xy	tr	du	wo	os	ho	ic	pu	a
b	sk	wm	dg	ia	cw	pf	lf	vd	da	xz	fo	dh	px	rr	iv	gh	mu	ae	qr	tb	og	sr	vu	qg	zt	pm	b
c	hp	no	ij	xp	ji	yf	eo	xh	zu	pl	ft	yv	qw	am	qp	lz	bg	be	lc	nw	ap	vx	rs	yi	wr	gi	c
d	cv	gg	tk	vs	hm	tx	eq	qa	iu	zo	ud	gj	lh	bn	fm	ta	cj	hi	jc	sv	vp	rd	br	rh	kt	tw	d
e	di	wz	qo	ps	ar	mk	fl	uo	ll	oe	ph	jq	gl	vy	lf	af	vt	cj	vq	yz	rz	fc	ps	pq	ro	zq	e
f	cu	rf	nt	xr	ya	tg	xj	db	sc	hg	zr	hs	em	xv	vr	ul	wn	sh	ku	mv	va	ad	fg	zp	ut	lb	f
g	sx	hd	vk	st	lk	xf	gn	lv	yr	yd	xg	kr	hc	xl	xw	pa	au	eb	gb	li	id	rj	tz	xq	wd	rn	g
h	bq	oy	sb	mw	qx	zd	ar	po	on	rx	sj	om	as	mb	ve	ke	yy	xy	uj	hb	ro	jg	co	fq	jr	pe	h
i	cb	sl	ri	cf	qt	ek	un	kl	nx	to	hk	ew	yo	wp	kj	kh	su	xi	jo	of	dt	ml	zi	bk	qq	gu	i
j	vv	tf	fi	mp	ky	hl	qo	iq	na	gd	up	tq	bq	xs	xb	wt	ex	mm	hj	vg	eh	do	qe	ti	uk	cg	j
k	uv	bt	bf	ax	ks	zw	ex	nh	ac	av	tt	aw	ye	dw	dy	nv	wf	dn	sf	eg	lg	wc	kx	ur	pc	od	k
l	ir	ea	kn	le	jb	nu	at	hu	zl	fw	ce	ka	jv	bm	ev	ak	cp	gm	yn	cd	kd	ue	xm	ig	fy	ht	l
m	nv	el	yg	uy	bu	cq	fk	wq	pk	oo	me	sz	rl	pr	qi	te	qn	kf	ge	uc	kv	kc	dl	kp	cl	lp	m
n	je	aq	gz	te	dk	vo	xo	ge	mj	qv	mi	dp	vf	rb	yj	bj	mg	vl	qs	uw	rq	pb	mh	lt	oz	qk	n
o	vo	gk	fl	vz	np	vm	by	om	re	wv	us	yt	ww	gp	je	en	tv	jn	bo	tm	sp	or	fj	ub	ck	td	o
p	hr	ah	ik	xn	so	zk	ds	in	dz	ym	ci	qu	dv	df	nk	yk	pt	iz	ef	ws	es	ip	fz	se	jk	ct	p
q	ec	xc	jj	vb	vh	ot	pg	ib	ty	oh	pd	qz	qf	fd	oh	sa	bc	zj	ba	fp	nq	wa	ie	vi	oq	lw	q
r	wi	uq	ln	ja	gq	lo	rp	sd	ko	iy	ei	mc	uu	io	yh	ru	xx	qy	fr	hy	ob	ox	nl	uh	fh	ga	r
s	zg	nf	sy	jw	nn	kq	vn	ld	go	mt	pn	jf	he	um	ua	za	xt	bb	op	qh	gf	yl	md	os	ju	ei	s
t	yw	wg	mx	ol	sw	ee	rv	yp	us	rk	dx	zs	bz	dj	cn	mf	hx	de	it	ai	ug	mk	ql	cs	ix	pi	t
u	gy	fa	ow	gr	vw	bh	ly	kw	ry	mz	pj	ag	jz	gt	dd	nd	et	az	tp	jh	cx	iw	la	zq	rw	lm	u
v	gv	bi	oi	ii	xb	lj	hz	zh	nb	ke	cy	yq	jx	dq	ma	hf	tr	lq	jp	ng	gw	jl	rg	tl	lr	wh	v
w	aj	gx	nr	qb	uf	ok	rt	xu	bp	wb	qd	jt	mr	aa	pv	yu	nj	xd	eu	mq	hw	nz	ze	km	uy	tn	w
x	kb	yx	ui	pw	we	xk	fe	vj	gc	pp	ep	hh	zn	ha	zf	ax	do	py	nm	xe	ff	eo	tc	sm	fb	fx	x
y	fs	ay	ni	wj	wu	fu	ed	an	fv	xm	cv	cz	ba	ve	th	cc	bx	ra	cr	im	ne	hn	sv	oj	yb	tj	y
z	kg	bd	wx	sz	zx	lu	jy	sn	zc	tu	is	ao	dr	ki	la	ey	qj	ee	lx	hv	nc	dm	jd	me	jm	kk	z
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	Pnr. 8878

Obr. 7: Šifrovacia tabuľka H-1 bigramovej šifry zostavenej pre rádiovú sieť RSHA v Nórsku

Figl odišiel 2. januára 1940 do Berlína aby pracoval na rádiovej pozorovacej stanici Amt VI. Keď ostatní kryptoanalytici ostali z prijatých šifrovaných správ absolútne zmätení, povráva sa, že Figl si zobral svoju šálku čiernej kávy do zadnej miestnosti a nečakane rýchlo sa z nej vrátil aj s ich riešením. Ale na tomto stanovišti sa lúštili iba systémy vojensky druhotriednych krajín a bolo zrušené v roku 1943.

Okrem týchto povinností sa mal aj významne podieľať na zostavení schém šifrovania volacích znakov (tzv. **bipartitná bigramová substitúcia**, znázornená na obr. 7), ktoré sa používali v rádiovej sieti **RSHA** (*Reichssicherheitshauptamt*) v Nórsku.

Figl sa vrátil do Rakúska 28. júla 1941. Už nikdy viac sa nedostal k lúšteniu šifier a nič viac nenapísal, ale žil, neskôr v Salzburgu, obklopený a vysoko ctený svojimi blízkymi druhmi z rakúskej armády, až do dňa 11. novembra 1967, keď zomrel vo veľmi úctyhodnom veku 95 rokov. Je pochovaný v Salzburgu na Maxglanerskom Cintoríne.

Literatúra:

1. Oberst a.D. Andreas Figl und der k.u.k. Radiohorch- und Dechiffrierdienst : die "*Kryptographischen Erinnerungen*" / Otto J. Horak. Graz: Ares-Verlag, 2011, xviii, 318p. ISBN: 9783902475909

2. Otto J. Horak.*Andreas Figl: Leben und Werk*, 1873–1967.Vol. I:Altmeister der osterreichischen Entratselungskunst und kryptographischen Wissenchaft, Hofrat i.R. und Oberst a.D. Band 3, Johannes Kepler Universitat Linz. Linz: Universitats Verlag Rudolf Trauner, 2005. 303 pp. ISBN: 3–85487–770-X.

3. Otto J. Horak. *Andreas Figl: Leben und Werk*, 1873–1967.Vol. II:Was Ubrig Blieb: Kommentare und Dokumente.Schriftenreihe Geschicht der Naturwissenschaft und der Technik, Band 6. Johannes Kepler Universitat Linz. Linz: Universitats Verlag Rudolf Trauner, 2005. 292 pp. ISBN: 2–85487–790–0.

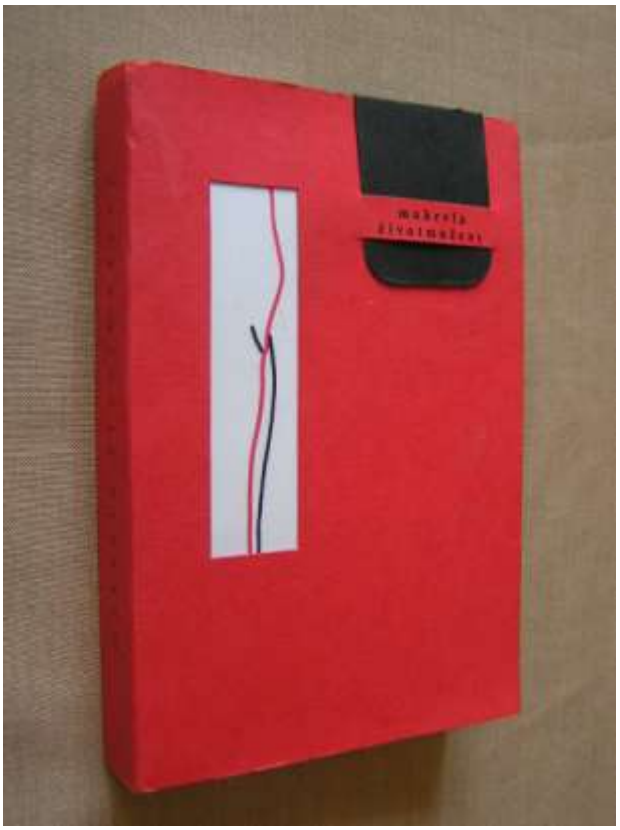
4. David, Kahn, *The Codebreakers*, New York: Scribner, 1996, s. 316-318,

5. Bauer, Friedrich, L.: *Decrypted Secrets, Methods and Maxims of Cryptology*, Berlin: Springer-Verlag, 2007, s.60-61, s.500.

