Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 12, číslo 5/2010 **15. květen 2010**

5/2010

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese

http://crypto-world.info

(1358 registrovaných odběratelů)

Obsah:

A. Analýza Blue Midnight Wish – současné útoky na BMW-n

Vlastimil Klíma, kryptolog konzultant, Praha
(http://cryptography.hyperlink.cz, v.klima@volny.cz)
Prof. Danilo Gligoroski, Norwegian University of Science and Technology, Norway (danilog@item.ntnu.no , http://www.item.ntnu.no/people/personalpages/fac/danilog/start)


Dr. Vlastimil Klíma

Článek volně navazuje na články o BMW v 12/2009, 3/2009 a 7-8/2009 a na příspěvky v číslech 1 - 4 Crypto-Worldu 2010..V čísle 1 jsme se zabývali hledáním vzoru (úloha první), v čísle 2 hledáním kolize (úloha druhá), v čísle 3 různými bloky BMW a v čísle 4 aspektem složitosti.


Prof. Danilo Gligoroski

Dosud byly analýze BMW, kromě autorské analýzy (zde v Crypto-Worldu a v [6], [7]), věnovány tři příspěvky, viz [3], [4], [5]. Všechny tři jsou tzv. "rozlišovací" útoky (distinguishing attacks) na kompresní funkci BMW. V práci Aumassona [3] má útok složitost cca 2^{19}, v práci Nikolice [4] je to útok na modifikovanou variantu BMW512 se složitostí 2^{278}. Nejvýznamnějším a slibně znějícím je příspěvek Guo-Thomsena [5]. Má minimální složitost, proto se mu budeme věnovat jako prvnímu.

Guo-Thomsenův útok

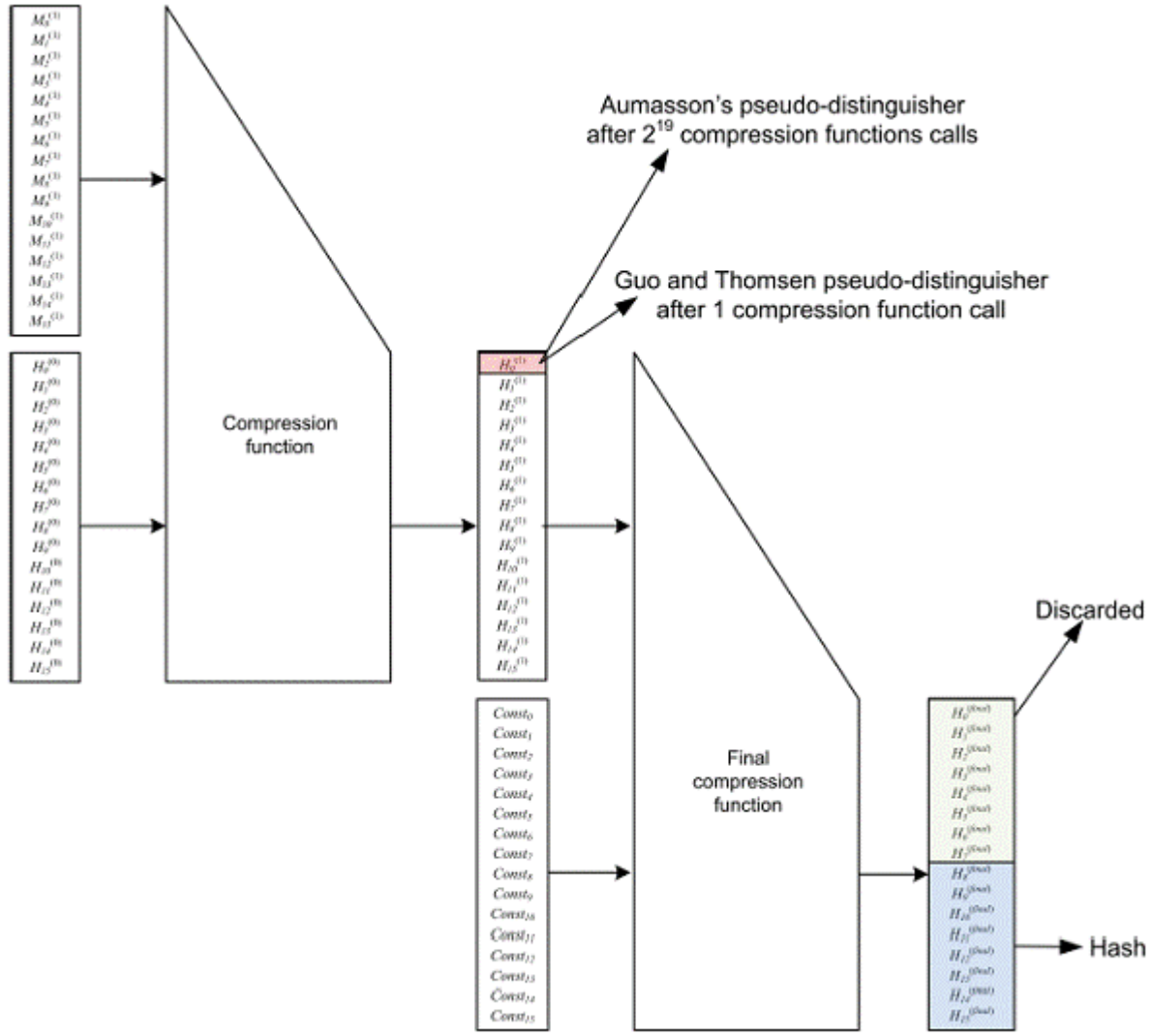
Nejprve poznamenejme, že se jedná o pseudoútok. Oč jde, uvidíme z následující ilustrace. Úvodní volání kompresní funkce na blok zprávy M lze našimi nástroji (z citovaných článků v Crypto-Worldu) jednoduše zapsat takto