B. Kryptologické perličky 1

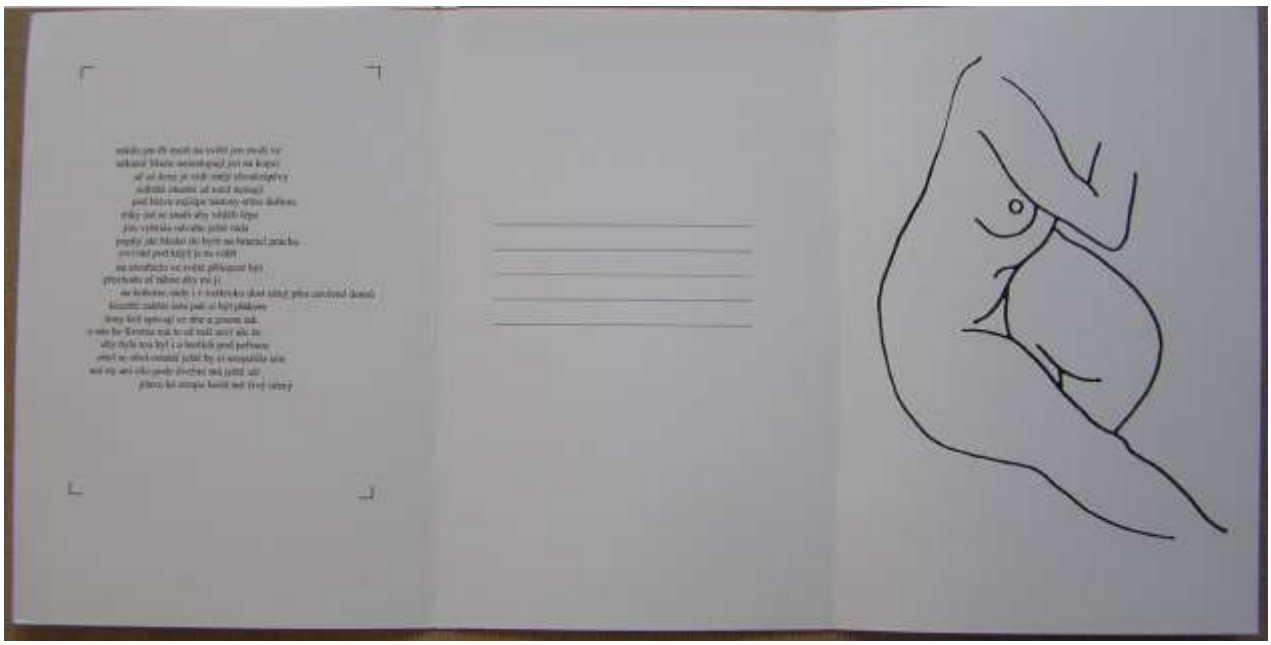
Mgr. Karel Šklíba (karel.skliba@cryptoworld.info)

Perlička první.



V roce 2009 vydalo Nakladatelství Hněvín se sídlem v Mostě pozoruhodnou publikaci. Jedná se o básnickou sbírku nazvanou **Životmuženy** autora uvedeného pod pseudonymem Makrela (viz obr. 1).

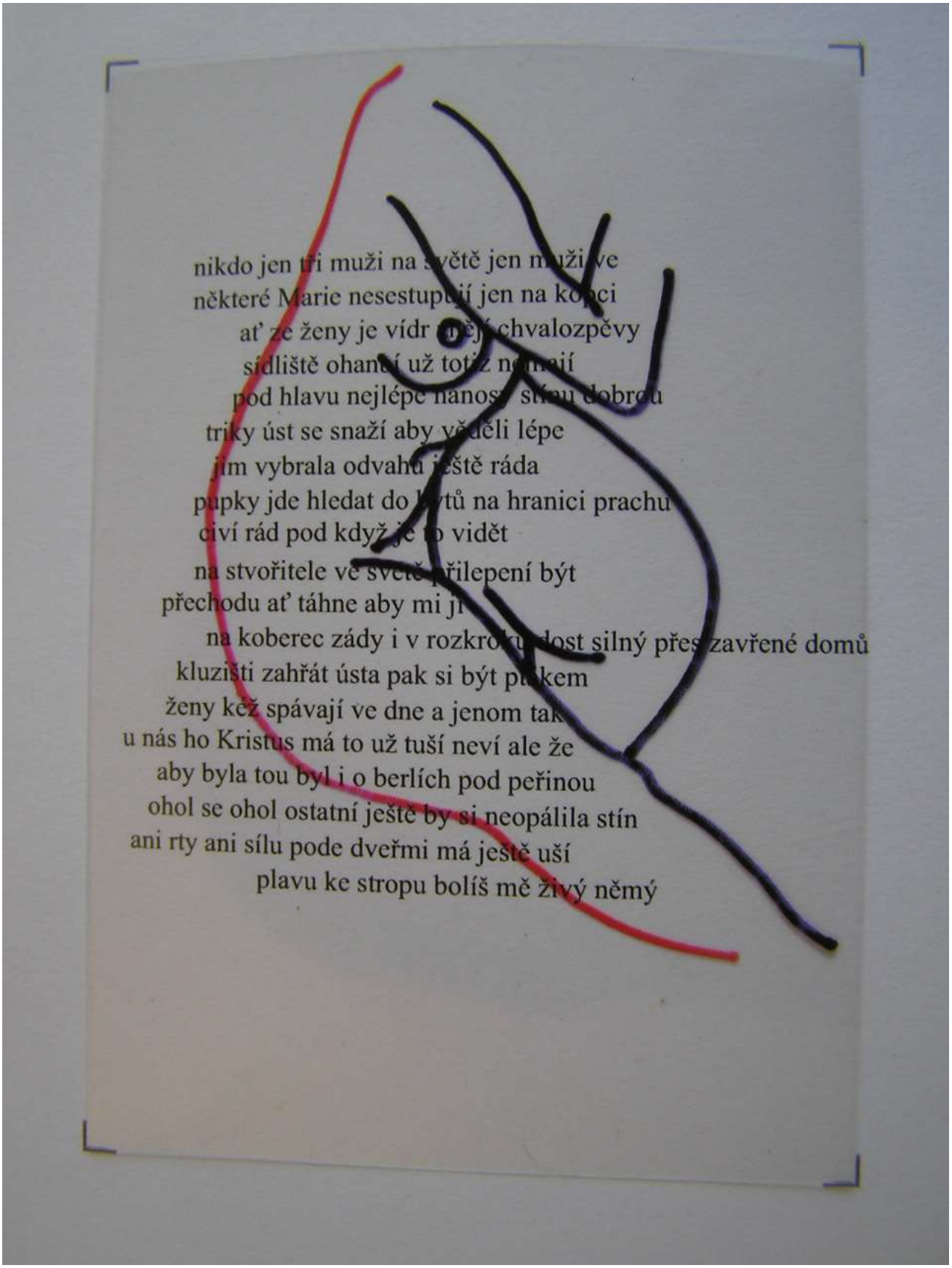
Ilustrace ke sbírce nakreslila Janina Jungmannová a grafickou úpravu vytvořili společně Janina Jungmannová a Makrela. Ilustrace a jejich grafické provedení hrají velmi důležitou úlohu v možnostech čtení textu. Žádný explicitní návod, jakým způsobem by se měl text číst, přiložen není. Vše je ponecháno na důvtipu a fantazii čtenáře, takže je možné, že existují i další jiné varianty čtení textu, než ta, která je popsána zde. 26 básní sbírky je vytištěno na 26 samostatných volných papírových listech dvou velikostí očíslovaných 1 až 26. Prvních 24 básní má název a je opatřeno ilustracemi. Poslední dvě básně



jsou bez názvu a ilustraci nemají. Menší listy jsou přeloženy na polovinu a obsahují pouze báseň a příslušnou ilustraci. Většina listů má však o třetinu větší rozměr, je poskládána na třetiny a kromě básně a ilustrace obsahují i volné řádky, kam si čtenář může vepsat text, který dešifroval kombinací textu básně a ilustrace (viz obr. 2).

Složením každého listu vzniklo 26 samostatných částí sbírky, které jsou uloženy v červeném papírovém pouzdru. V tomto pouzdru je dále umístěno 21 obdélníkových průhledných plastových folií. Na 19 těchto foliích jsou nakresleny dvoubarevně černočerveně tytéž obrázky, jako jsou ilustrace u jednotlivých básní na větších listech (viz obr. 3). Dvě folie jsou prázdné a jsou určeny nejspíše pro vlastní tvorbu čtenáře, který si může vytvořit vlastní obrázky, pomocí nichž vyluští texty ukryté v posledních dvou básních.

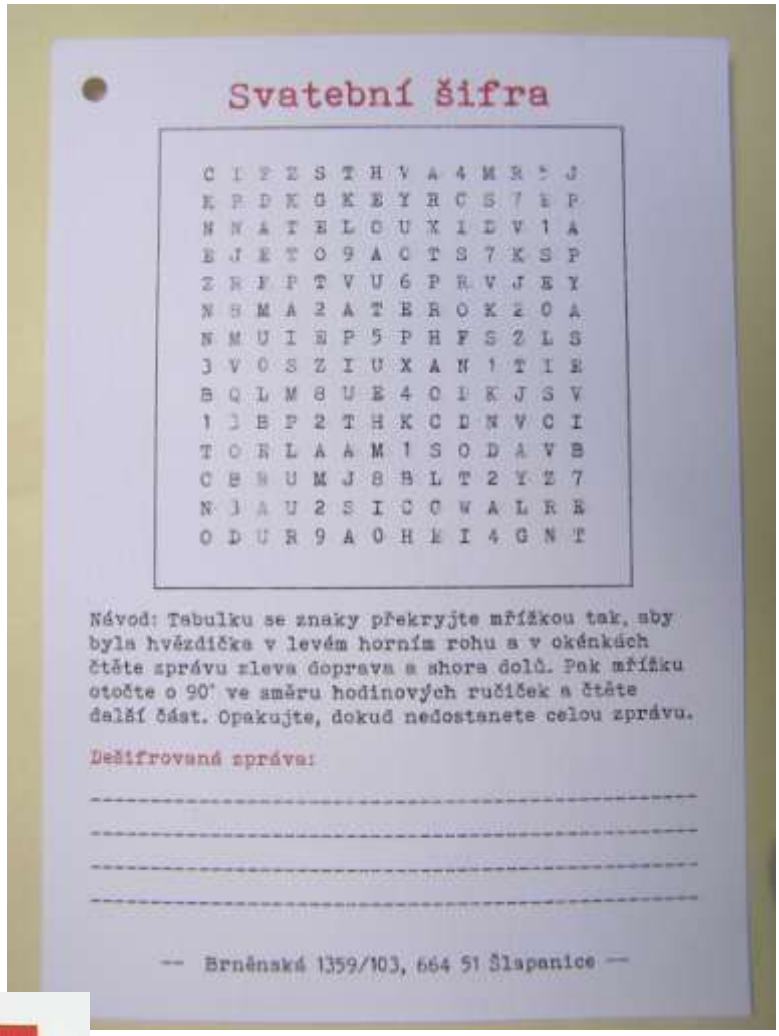
Básně mají většinou erotická témata a lze je číst jako samostatné celky. Pokud se ovšem na vytištěnou báseň přiloží folie se stejným obrázkem, jako je ilustrace k příslušné básni, je možné po červených liniích obrázku číst slova, která vytvoří jinou novou báseň (viz obr 4). Tato nová báseň je samozřejmě kratší než báseň původní a všechna její slova byla v původní básni obsažena. Ovšem smysl textu nové básně je podstatně nebo zcela jiný. Je to nová báseň ukrytá v básni původní. Jedná se o literární dílo, kde v kombinaci s použitými výtvarnými ilustracemi vznikne literární dílo jiné.

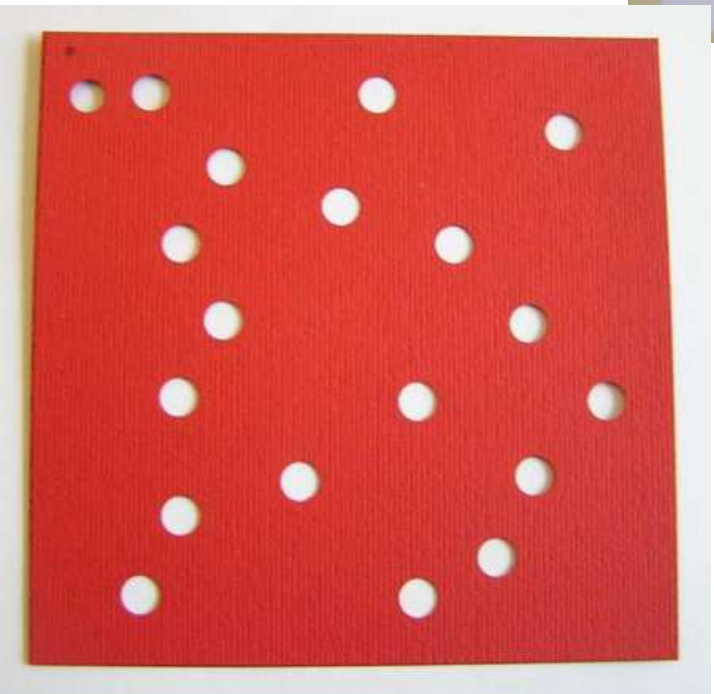

nikdo jen tři muži na světě jen muži ve
některé Marie nesestupují jen na kopci
ať ze ženy je vídr
sídliště ohanbí už totiž
pod hlavu nejlépe
triky úst se snaží aby
jim vybrala odvahu
pupky jde hledat do
cíví rád pod když
na stvořitele ve
přechodu ať táhne aby mi
na koberec zády i v rozkro
kluzišti zahřát ústa pak si být
ženy kéž spávají ve dne a jenom tak
u nás ho Kristus má to už tuší neví ale že
aby byla tou byl i o berlích pod peřinou
ohol se ohol ostatní ještě by si neopálila stín
ani rty ani sílu pode dveřmi má ještě uší
plavu ke stropu bolíš mě živý němý

Perlička druhá.

S laskavým svolením novomanželů Ivety a Radka Paličkových si zde dovolím reprodukovat jejich velmi vtipné svatební oznámení, které od nich v dubnu letošního roku obdržela moje manželka. Jejich oznámení bylo vytvořeno ve formě modifikovaného klasického šifrového systému transpozice (v tomto případě včetně tzv. klamačů), který je čtenářům jistě dobře znám (viz obr. 5).

Text nebylo v tomto případě nutno luštit, neboť šifrový klíč byl přiložen včetně návodu na jeho použití (viz obr. 6).

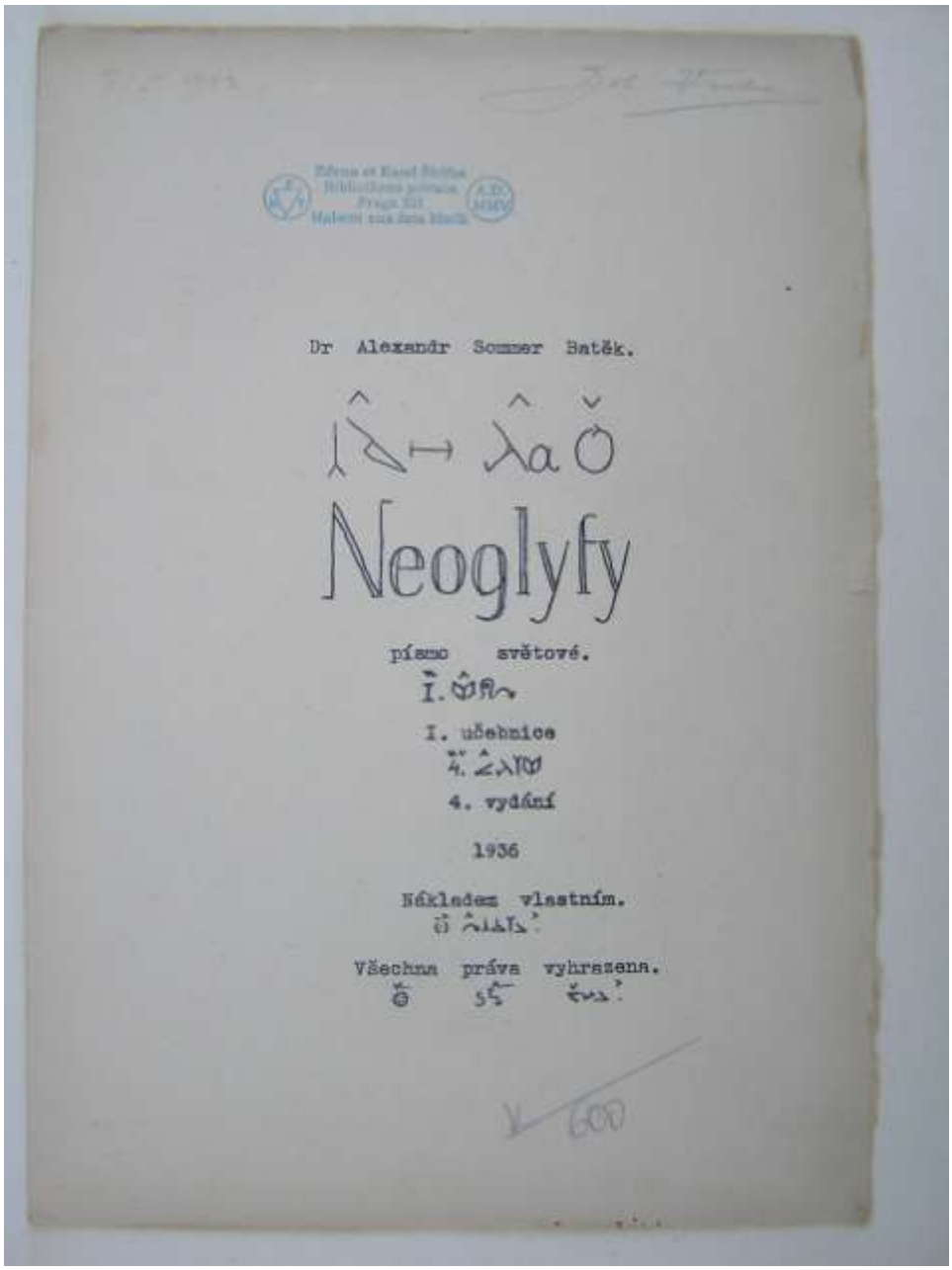




Je možné, že někteří z jejich přátel otočnou mřížku neobdrželi a byli nuceni prověřit své luštitelské schopnosti. To by ovšem nebylo zdaleka tak jednoduché, jak by se na první pohled mohlo zdát, protože poměr počtu znaků s informační hodnotou ke klamačům je 72 : 124. Pokud ovšem klamače představují opravdu klamače.

V každém případě svatební oznámení je to velice originální.

Perlička třetí – Neoglyfy.



Asi největší zajímavost, se kterou se můžeme setkat v souvislosti se starší českou kryptografií, jsou publikace PhDr. Alexandra Sommera Batěka, které vydával vlastním nákladem ve formě většinou šestnáctistránkových sešitů ve třicátých letech minulého století. Jedná se o vytvoření systému Neoglyfů neboli písma světového (viz obr. 7).

Jde o dílo podivuhodné a velmi rozsáhlé a je možné předpokládat, že patří i do kategorie jevů, které popisoval prof. Vladimír Vondráček ve své slavné práci „Podivuhodné a zvláštní z hlediska psychiatrie“. V dnešní době rozsáhlého používání ikon v počítačové a komunikační technice však získává nový rozměr. Dovolím si zde zatím reprodukovat pouze jeden z reklamních letáků na systém neoglyfů doktora Sommera Batěka z roku 1935 (viz obr. 8 – 11)

PASIGRAFIE Číslo 1. 1935

Leták v pokračováních. - Příloha Neoglyfů a Správného života.