$$Q_a = A_2(A_1(M \oplus CONST^{(0)})) + ROTL^1(CONST^{(0)}),$$
$$Q_b = T^L(T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(CONST^{(0)})))$$
$$G = (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)),$$
$$X = (f_6(G)).$$

Guo a Thomsen uvažují, že mohou měnit současně blok zprávy M a hodnotu průběžné haše, což u prvního bloku je konstanta $CONST^{(0)}$. Protože takový útok právě neřeší co s prvním voláním kompresní funkce (a u BMW speciálně navíc i s posledním voláním), říká se mu pseudoútok. Tak tedy, zkoumají kompresní funkci

$$Q_a = A_2(A_1(M \oplus H)) + ROTL^1(H),$$
$$Q_b = T^L(T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(H)))$$
$$G = (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)),$$
$$newH = (f_6(G)),$$

kde mohou měnit jak M, tak H. Konkrétně je mění současně tak, aby M ⊕ H bylo konstantní. Tím vyblokují změnu v dosti nepříjemné difúzní funkci $A_2(A_1(M \oplus H))$ a nastane jen v $ROTL^1(H)$. Konkrétně mění jen slovo M_1 a H_1, takže změna v $Q_a = A_2(A_1(M \oplus H)) + ROTL^1(H)$ nastane jen v jeho nejnižším slově (Q_0). Z Q_a pak tato změna postupuje dále do Q_b, kde se podařilo zjistit, co způsobí, a dojít přes Q_b zatím nejdále k nejnižším bitům nultého slova proměnné G, viz obrázek.



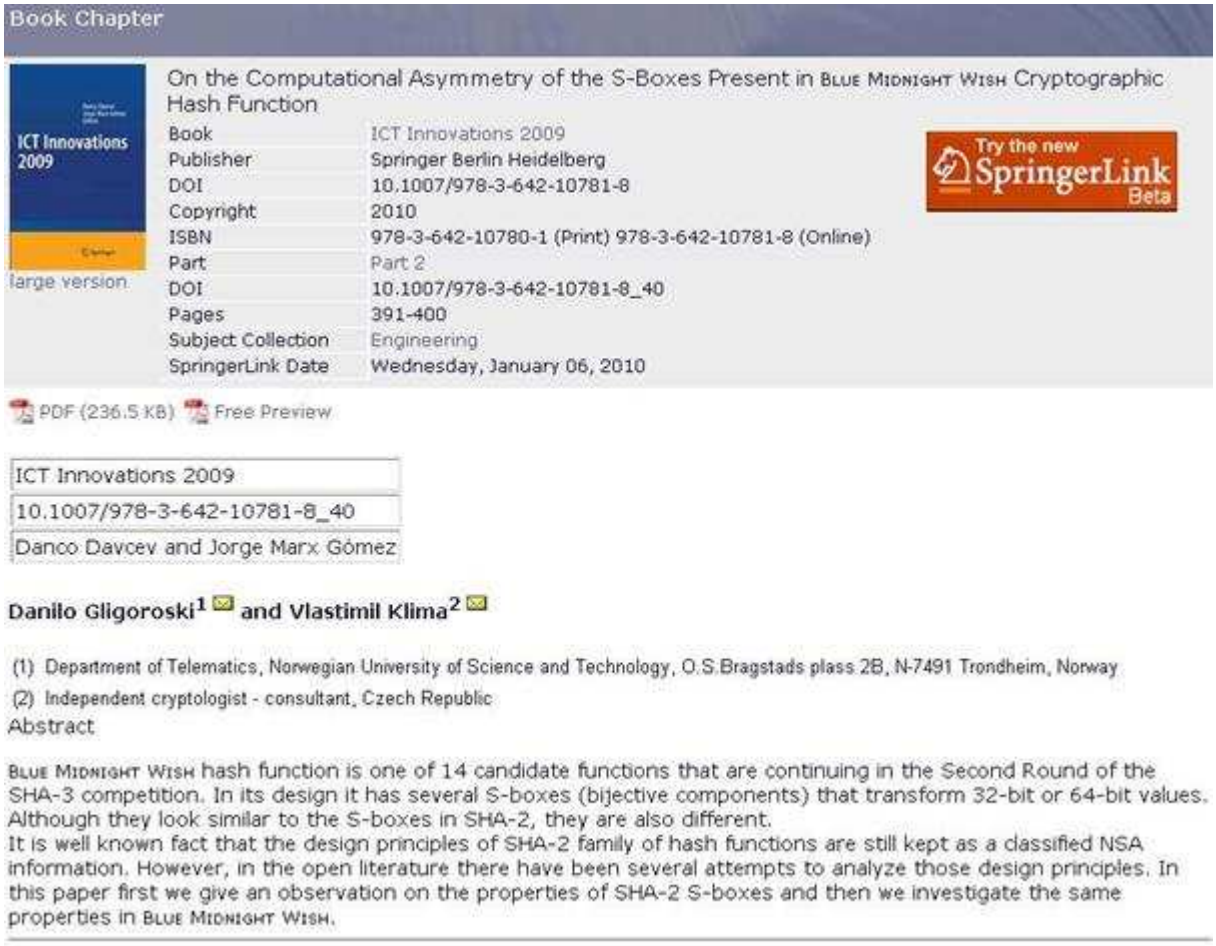
Obr.1: Výsledky současných útoků na BMW256/512

V těchto místech jsou schopni říci, jak se tyto bity změní nebo je odlišit od náhodných. Konkrétní počty dotčených bitů jsou uvedeny na následujících dvou obrázcích. Jsou zde uvedeny i varianty BMW 0/16, 1/15 a 2/14, z nichž ta poslední je definitorická BMW s dvěma rundami číslo jedna a 14 rundami číslo 2, ostatní jsou pouze nestandardní varianty. V nejlepším případě se jedná o 11 bitů u nestandardních verzí a o 1 bit u standardních verzí. O změnách ostatních z 512 nebo 1024 bitů (pro BMW256/512) proměnné G nejsou schopni prohlásit už nic. Nová proměnná newH má tak určeno několik nejnižších bitů, které přebírá z G. Jakmile však newH vstoupí do posledního volání kompresní funkce, je zde jednak chování tohoto vstupu už dosti omezeno (právě jsme si řekli, že víme jak se chová pár jeho bitů z 512 nebo 1024) a jednak zbývající vstup už nemůžeme měnit, neboť je to konstanta $CONST^{(final)}$:

$$Q_a = A_2(A_1(newH \oplus CONST^{(final)})) + ROTL^1(CONST^{(final)}),$$

$$Q_b = T^L(T^U(Q_a) + ((B(rotnewH) + K) \oplus ROTL^7(CONST^{(final)})))$$
$$G = (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)),$$
$$Hash = 8\_lswords\_of(\ f_6(G)\ ).$$

Tedy do tohoto posledního bloku vstupuje mnoho neznámým způsobem změněných bitů zcela na počátku v proměnné newH a několik známých změn. Autoři sami potvrzují, že o výsledku (Hash) nejsou schopni nic říci, a že jejich přístup ukazuje pouze vlastnost kompresní funkce, ale neohrožuje bezpečnost celé hašovací funkce.



Book Chapter

On the Computational Asymmetry of the S-Boxes Present in Blue Midnight Wish Cryptographic Hash Function

Book	ICT Innovations 2009
Publisher	Springer Berlin Heidelberg
DOI	10.1007/978-3-642-10781-8
Copyright	2010
ISBN	978-3-642-10780-1 (Print) 978-3-642-10781-8 (Online)
Part	Part 2
DOI	10.1007/978-3-642-10781-8_40
Pages	391-400
Subject Collection	Engineering
SpringerLink Date	Wednesday, January 06, 2010

Try the new SpringerLink Beta

large version

PDF (236.5 KB) Free Preview

ICT Innovations 2009
10.1007/978-3-642-10781-8_40
Danco Davcev and Jorge Marx Gómez

Danilo Gligoroski[1] and Vlastimil Klima[2]

(1) Department of Telematics, Norwegian University of Science and Technology, O.S.Bragstads plass 2B, N-7491 Trondheim, Norway
(2) Independent cryptologist - consultant, Czech Republic

Abstract

Blue Midnight Wish hash function is one of 14 candidate functions that are continuing in the Second Round of the SHA-3 competition. In its design it has several S-boxes (bijective components) that transform 32-bit or 64-bit values. Although they look similar to the S-boxes in SHA-2, they are also different.
It is well known fact that the design principles of SHA-2 family of hash functions are still kept as a classified NSA information. However, in the open literature there have been several attempts to analyze those design principles. In this paper first we give an observation on the properties of SHA-2 S-boxes and then we investigate the same properties in Blue Midnight Wish.

Aumassonův útok

V práci Aumassona [3] má útok složitost cca 2^{19}, ale na BMW-512 má srovnatelné výsledky jako Guo-Thomsen [5]. Postup je téměř stejný, i když vznikl nezávisle. Opět se jedná o pseudoútok a opět mění současně M a H tak, aby $M \oplus H$ bylo konstantní. Zde však mění dvě slova, a to M_1 a H_1 a M_5 a H_5 současně. Výsledkem je znalost nikoli přesné diference v dolních 4 bitech nultého slova proměnné G, ale možnost diference odlišit od náhodných diferencí pomocí 2^{19} párů M_1 a H_1 a M_5 a H_5.