Co jest pasigrafie ?

Velký filosof německý Gottfried Wilhelm Leibniz, narozený r. 1646 v Lipsku byl po Aristotelovi nejgeniálnějším polyhistorem, to je učencem, který obsáhl všechno vědění své doby. Ve svém spise Charakteristica Magna Universalis vyslovil myšlenku potřebnosti světového písma pasigrafie, doslova Všepísma, t. j. písma, které by vyjadřovalo nikoli slova, nýbrž přímo myšlenky. Tato jeho myšlenka se ujala ve světě vědeckém, který užívá značek čili symbolů pro své pojmy, které se tím stávají nejen přesnými, nýbrž i všem lidem srozumitelnými. Zvláště chemie, když v ní byly zavedeny pro prvky značky a pro sloučeniny vzorce, se stala vědou tak důležitou, že by bez ní naše vzdělanost byla sotva myslitelna.

Leibniz výslovně žádá universální písmo a nikoli universální řeč, protože písmo jest něčím stálejším, co lze snáze přenésti na potomstvo a zachovati věkům budoucím, než řeč, která se mění i během jedné generace.

My sami dnes slyšíme mládež mluviti hantýrkou, které by naši rodiče již sotva rozuměli. Napřed nás to uráží, potom na to zvykneme a konečně přechází tato mluva i do literatury. Jest jisto, že i pojmy se mění, ale ty lze zachytiti definicemi a tím je zvědečtiti a ustáliti.

I náš celý život stává se pomalu, ale jistě rozumějším a vědečtějším, než byl život našich předků. O různých typech létadel a automobilů slyšíme mluvit naše chlapce a názory vědecké dostávají se i do mluvy prostých lidí. Lidé dnes vědí o tuberkulose a jiných nemocech více, než před dvěma generacemi věděli lékaři.

Jest v tom mnoho šarlatánství a nepravé vědy, ale to jest jen vinou těch, kdo lid poučují. Budou-li lepší učitelé lidu, bude-li dozor, aby se do novin nedostávaly zprávy zkroucené a nesprávné, stane se všechen lid nikoli učeným, ale vzdělaným a moudrým.

Jaký div, že nastává dnes doba, kdy Leibnizova pasigrafie se stává požadavkem dne. Proto řešení pasigrafie mými neoglyfy se událo v pravý čas, kdy ho je potřebí.

Co jsou neoglyfy?

Neoglyfy jsou znaky pro pojmy tak vytvořené, že jimi lze vyjadřovati myšlenky snáze a přehledněji, než písmem. Jsme arci zvykli mluviti a mysliti ve větách, takže i neoglyfy se musí na počátku vázati na tento způsob vyjadřování. Ale myslím, že časem povstane i osobitý způsob vyjařování, při čemž vzniknou jakési obrazce, které se budou čísti přímo myšlenkami. Stane se něco podobného jako v chemii, kde ze značek prvků povstaly vzorce, které se spojují v rovnice, nebo v strukturní obrazce, které nám znázorňují přímo vnitřní složení hmoty, tak jako plán lépe vyjadřuje vnitřní zařízení domu, než popis sebe lepší. To vystihl francouzský inženýr PERDRIZET, který mi o mých neoglyfech napsal ve svém dopisu z 1. srpna 1933:

»Studoval jsem Vaše neoglyfy a nacházím je mnohem filosofičtější, než jest etymologie kteréhokoli nynějšího jazyka živého. Studenti studovali by mnohem rychleji Vašimi neoglyfy, protože by nebyli nuceni sledovati pochody potřebné k porozumění každého slova.«

Sinolog R. H. GEOGHEGAN ve Fairbanks na Aljašce po přečtení jediného anglického sešitu byl s to již přepsati neoglyficky Menciův čínský spis Příkaz nebes, který mi zaslal na důkaz, že čínština se přepisem neoglyfickým stává srozumitelnou lépe než japonskými soustavami Kanamajiri a Katakana.

Jak vycházejí neoglyfy?

Neoglyfy vycházejí v sešitech po 5 Kč a vyšlo již 33 sešitů českých, 3 německé a po jednom sešitu francouzském, anglickém a esperantském. Jeden sešit vyšel pro děti, jehož však mohou dobře použíti k učení i dospělí, tak jako se řeči učí nejlépe z dětských slabikářů. Připravuje se také vydání ruské spoluprací spisovatele Bulgakova, jenž býval sekretářem hraběte Tolstého.

Lze neoglyfy dostati laciněji?

Ano. Každý, kdo se přihlásí k obci neoglyfické má právo na slevu 40%, takže sešit dostane za 3 Kč místo za 5 Kč, ale zavazuje se tím 1. k tomu, že bude se neoglyfům učiti, 2. že je bude mezi známými šířiti.

Jak se nejsnáze naučíme neoglyfům?

K učení neoglyfů se hodí nejlépe na počátku 1. sešit neoglyfů pro děti zvaný Prvouka. Moje vnoučata se z toho sešitu učí rychle

a ráda. Název »Neoglyfíčky« vyjadřuje jejich lásku k tomu druhu učení. Také jiné děti se dychtivě učí neoglyfům. Kdyby lidé místo řešení křížovek si oblíbili psaní a čtení neoglyfů, měli by z toho mnohem více.

Když jsme prošli první sešit pro děti, čteme souvisle první sešit Neoglyfické učebnice, v němž nabudeme důkladného vědění o skládání obrazců neoglyfických podle pravidel mluvnických, jakož i přehledu o 360 znacích, z nichž se tyto obrazce skládají. Potom již můžeme pokračovati ve čtení dalších sešitů, při čemž věnujeme zvláštní píli článkům v sešitech obsažených, které se učíme čísti srovnávajíce své čtení vždy s přepisem českým v sešitu následujícím.

Pokračujeme-li tímto způsobem, stane se nám vyjadřování neoglyfické běžným a snadným. Slovník na konci celého díla nás naučí vyjádřiti kterýkoli pojem kresbou.

Dostávám již celé dopisy od lidí, kteří se studiu tomu věnovali.

Jak máme neoglyfy šířiti?

Šíření neoglyfů jest v zájmu jednoho každého, protože

1. lze se tím způsobem nadíti, že při větším oběhu budou neoglyfy lacinější, nebo že se za týž peníz dostane více.

2. Rozšířením neoglyfů zvláště v cizině se nám naskytne možnost dopisovati si se členy zahraničními a seznamovati se také se způsobem myšlení za hranicemi.

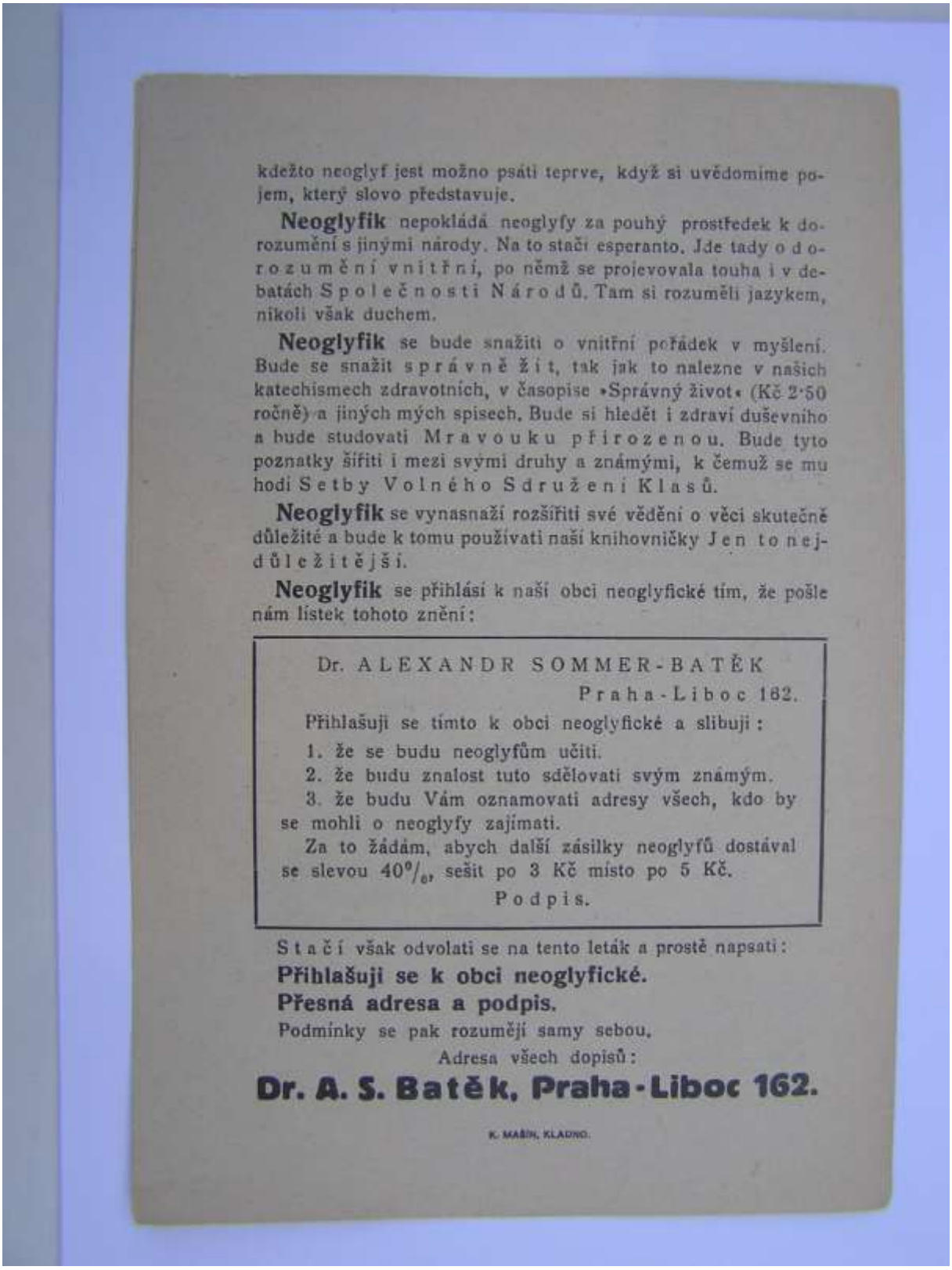
Proto se budeme snažiti neoglyfy rozšířiti mezi svými známými, tím že dáme čísti svým známým letáky neoglyfické, jakož i časopis »Správný život«, jenž přináší pravidelné zprávy o neoglyfech a jejich rozšíření.