	Distinguisher of Aumasson		Distinguisher of Guo and Thomsen			
BMW-256	Compression function 2/14	Full BMW-256	Compression function 0/16	Compression function 1/15	Compression function 2/14	Full BMW-256
Distinguished bits	4	0	9	1	1	0
Distinguished Variables	H_{new_0}	/	H_{new_0}, H_{new_5}	H_{new_0}	H_{new_0}	/

Obr.2: Počet odlišitelných bitů kompresní a hašovací funkce BMW256

BMW-512	Compression function 2/14	Full BMW-512	Compression function 0/16	Compression function 1/15	Compression function 2/14	Full BMW-512
Distinguished bits	4	0	11	1	1	0
Distinguished Variables	H_{new_0}	/	H_{new_0}, H_{new_5}	H_{new_0}	H_{new_0}	/

Obr.3: Počet odlišitelných bitů kompresní a hašovací funkce BMW512

Porovnání s naším seriálem

V předchozích 4 dílech jsme otázku rozlišovače na úrovni průběžné hašovací hodnoty neuvažovali, protože jsme se zabývali možnostmi skutečných útoků. I když představené útoky nevedou k použitelným výsledkům na prolomení BMW, jsou to samozřejmě cenné analýzy, neboť ukazují hranice, kam se dá s diferenciální kryptoanalýzou u BMW dostat. Současné útoky mají cenný význam pro analýzu vlastností konstrukce BMW, nikoli jako útoky, což uvádí ostatně i autoři těchto prací
[3]:

"***Conclusion.*** *The compression functions of BMW-256 and BMW-512 do not behave ideally, as they admits strong differential biases. However, these seem difficult to exploit to build a distinguisher (or any other attack) for the hash function, because*

1. *the IV is fixed, hence an adversary cannot choose differences in the chaining values entering the compression function;*
2. *even if differences in the IV could be controlled, the additional "blank" invocation to the compression function would prevent an adversary from observing the output differences of the first compression function."*

a [5]:

final note present in the work of Guo and Thomsen: "*Another interesting problem to consider is to devise distinguishers on other output words than merely* H_0^*. *In particular, a bias on one of the output words* $H_8^* \ldots H_{15}^*$ *would be interesting.*"

Ten, kdo se hlouběji ponoří do studia BMW, uvidí mnohem více podobných přístupů i to, proč musí skončit a na co vlastně „umřou“. Pro zájemce dáváme malý „hint“: příčina je v trojúhelníkových transformacích, které následují po sobě – horní a dolní trojúhelníkové transformace rozprostírají změny proti sobě. Chceme-li co nejmenší změnu v T^U, zapříčiníme největší změnu v T^L, použijeme-li co nejmenší změnu v T^L, způsobíme změnu všech slov v T^U. A navíc, T^L a T^U jsou bijekce, takže změna nastat musí (!), a to v obou (!) transformacích. Toto se nedá obejít jinak než anulováním změn uprostřed – tj. pomocí AddElement. Útok je pak zcela určen tím, jak se výzkumník vypořádá s touto anulací nebo, je-li odvážný, s řízenou změnou ve všech transformacích AddElement, T^L a T^U. Držíme Vám palce, ať jste úspěšnější, než dosavadní útočníci, hodně štěstí!

Literatura

[1] domácí stránka týmu BMW: http://www.q2s.ntnu.no/sha3_nist_competition/start

[2] stránka NIST k projektu SHA-3: http://csrc.nist.gov/groups/ST/hash/index.html

[3] J. P. Aumasson: Practical distinguisher for the compression function of Blue Midnight Wish, Feburary 2010, http://131002.net/data/papers/Aum10.pdf

[4] I. Nikolic, J. Pieprzyk, P. Sokolowski, R. Steinfeld: Rotational Cryptanalysis of (Modified) Versions of BMW and SIMD, March 2010, tento link vypadá podivně, ale funguje, pokud ho vložíte celý do adresy prohlížeče:
https://cryptolux.org/mediawiki/uploads/0/07/Rotational_
distinguishers_%28Nikolic%2C_Pieprzyk%2C_Sokolowski%2C_Steinfeld%29.pdf

[5] J. Guo and S. S. Thomsen: Distinguishers for the Compression Function of
Blue Midnight Wish with Probability 1, March 2010, http://www2.mat.dtu.dk/people/S.Thomsen/bmw/bmw-distinguishers.pdf

[6] Danilo Gligoroski, Vlastimil Klima: On the Computational Asymmetry of the S-boxes Present in Blue Midnight Wish Cryptographic Hash Function, Information on ICT Innovations 2009, Sept. 28 - 30, Ohrid, R. Macedonia, in Danco Davcev and Jorge Marx Gómez (eds): ICT Innovations 2009, Springer, Berlin, Heidelberg, 2010, pp. 391 - 400, http://cryptography.hyperlink.cz/BMW/BijectionsInBMW03-plain.pdf

[7] Danilo Gligoroski, Vlastimil Klima: On Blue Midnight Wish Decomposition, SantaCrypt 2009, Dec. 3-4, 2009, Prague, Czech Republic, Proceedings of SantaCrypt 2009, ISBN 978-80-904257-0-5, pp. 41-51, available on line: http://cryptography.hyperlink.cz/2009/BMWDecomposition04.pdf

B. Dílčí diferenciální vlastnosti zobrazení $A_2(A_1(M))$ ve funkci f_0, v návrhu hašovací funkce BMW

Václav Plátěnka, vaclav.platenka@unob.cz, Univerzita obrany

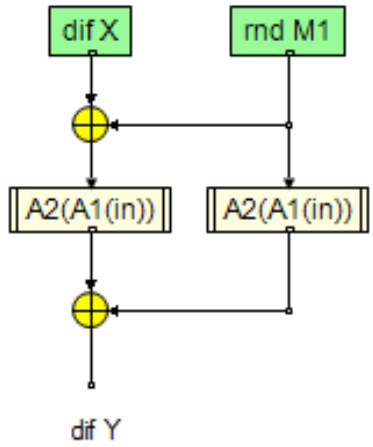
Článek reaguje na výzvy učiněné v příspěvcích čísel 2 a 3 Crypto-Worldu 2010 - Analýza Blue Midnight Wish. Na závěr příspěvku v CW 2/2010 autoři nabádali ke zkoumání diferenčních vlastností funkce $Q_a : M \dashrightarrow Q_a(M) = A_2(A_1(M))$. V příspěvku v CW 3/2010 pak autoři zadali celou řadu úloh z hlediska zkoumání jednotlivých stavebních bloků algoritmu BMW, přičemž úloha D se prakticky shodovala s námětem z CW 2/2010. Tímto článkem tedy reaguji na nadnesenou problematiku a pokusím se alespoň dílčím způsobem přispět k vyvolané diskusi.

Zadání, viz Crypto-World 3/2010, strana 4 a 5, úloha D

Najít blízká řešení $f_0(M_1,H_1) = f_0(M_2,H_2)$, pro $H_1 = H_2$ … shoda na co nejvíce bitech

Vstupní xor diference: $\Delta X = M_1 \oplus M_2$

Výstupní xor diference: $\Delta Y = A_2A_1(M_1 \oplus \Delta X) \oplus A_2A_1(M_1)$ … po úpravě funkce f_0 vzhledem k počáteční podmínce $H_1 = H_2$



Obr. 1: Výpočet výstupní diference ΔY.

Odpověď

Volíme-li ΔX tak, že diference jsou na pozicích bitů $j = k*w$, kde $k = (0, 1, \ldots, 15)$ a $w = 32$ nebo 64 bitů podle verze algoritmu, potom bude platit:

1) Výstupní diference ΔY jsou nezávislé na vstupním bloku M_1! ΔY závisí pouze na ΔX.
2) Pro BMW 512, $n = 16*w$, $w = 64$ platí, že váha výstupní diference ΔY se pohybuje v intervalu <13, 45> (experimentálně ověřeno).

Popisované vlastnosti se týkají všech kombinací 16 bitů na pozicích $k*w$, tj. 2^{16} vstupních diferencí ΔX. Jestliže je $\Delta X = 0$, jedná se o triviální řešení, viz úloha d.

Příklad 1

Pro BMW 512, $n = 16*w$, $w = 64$

ΔX (pro log 1 u všech 16 sledovaných pozic *j*):

0x8000000000000000 0x8000000000000000 0x8000000000000000 0x8000000000000000
0x8000000000000000 0x8000000000000000 0x8000000000000000 0x8000000000000000
0x8000000000000000 0x8000000000000000 0x8000000000000000 0x8000000000000000
0x8000000000000000 0x8000000000000000 0x8000000000000000 0x8000000000000000

Váha ΔX = 16

ΔY:

0x4000001000000008 0x4000040000001000 0x2010000000040000 0x2400000008000000
0xC000000000000000 0x4000001000000008 0x4000040000001000 0x2010000000040000
0x2400000008000000 0xC000000000000000 0x4000001000000008 0x4000040000001000
0x2010000000040000 0x2400000008000000 0xC000000000000000 0x4000001000000008

Váha ΔY = 45.

Platí pro libovolné M_1 , tj. ΔY je stejné, jak je uvedeno výše, pro libovolnou hodnotu vstupního bloku M_1.

Příklad 2

Pro BMW 512, $n = 16*w$, $w = 64$

ΔX:

0x0000000000000000 0x0000000000000000 0x0000000000000000 0x**8**000000000000000
0x0000000000000000 0x0000000000000000 0x0000000000000000 0x0000000000000000
0x0000000000000000 0x0000000000000000 0x0000000000000000 0x0000000000000000
0x0000000000000000 0x0000000000000000 0x0000000000000000 0x0000000000000000

Váha ΔX = 1

ΔY:

0x0000000000000000 0x0000000000000000 0x0000000000000000 0x0000000000000000
0x0000000000000000 0x4000001000000008 0x4000040000001000 0x0000000000000000
0x0000000000000000 0xC000000000000000 0x0000000000000000 0x0000000000000000
0x2010000000040000 0x0000000000000000 0xC000000000000000 0x0000000000000000

Váha ΔY = 13

Platí pro libovolné M_1 , tj. ΔY je stejné, jak je uvedeno výše, pro libovolnou hodnotu vstupního bloku M_1.