3. Budeme zasílati do ústředí v Praze-Liboci 162 adresy všech, kdo mají zájem o tuto myšlenku.

4. Tím, že vyvěsíme letáky neoglyfické v místnostech hostinských, kancelářských a všude, kde se mnoho lidí schází a mohou letáky čísti.

5. Dáme letáky čísti lidem ve vlaku, v tramvaji a všude, kde mají k tomu lidé čas, a rádi si ukrátí dlouhou chvíli.

Neoglyfik nepokládá neoglyfy za pouhý sport ani za hračku k ukrácení dlouhé chvíle. On v nich vidí prostředek, jak se naučiti správně myslit a správně mluvit. Slovo psané písmenami lze napsat i když nerozumíme jeho významu,



kdežto neoglyf jest možno psáti teprve, když si uvědomíme pojem, který slovo představuje.

Neoglyfik nepokládá neoglyfy za pouhý prostředek k dorozumění s jinými národy. Na to stačí esperanto. Jde tady o d o r o z u m ě n í v n i t ř n í, po němž se projevovala touha i v debatách S p o l e č n o s t i N á r o d ů. Tam si rozuměli jazykem, nikoli však duchem.

Neoglyfik se bude snažiti o vnitřní pořádek v myšlení. Bude se snažit s p r á v n ě ž i t, tak jak to nalezne v našich katechismech zdravotních, v časopise »Správný život« (Kč 2·50 ročně) a jiných mých spisech. Bude si hledět i zdraví duševního a bude studovati M r a v o u k u p ř i r o z e n o u. Bude tyto poznatky šířiti i mezi svými druhy a známými, k čemuž se mu hodí S e t b y V o l n é h o S d r u ž e n í K l a s ů.

Neoglyfik se vynasnaží rozšířiti své vědění o věci skutečně důležité a bude k tomu používati naší knihovničky J e n t o n e j d ů l e ž i t ě j š i.

Neoglyfik se přihlásí k naší obci neoglyfické tím, že pošle nám lístek tohoto znění:

Dr. ALEXANDR SOMMER-BATĚK
P r a h a - L i b o c 162.

Přihlašuji se tímto k obci neoglyfické a slibuji:
1. že se budu neoglyfům učiti.
2. že budu znalost tuto sdělovati svým známým.
3. že budu Vám oznamovati adresy všech, kdo by se mohli o neoglyfy zajímati.

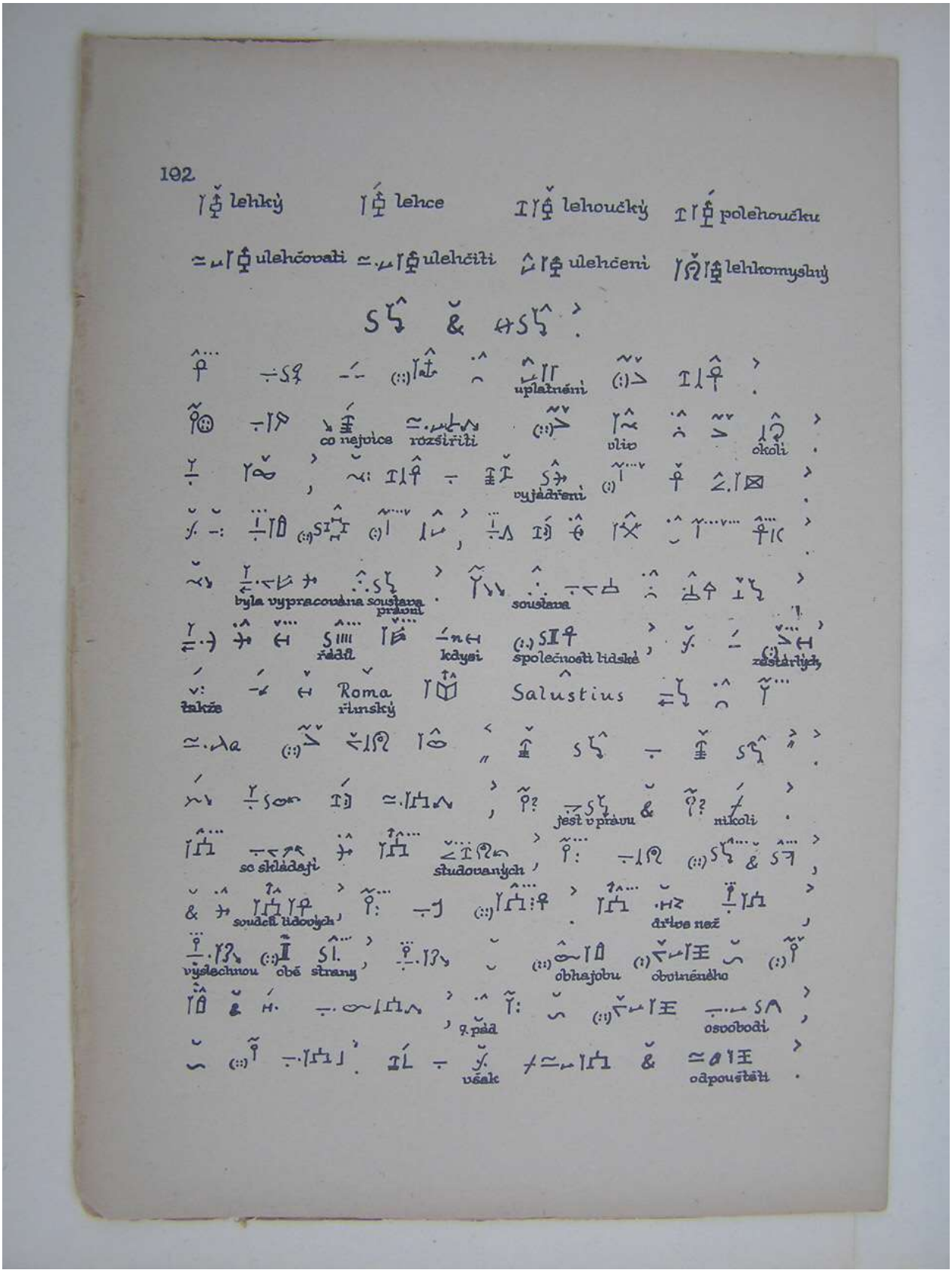
Za to žádám, abych další zásilky neoglyfů dostával se slevou 40%, sešit po 3 Kč místo po 5 Kč.

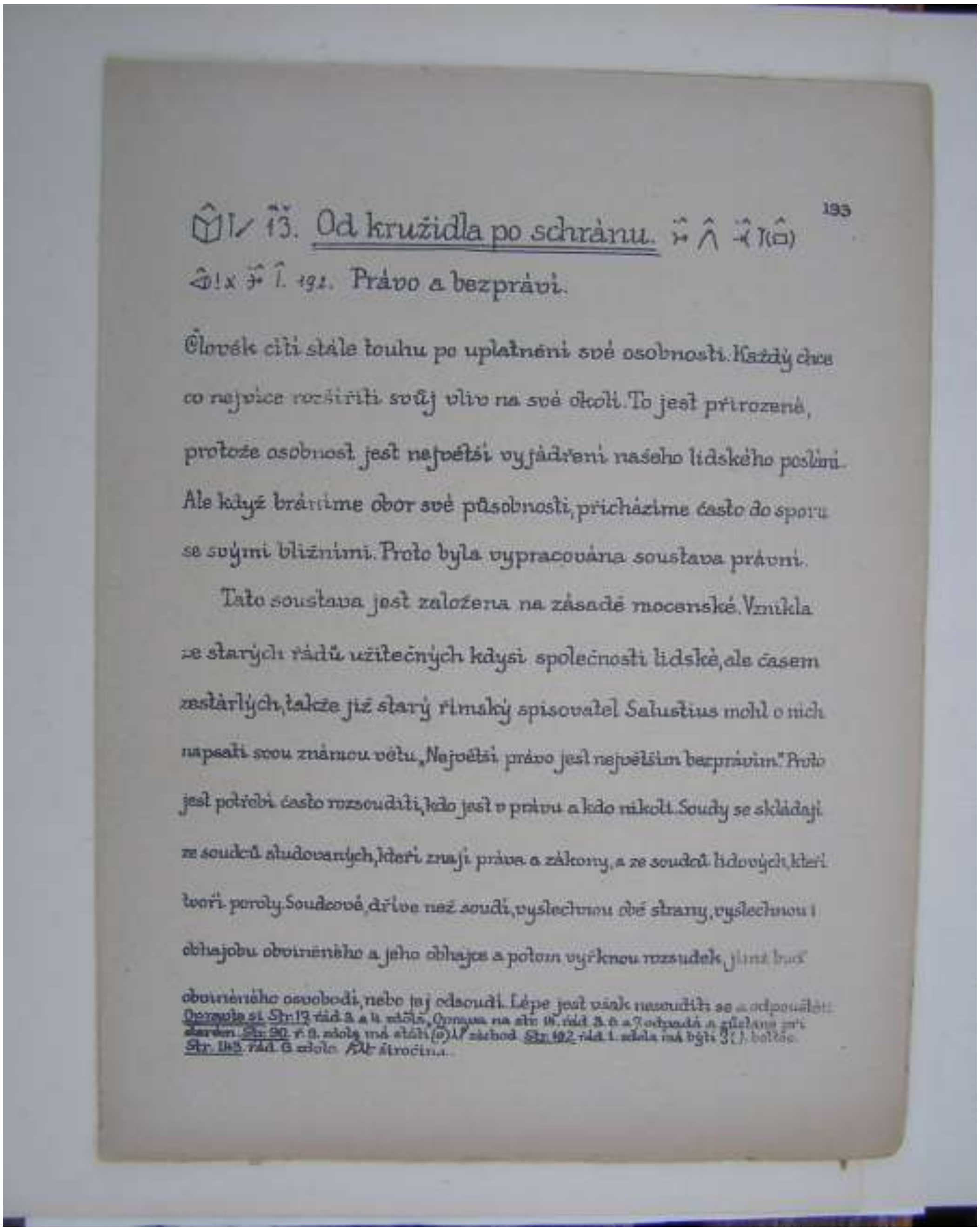
P o d p i s.