Zdůvodnění

Ad 1)

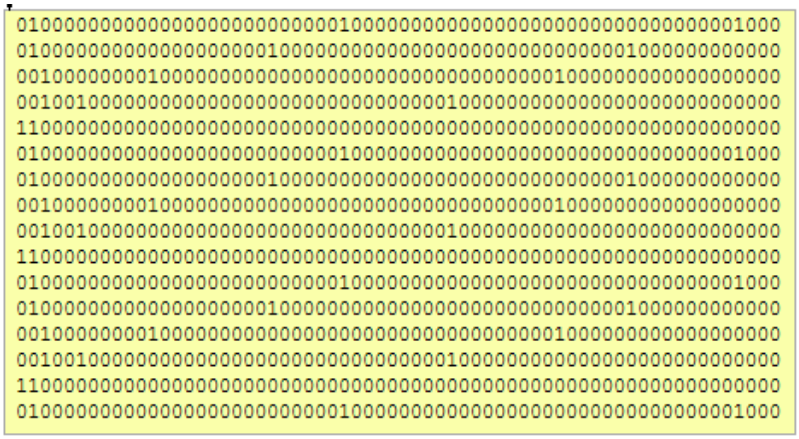
Zobrazení A_1 provádí s jednotlivými vstupními slovy sčítání a odečítání modulo 2^w. Každé výstupní slovo je dáno součtem a rozdílem pětice vstupních slov. Při součtu a rozdílu slov modulo 2^w nedojde k přenosu nejvyššího bitu. Pro nejvyšší bity se tyto operace v případě, že jsou slova až na nejvyšší bit nulová, chovají stejně jako binární sčítání xor. Je-li tedy na vstup zobrazení A_1 přivedena výše popsaná vstupní diference ΔX, tak na výstupu A_1 je diference $\Delta Z = A_1(M_1 \oplus \Delta X) \oplus A_1(M_1)$. S ohledem na popsané vlastnosti sčítání a odečítání modulo 2^w se diference ΔZ mohou projevit pouze na pozicích bitů $k*w$.

Poté následuje zobrazení A_2, kde se tyto diference na výstupu projeví přesně podle napevno daných posuvů, popřípadě rotací v lineárních s-boxech (s_0, s_1, s_2, s_3, s_4). Dobře je vidět čin-

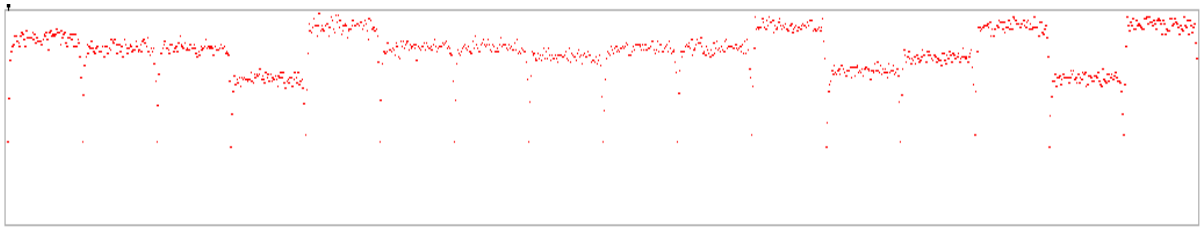
nost zobrazení A_2 pro ΔX z příkladu 1 na výstupu ΔY, viz obr. 2. V tomto konkrétním případě je $\Delta Z = \Delta X$, z čehož plyne, že $\Delta Y = A_2(M_1 \oplus \Delta X) \oplus A_2(M_1)$.

Ad2)

S ohledem na malou váhu uvažované vstupní diference ΔX a také s ohledem strukturu zobrazení A_2A_1, je malá váha ΔY předvídatelná. Na obr. 3 lze sledovat vliv jednobitové vstupní diference na váhu výstupní diference. Vidíme tedy patrný vliv vlastností součtu a rozdílu modulo 2^w popsaných v bodě 1). Je zřejmé, že statisticky se tato vlastnost projevuje nejen u diferencí na nejvyšším bitu vstupních slov, ale méně výrazně i u dalších vysokých bitů. Ověřené poznatky platí analogicky i pro BMW 256, konkrétní interval váhy ΔY nebyl v tomto případě ověřován.



Obr. 2: ΔY z příkladu 1 v binárním tvaru.



Obr. 3: Vliv jednobitové vstupní diference na váhu výstupní diference (*min* = 13, *max* = 36,16, kde *min* a *max* jsou brány jako průměrné hodnoty váhy výstupní diference v závislosti na konkrétní jednobitové vstupní diferenci pro 1000 pseudonáhodných vstupních bloků M_1).

Závěr

Článek se zabývá skupinou vstupních diferencí ΔX, které vedou u zobrazení A_2A_1 ke shodě u většiny bitů, což jak bylo popsáno výše, je předvídatelné. Za povšimnutí ovšem stojí vlastnost, kdy při použití výše popsaných vstupních diferencí ΔX jsou výstupní diference ΔY na vstupním bloku M_1 zcela nezávislé.