S t a č í však odvolati se na tento leták a prostě napsati:
Přihlašuji se k obci neoglyfické.
Přesná adresa a podpis.
Podmínky se pak rozumějí samy sebou.
Adresa všech dopisů:
Dr. A. S. Batěk, Praha-Liboc 162.

K. MAŠÍN, KLADNO.

a jeden z cvičných neoglyfických textů ze 4. vydání první učebnice neoglyfů z roku 1936 s překladem do češtiny (viz obr. 12 - 13).


192
lehký
lehce
lehoučký
polehoučku
ulehčovati
ulehčiti
ulehčení
lehkomyslný
uplatnění
vliv
okolí
co nejvíce
rozšířiti
vyjádření
byla vypracována soustava
soustava
přání
kdysi
společnosti lidské
zastárlých
řádů
takže
Roma
římský
Salustius
jest v právu
nikoli
se skládají
studovaných
soudců lidových
dříve než
výslechnou
obě strany
obhajobu
obviněného
osvobodí
odpouštěti
však


193

13. Od kružidla po schránu.

191. Právo a bezpráví.

Člověk cítí stále touhu po uplatnění své osobnosti. Každý chce co nejvíce rozšířiti svůj vliv na své okolí. To jest přirozené, protože osobnost jest největší vyjádření našeho lidského poslání. Ale když bránime obor své působnosti, přicházíme často do sporu se svými bližními. Proto byla vypracována soustava právní.

Tato soustava jest založena na zásadě mocenské. Vznikla ze starých řádů užitečných kdysi společnosti lidské, ale časem zestárlých, takže již starý římský spisovatel Salustius mohl o nich napsati svou známou větu „Největší právo jest největším bezprávím.“ Proto jest potřebí často rozsouditi, kdo jest v právu a kdo nikoli. Soudy se skládají ze soudců studovaných, kteří znají práva a zákony, a ze soudců lidových, kteří tvoří poroty. Soudcové, dříve než soudí, vyslechnou obě strany, vyslechnou i obhajobu obviněného a jeho obhájce a potom vyřknou rozsudek, jímž buď obviněného osvobodí, nebo jej odsoudí. Lépe jest však nesouditi se a odpouštěti.

Myslím, že je to pro první seznámení zcela postačující, neboť systému neoglyfů bude vhodné věnovat samostatnou obsáhlejší perličku. PhDr. Sommer Batěk (narodil se 15. června 1874 v Prádle u Nepomuku a zemřel 6. dubna 1944 v Praze) byl středoškolským profesorem chemie a výraznou osobností českého prostředí. Kromě chemie publikoval i v mnoha jiných oborech, někdy pod pseudonymem Heliar. Měl i to veliké štěstí, že je zmíněn v Haškově románu Osudy dobrého vojáka Švejka, a to v pasáži popisující rozjařený stav polního kuráta Otto Katze. Pozoruhodná je rovněž skutečnost, že známý systém přípon pro chemické názvosloví zavedený v češtině profesorem Emilem Votočkem měl základ v díle doktora Sommera Batěka.

C. Z NISTu unikl interní dokument k SHA-3

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

Do poštovní konference, zřízené pro libovolné zájemce a účastníky soutěže SHA-3 byl odeslán dokument, který měl být odeslán pouze do interní skupiny NISTu pro výběr SHA-3.

Dokument v originální podobě si lze stáhnout z našeho webu
http://crypto-world.info/casop14/NIST_unikly_dokument.pdf

Odeslal ho William Burr, toho času již ne vedoucí Security Technology Group divize Computer Security NISTu, ale v NISTu nyní pouze hostující výzkumník.

Jako účastník soutěže jsem s kolegou Danilem Gligoroským po vyhlášení pěti finalistů zvažoval dopis NISTu, který měl navrhnout odvolání Williama Burra, zodpovědného za zmaření soutěže SHA-3. Zmařené nikoli proto, že náš algoritmus BMW (nejrychlejší z kandidátů a splňující zadání) nepostoupil do finále, ale proto, že během soutěže byly zásadně změněny její podmínky. Podmínkou bylo, že vítězný algoritmus musí být mnohem rychlejší než stávající algoritmy SHA-2. Výsledkem soutěže však je, že **žádný z finalistů toto zadání nesplňuje**.

Přitom byla možnost zvolit jiné finalisty, minimálně namísto tří zcela evidentně do počtu přidaných outsiderů (JH, Groestl, Keccak). Tito outsideři se nyní jasně ukazují ve zprávě NISTu. I kdyby tato zpráva neunikla, bylo to veřejné tajemství, které bylo možné skrývat jen do finálního odůvodnění. Bylo pro mě tedy překvapení, že W. Burr podle podpisové doložky v uniklém mailu už vedoucí místo nezastává.

Docela zajímavé jsou změny, které William Burr v textu udělal, i komentáře. Pochopitelně, je to pracovní dokument, takže by nebylo slušné se v něm příliš šťourat, proto ho necháváme bez komentáře.

Avšak zajímá vás, kdo má podle téhle zprávy větší šanci na výhru? Skein nebo Blake? Pro ty, koho to zajímá, jsme udělali následující – z textu zprávy jsme vyloučili

texty, týkající se outsiderů a pro Skein i Blake ponechali jen hodnotící a srovnávací text (z důvodu délky i přehlednosti). To, co zbylo, uvádíme dále.

Performance Comparison of SHA-3 Finalists

This section discusses how the finalist candidates perform when implemented in software for different computers, and in hardware circuits.

All of the SHA-3 finalist candidates, as well as SHA-2, have four variants with 224, 256, 384 and 512-bit message digest outputs. Skein generates all four message digest sizes with the same compression function, and therefore, all four run at about the same rate. Blake and SHA-2 use two different compression functions, one for 512 and 384-bit message digests, and one for 256 and 224-bit message digests. The 512/384 bit and the 256/224 bit hash functions usually run at different speeds on the same platform.

In the performance discussion, whenever the name of an algorithm is used without a specific digest size attached, then the statement applies for all four digest sizes.

eBASH: General-Purpose Computers

The eBASH homepage is found at: http://bench.cr.yp.to/ebash.html. During the course of the SHA-3 competition, a large number of hash functions were benchmarked on general purpose computers, and much data on all of them can be found on the eBASH site. The best comparative presentation of the data for the SHA-3 finalists and SHA-2 is the “shootout” graphs found at: http://bench.cr.yp.to/results-sha3.html.

We categorize the computers used in eBASH into four of the five groups described above:

- AMD64: use the AMD64 ISA and generally **include** a vector unit.
- X86: use the 32-bit X86 ISA and **may** include a vector unit.
- 32-bit RISC: use the following 32-bit RISC ISAs: ARM, MIPS or PPC. A vector unit is **not used**.
- ARM-NEON: use the 32-bit ARM ISA **with** the NEON vector unit.

Long Messages

AMD64: Skein (all sizes) and Blake-512 are consistently the fastest algorithms and the only two algorithms that generally are faster than SHA-512 on AMD64 platforms.

X86: The high group here is Blake-256, Skein, and SHA-256.

ARM - NEON*:* The high group is Blake, Skein and SHA-256. The ability of the NEON vector unit to do 64-bit operations probably helps Skein and Blake-512 here.

32-bit RISC: The high performance algorithms are Blake-256 and SHA-256.

Algorithm	AMD64			X86			ARM-NEON			32-bit RISC		
	High	Med	Low	High	Med	Low	High	Med	Low	High	Med	Low
Blake-512	✓				✓		✓				✓	
Blake-256	✓	✓		✓			✓			✓		
Skein	✓			✓	✓		✓				✓	
SHA-512		✓			✓				✓		✓	
SHA-256		✓		✓			✓			✓		

Table x - eBASH performance comparison for long (> 4096-byte) messages

64-byte Messages

AMD64: As with long messages, Blake and Skein lead all others.

X86: Blake-256, Skein and SHA-256 are fast on this 32-bit word ISA.

ARM-NEON: Blake-256, Blake-512 and SHA-256 are fast, while SHA-512 is the slowest.