Literatura

[1] stránka NIST k projektu SHA-3: http://csrc.nist.gov/groups/ST/hash/index.html

[2] Vlastimil Klima, Danilo Gligoroski: Analýza Blue Midnight Wish – útok na vzor, Crypto-World, 2/2010, http://crypto-world.info/casop12/crypto02_10.pdf

[3] Vlastimil Klima, Danilo Gligoroski: Analýza Blue Midnight Wish – útoky na stavební bloky, Crypto-World, 3/2010, http://crypto-world.info/casop12/crypto03_10.pdf

C. Ze vzpomínek armádního šifranta II.

Jeroným Knížek, knizek@centrum.cz

Volně navazuje na předchozí články *J.Knížek: Paměti armádního šifranta, Crypto-World 10/2007* a *J.Knížek: Ze vzpomínek armádního šifranta, Crypto-World 9/2009.*

ŠO 2. as a VVP

Po absolvování základního šifrantského kurzu na zámku Tloskov u Neveklova na jaře r. 1952 jsem praktikoval na ŠO 2. as v Písku, ač jsem stále kmenově patřil k 22. žen. praporu. Tam jsem rovnýma nohama vpadl do praxe, neboť zde chyběl nemocný pomocník NŠO a převzal jsem jeho zastupování se vším všudy. Zejména to byla šifrová korespondence, běžná administrativa ŠO a nepřetržitá šifrová pohotovost – ve dne/v noci. Každé své vzdálení, činnost, místo a čas návratu jsem musel oznámit operačnímu dozorčímu [OD] sboru, aby pro mne mohl poslat spojku, třeba i do divadla (jiná možnost vyrozumění tehdy nebyla). Tehdy za ministra Čepičky se začala konat letní a zimní soustřední vojsk ve VVP. Náčelník ŠO pplk.Vaněk v té době ve štábu řešil nové podmínky utajení v posádkách, přesuny a umísťování tisíců vojáků i techniky. Proto byla zvýšená i šifrová korespondence, takže jsem si moc neodpočinul. Štábům 2. as a 8. md byly vyhrazeny chalupy v Boleticích, štábu 1. pd v Oticích a štábu 2. pd na Slučím tahu ve VVP Dobrá Voda u Hartmanic.

Vojska si musela podle sovětského vzoru předem vybudovat typizovaná stanová tábořiště s uličkami, nástupními prostory, umývárnami, latrínami, parky pro dopravní i bojovou techniku, stanovišti dozorčích/strážných a zajistit si i zásobování (hlavně vodou). S sebou se vozily bedny s písemnostmi i malé trezory, pro štáby i trochu kancelářského nábytku. Jídelny štábů a vojsk byly oddělené. V Boleticích u kostela na kopci, jemuž jsme říkali Olymp, byla spojovací ústředna včetně dálnopisu a rádiového uzlu. Pro ŠO sboru byla vyhrazena chalupa uprostřed vsi. Vojska sborových útvarů měla tábořiště v Třebovicích, 8. md západně Chvalšin v blátivém Podvoří a 1. pd poblíž Otic. Vojska 2. pd měla společné tábořiště pro divizní útvary, ale každý pluk měl tábořiště vlastní.

Pokud za někým měla přijet z domova návštěva, musela zůstat v nejbližším civilním místě a navštívený měl problémy se k ní vůbec dostat. K návštěvě rodiny se podle možnosti s ohledem na plánované akce udělovaly krátkodobé dovolenky. Letní soustředění ve VVP trvalo asi 6 měsíců, zimní asi 3 měsíce. Postupně se podmínky táboření zdokonalovaly; budovaly se vodovody, polní venkovní učebny, místy byla budována i sportoviště, dokonce závodní bazény a parčíky; uličky tábořišť se dláždily kameny a pískované cesty se denně uhrabávaly. Osazovaly se také obrázkové panely s hesly. Někdy nastaly problémy s rozbahněným terénem, nebo i zdravotní (dyzentérie), kdy musely přijet zdravotnické posily a zjistit zdroje nákazy. Nakonec si na polní život všichni zvykli.

V létě r. 1954 organizovalo MNO velké cvičení ve VVP Doupov, jehož se zúčastnily všechny druhy vojsk. Město Doupov dosud existovalo a obsadilo si jej samo MNO, kdežto všechna vojska se štáby se ubytovaly skrytě ve vyhrazených rajonech. Týl MNO zabezpečil u každého štábu prodejnu Army s běžnými potřebami, ale měla i lihoviny. Byl jsem přidělen jako rozhodčí ŠO strany „modré“ ke 2. pd a byl mi přidělen na zkoušku nově vyvinutý ruční šifrátor Magda s vlastní tvorbou hesla, pro něž bylo třeba provést zákl.

Polní šifrátor Magda

nastavení. Měl vlevo točítko, kterým se nastavovalo písmeno OT a vpravo se muselo jednou otočit kličkou. Otevřený i šifrový text [OT/ŠT] se otiskovaly na pásce dvojité šíře nad sebou, ale stejně pro odeslání spojařem se musel ŠT přepsat na šifrogram (nebo jsem jej mohl diktovat z pásky do telefonu). Takhle jsem jeden dlouhý šifrogram diktoval osobně náčelníkovi ŠO MNO-GŠ plk. Fr. Rubešovi, který zrovna držel šifrovou pohotovost. Bylo to děsně zdlouhavé, o čem se sám přesvědčil a tak po krátkém zkoušení u vojsk byl šifrátor z užívání vyřazen.