32-bit RISC: The two algorithms that use 32-bit modular addition extensively are fast

Algorithm	AMD64			X86			ARM-NEON			32-bit RISC		
	High	Med	Low	High	Med	Low	High	Med	Low	High	Med	Low
Blake-512	✓				✓		✓				✓	
Blake-256	✓	✓		✓			✓			✓		
Skein	✓			✓	✓			✓			✓	
SHA-512		✓				✓			✓		✓	
SHA-256		✓		✓			✓			✓		

Table y - eBASH performance comparison for 64-byte messages

XBX: Embedded Microcontrollers

Most of our data on embedded microcontrollers comes from the XBX effort. The website for the effort is at: http://xbx.das-labor.org/trac/wiki.

Eight-bit: ….

Sixteen-bit: Overall, Blake-256 was fast and small, and SHA-256 was second.

ARM (thumb instructions): This version of the ARM processor is a low-end microcontroller that only implements the 16-bit thumb instructions. Blake is the smallest algorithm. Blake-256 and SHA-256 have the highest similar throughputs. Skein has the largest area requirement.

32-bit RISC (without the NEON vector processor): SHA-256 is the fastest algorithm overall, followed by Blake-256. Skein, Blake-512 and SHA-512 vie for third place. In area, Blake-256 is usually the smallest.

ARM with NEON: This is a relatively fast ARM core with the addition of a vector unit that supports 64-bit operations. With the addition of the vector unit, Skein becomes the fastest algorithm, followed fairly closely by Blake-256, Blake-512 and SHA-256. In that ranking Blake is first, SHA-2 second, Skein third. The smallest is Blake-256. Blake-256 has the overall advantage.

The Future

Zde je místo textu použito tabulek, které ukazují, že v procesorech v blízké budoucnosti bude mít Blake o něco navrch nad Skeinem.

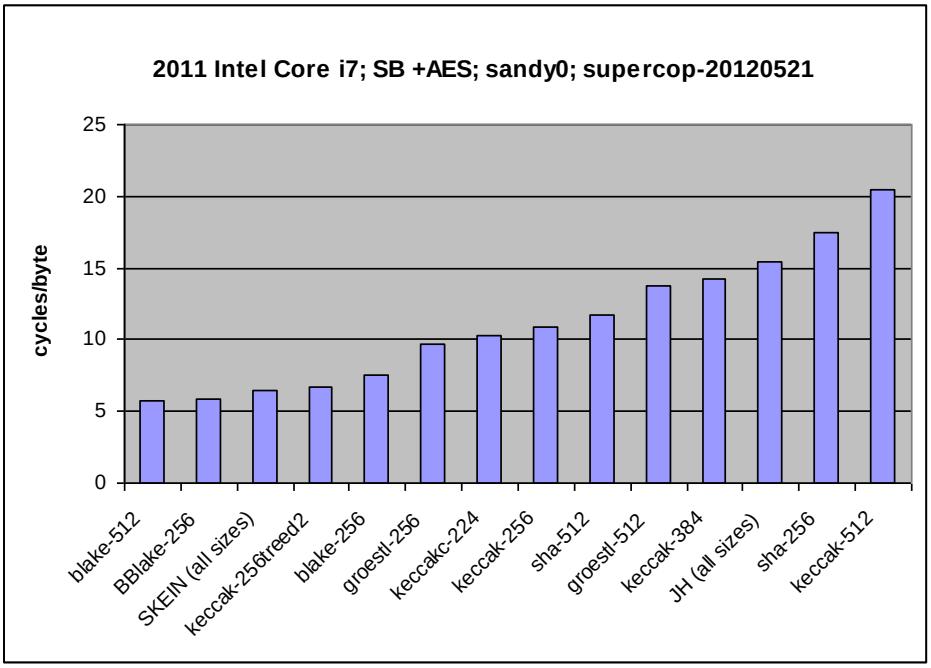


Figure z-1 – SHA-3 Finalist Cycles/Byte on Current Sandy Bridge Desktop Processor

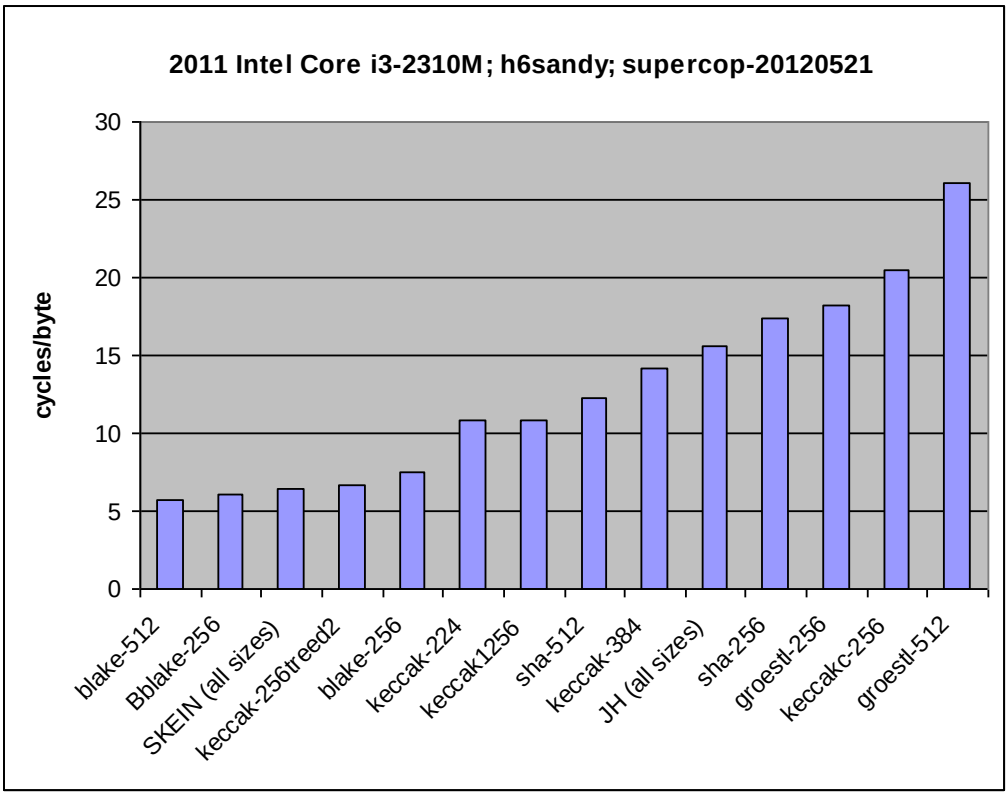


Figure z-2 – SHA-3 Finalist Cycles/Byte on Current Sandy Bridge Laptop Processor

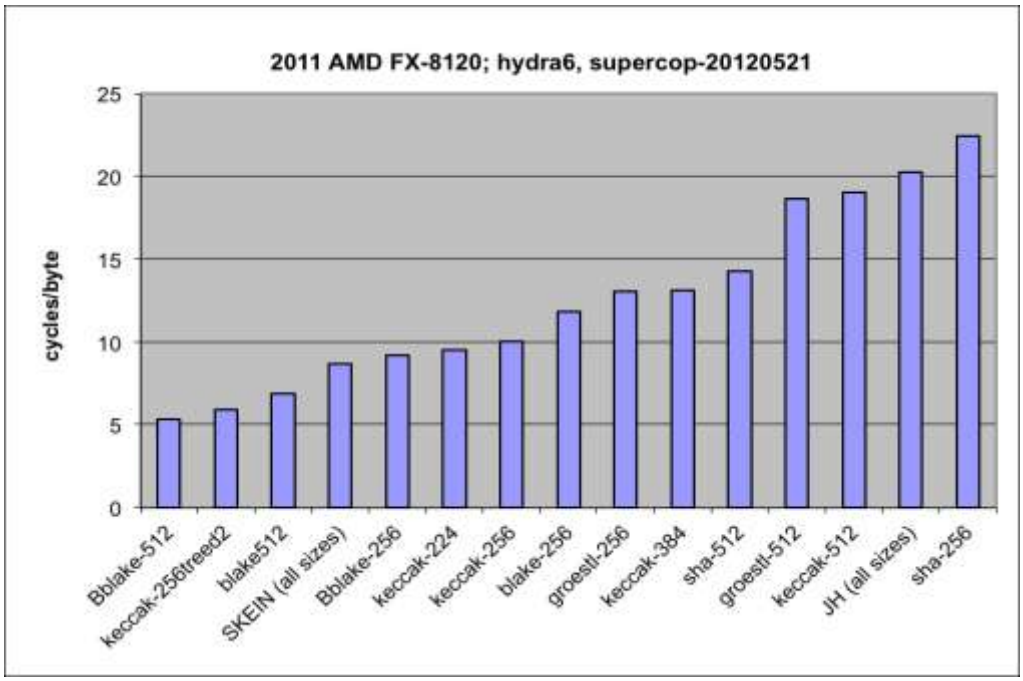


Figure z-3 - SHA-3 Finalist Cycles/Byte on Current Bulldozer Desktop Processor

Software Performance Summary

Skein and Blake, the two ARX finalist candidates, have the best overall software performance. Only Skein and Blake seem to be faster than SHA-2 in most cases.

Skein-256 has a small to moderate performance advantage over Blake-256 on AMD64 platforms, which may, or may not carry over to future 64-bit ARMv8 processors. Blake-512 seems to gain a modest performance advantage over Skein-512 on more recent AMD64 machines.

On 32-bit machines (mainly ARM processors) without vector units, Blake-256 is the clear overall leader, although it does not offer any real speed advantage over SHA-256. On ARMs with the NEON vector unit, Skein seems the fastest algorithm, followed fairly closely by Blake.

On small embedded computers, Blake-256 has decisively the best overall performance. Its maximum throughput is often similar to, or sometimes less than SHA-256, but Blake-256 generally had smaller memory requirements than SHA-2 and most of the other candidates.

Závěr

Pokud by se hodnotilo jen podle této zprávy, vypadá to, že by měl být zvolen Blake. Kritérií je však více, takže opět žádná velká jistota, že vyhraje nad Skeinem. Hlavní přínos zprávy je tak vlastně v tom, že NIST potvrzuje, že další tři kandidáti tu byli doopravdy do počtu, neboť rozdíly ve výkonnosti jsou příliš velké.

D. Kniha Kryptologie, šifrování a tajná písma rozebrána

Pavel Vondruška, pavel.vondruska@crypto-world.info

Citace: P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006

Vážení čtenáři,
dovoluji si Vás informovat, že moje kniha *Kryptologie, šifrování a tajná písma* je v současné době zcela rozebrána a již ji není možné objednat ani u vydavatele.

V mých skrovných zásobách, které jsem postupně nákupem doplňoval a ze kterých jsem pak tuto knihu využíval jako cenu při soutěžích v luštění pořádaných našim e-zinem nebo jako cenu za nejlepší výsledek v testu při školeních apod., zůstal volný poslední kus (získá jej jeden z úspěšných účastníků kurzu Akademie CZ.NIC - Problematika infrastruktury veřejných klíčů (PKI) 26.9. – viz *následující pozvánka*..).

Kniha vznikla na základě smlouvy uzavřené v dubnu 2004 s nakladatelstvím Albatros. Práci na knize jsem ukončil ve stanoveném termínu do konce roku 2005. Kniha pak vyšla v nákladu 8000 výtisků (což je na současný trh poměrně hodně) ve druhém pololetí 2006 (konkrétně se dostala do prodeje v listopadu 2006).
Přibližně po čtyřech letech byla její dostupnost již jen omezená a dala se sehnat spíše náhodně v některých knihkupectvích, kde se „schovávala“ cudně mezi dalšími výtisky této edice.

K 31.12.2011 mi nakladatel oznámil, že celkové zásoby neprodaných výtisků jsou již jen 138 ks. V únoru, kdy jsem si chtěl doplnit své zásoby ☺, mi pak bylo oznámeno, že skladové zásoby jsou vyprodány a všechny výtisky byly distribuovány do knihkupectví.


ALBATROS MEDIA a.s.

Pavel Vondruška: Kryptologie, šifrování a tajná písma, MČ: 24729
- smlouva čj. V-300/2004 ze dne 15. 4. 2004, skladové zásoby k 31. 12. 2011 – 138 ks

V současné době již není možné knihu objednat. **Je rozebrána**.

Děkuji za Váš zájem o tuto knihu, děkuji za zajímavé a milé e-maily s dotazy a nápady na možné případné doplnění. Tyto reakce byly velmi příjemné a byly moji největší odměnou za čas, který jsem strávil při přípravě textu knihy.

E. Problematika infrastruktury veřejných klíčů (PKI), kurz Akademie CZ.NIC

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

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

Problematika infrastruktury veřejných klíčů (PKI)

Obsah kurzu je nově aktualizován a přepracován. Kurz by měl být svým obsahem dostupný nejširší veřejnosti. Délka kurzu byla zkrácena na jeden den, byly vypuštěny detaily k fungování CA a vypuštěn exkurz do problematiky archivace, fakturace a užití datových schránek. Tím se získal prostor na detailní probrání pojmů podpisové schéma, ověření podpisu a certifikátu (včetně rozhodnutí zda je kvalifikovaný).

Problematika infrastruktury veřejných klíčů (PKI)

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

http://www.nic.cz/akademie/course/15/detail/

Termín: 26. září 2012 (středa, 9.00 - 17.00 hod.)
Garant: Pavel Vondruška Základní cena: 2 000,00 Kč

Cíl kurzu

Po absolvování kurzu bude účastník:

- rozumět principu asymetrických šifer
- znát vybrané definice zákona o elektronickém podpisu (typy certifikátů, typy podpisů, typy certifikačních autorit atd.)
- umět vygenerovat certifikát a zacházet s ním a s příslušným soukromým klíčem
- pochopit princip důvěry v PKI a certifikáty
- mít základní přehled o možných útocích na PKI a použité šifry

Osnova

1. Základní pojmy asymetrické kryptografie
   - filozofie
   - algoritmy
   - podpisové schéma

2. Zákon o elektronickém podpisu č.227/2000 Sb.
   - stručné opakování základních pojmů
   - typy podpisů (elektronický podpis, zaručený elektronický podpis, elektronická značka, „biometrický podpis“)
   - typy poskytovatelů (kvalifikovaný, akreditovaný)
   - typy certifikátů (obyčejný, kvalifikovaný, systémový kvalifikovaný certifikát)
   - ověření podpisu (Vyhláška 212/2012 Sb. o postupech při ověření platnosti zaručeného elektronického podpisu)
   - „velká“ novela zákona 227/2000 Sb.

3. Certifikační autority
   - přehledy poskytovatelů (ČR, SR, EU)
   - jak ověřit, že je certifikát kvalifikovaný

4. Praktické ukázky I.
   - certifikáty
   - úložiště
   - CRL
   - nastavení systému

5. Důvěra v elektronické podpisy
   - vystavitel
   - nastavení
   - certifikační cesta
   - technická důvěra x legislativa

6. Praktické ukázky II.
   - podpis S/MIME, Adobe,
   - podpis MS prostředí (MS Office)
   - PAdES, XAdES, CAdES

7. Základní otázky bezpečnosti elektronických podpisů

F. ZPRÁVA - Nechcete být odposlouchávání? (Zavřete se do laboratoře)

TISKOVÝ SERVIS: **Mgr. Lucie Stejskalová, PEPR Consulting s.r.o., e-mail: stejskalova@peprconsulting.cz**

Praha, 27. června 2012 - V Brně začíná výstavba univerzitních laboratoří pro Vědecko-výzkumný park prof. Lista v areálu Vysokého učení technického v Brně. Vybaveny budou speciální technologií, která obyčejné měřicí laboratoře přemění v obří stíněné komory neboli Faradayovy klece. V laboratořích má instalace této technologie ochranný důvod - měřicí přístroje jsou chráněny před rušivým vyzařováním z vnějšího prostředí, které může mít vliv na výsledky měření, a okolí naopak před únikem elektromagnetického záření vznikajícím během řady laboratorních testů. Stíněné komory ale nacházejí své uplatnění i ve zcela jiných, nevědeckých sférách. Stále častěji se ve Faradayovy klece mění také jednací místnosti a podnikatelské prostory, které jsou pak bezpečně chráněny před jakýmikoliv odposlechy. Princip fungování je přitom stále stejný – stíněná místnost jednoduše nepropustí žádný signál dovnitř ani ven. Odposlouchávaný telefon, skryté štěnice či vzdálený rádiový odposlech se v nich stávají nefunkčními**.**

Stíněné komory jsou využívány v řadě odvětví. Instalovány bývají především tam, kde je třeba chránit zařízení či osoby před škodlivým elektromagnetickým polem či rádiovými vlnami. Nejčastěji se s nimi setkáme v laboratořích, měřících zařízeních, ve zdravotnictví nebo v datových centrech, kde chrání uložená data před útokem zvenčí. Své využití nacházejí i jako účinná ochrana před odposlechy či průmyslovou špionáží.

„Jednou z vlastností stíněných místností je absence signálu mobilních operátorů a zároveň zamezení vysílání a přijímání rádiového signálu,“ uvedl expert na bezpečnost a ochranu před odposlechy Jiří Schmidt ze společnosti Probin, která je dodavatelem stínící technologie pro VUT v Brně. *„Vytvoříme-li z vybrané místnosti Faradayovu klec, stává se pak tento prostor, mimo jiné, zcela bezpečným místem pro citlivá jednání. V tomto prostoru můžeme mít zkrátka jistotu, že směrem ven neunikne žádný signál vysílaný skrytou štěnicí nebo jiným odposlouchávacím zařízením,“* doplnil Jiří Schmidt.

Konstrukce stíněné komory má několik možností odvíjejících se od požadované stínící účinnosti. Pro nižší stínící účinnost je dostačující instalace metalizovaných tapet, které se aplikují na všechny stěny místnosti, strop i podlahu. Výsledná stínící účinnost tapet se pak pohybuje v rozpětí mezi 40 - 60 dB. Extrémně vysokého stínícího účinku lze dosáhnout pomocí instalace konstrukce skládající se z pozinkovaných plechů. Tyto stíněné komory dosahují účinků stínění až k hodnotě 120 dB.

Co je Faradayova klec?

V 19. století si Angličan Michael Faraday povšiml, že náboj přivedený na dutý vodič je rozmístěn pouze na jeho vnější straně a že nemá žádný vliv na předměty umístěné uvnitř. Díky jeho následným pokusům bylo prokázáno, že se náboj na dutých předmětech rozmisťuje pouze na povrchu vodiče, nikoliv v jeho objemu a tedy, že intenzita elektrického pole uvnitř takového předmětu je nulová. Jednoduše to znamená, že uvnitř vodiče nepůsobí žádné elektromagnetické či elektrické pole.

G. O čem jsme psali v létě 2000 – 2011

Crypto-World 78/2000

Příloha: 10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 78/2001

Příloha : priloha78.zip (dopis pana Sůvy - detailní informace k horké sazbě, viz. článek Záhadná páska z Prahy, Crypto-World 6/2001)

Crypto-World 78/2002

Crypto-World 78/2003

Crypto-World 78/2008

Crypto-World 7-8/2009

Přílohy: Simulátor šifrátoru ŠD-2 http://crypto-world.info/soutez2009/sd2/cti.txt
(viz článek Rekonstrukce šifrovacího stroje ŠD-2)
Program RSAM.EXE (viz článek Malá soutěž v luštění RSA – řešení).

Crypto-World 7-8/2010

Crypto-World 78/2011

H. Závěrečné informace

1. Sešit

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

2. Registrace / zrušení registrace

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

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška Jozef Krajčovič 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