O šifrování a utajování

Před šifrantským kurzem r. 1952 jsem prakticky o šifrové službě téměř neslyšel. Pamatuji, jak jsem nastoupil zákl. vojenskou službu r. 1950 ke 2. ženijnímu pluku v Písku. Po přijímači a přísaze byla zahájena naše poddůstojnická škola (PŠ), a právě začala Čepičkova velká reorganizace armády, spojená s redislokací vojsk. V té době ještě v budově budoucího 2. as fungovala filiální nemocnice, kam jsme viděli okny. Náš ženijní pluk měl spoustu materiálu – po kasárnách, na cvičištích, na řece Otavě, v mobilizačních skladech po městě a okolí. Přijely kolony študebakrů, a my z PŠ jsme byli pověřeni všechen materiál odvážet do přistavených vlaků. Na nádraží za námi vozili stravu a my nakládali, až se z nás kouřilo. Na chodbě naší PŠ měl kancelář nadporučík Klestil a stále mu tam nosili nějaké telegramy a on běhal na štáb. Později jsem se dověděl, že to byl plukovní šifrant. Během jednoho týdne bylo vše hotovo; zůstal tu jen náš nově organizovaný sborový 22. ženijní prapor a přibyly dělostřelecký pluk, protiletadlový oddíl, spojovací prapor, velitelská jednotka sboru a později raketometný oddíl. Sousední nemocnice byla zrušena a nastěhovalo se tam nově organizované Velitelství 2. armádního sboru (jemuž velel generál Patera a po něm gen. Sedláček), podřízené Velitelství 1. vojenského okruhu v Praze; jeho podřízené svazky jsem již vzpomínal. Po absolvování PŠ jsem byl v aspirantské škole v Seredi nad Váhom (s výcvikem v Bratislavě na Dunaji a ve VVP Lešť [Oremov Laz]). Po návratu k praporu jsem byl zakrátko vyslán do šifrantského kurzu v Neveklově [Tloskov]. Zde jsem teprve čerpal vědomosti o organizaci armády a činnosti šifrantů.

Pracovišť šifrantů bylo jako šafránu. Byly na štábech brigád a výše (jinde výjimečně), podřízeni jen náčelníkovi štábu; jeden šifrant připadal asi na 3-5 tisíc vojáků. Z počátku to byl tzv. Referát šifrové služby s číslem voj. odbornosti 8. (tj. absolvent VŠ, kterých se všude nedostávalo). Po čase byl název změněn na Šifrovací oddělení (ŠO), pak na 6. oddělení a naposledy na 8. oddělení (jako v SSSR). Vnitřně jsme všichni byli pracovníky ŠO (šifrového orgánu) a funkčně náčelník či pomocník, mechanik, někde PNPSS (pomocník pro speciální spojení). Podléhali jsme zvláštnímu režimu. Pokud vím, kontrarozvědka po prvním názvu Obranné bezpečnostní zpravodajství (OZ či OBZ) byla přejmenována na 5. oddělení a nakonec na OVKR, ale s nimi jsme neměli nic společného (jen nás sledovala a prověřovala do funkce).

Kromě ŠO zabezpečovaly utajené spojení štábů vyšších jednotek od poloviny 60-tých let ještě spojovací uzly ZAS (v péči spojovacího vojska), což byl speciální sovětský telefonní a dálnopisný systém se zvlášť zabezpečenými (zapečetěnými) linkami a přístroji, kde se mohly přenášet utajené hovory nejvýše povahy služebního tajemství (Tajné=T), kdežto PT jen přes ŠO. Podobně fungoval i utajený telefon VČ. Nezávisle na běžné linkové síti ve státě existovala i tzv. zvláštní telefonní síť (ZTS), jejíž stanice byly přidělovány důležitým řídícím funkcionářům do bytů i kanceláří a jimi se uváděly do činnosti pohotovostní plány v případě mimořádných situací, včetně vojenských. Ústředna ZTS byla v Černínském paláci na

Hradčanech. Na mnohých vrcholech poblíž zájmových center byly v neustálé činnosti dálkové radiostanice, které pohotovostní systém zdvojovaly a podobně byly připraveny další telefonní a dálnopisné okruhy ke spuštění na signál přes poštovní síť (např. u KVS). Všechny spojovací prostředky podléhaly jednotnému řízení a kmitočtové službě a měly připravené a většinou i vybavené záložní stanoviště; do systému patřilo i rozhlasové a televizní vysílání, varovný systém a všechny pohotovostní služby.

Jak již jsem uváděl, ochranu utajovaných skutečností ve státě řídilo Ministerstvo vnitra, takže alternativně jako uvnitř armády byla organizována šifrová služba i v dalších resortech podle stejných předpisů

Kategorie šifer a působnost ŠO

Šifrová služba a utajování byly centrálně řízeny Ministerstvem vnitra, nikoli však od počátku, ale až začátkem 50. let. Musím se také zmínit o kategorizaci šifer. Šiframi 1. stupně byly nazývány šifrové systémy a prostředky, s kterými směli pracovat jen šifrové orgány/pracoviště (ŠO), kdežto za šifry 2. stupně byly považovány signální a hovorové tabulky a také kódování map. Šifry 1. stupně byly chráněny jako Přísně tajné (státní tajemství), a ne každý ŠO měl všechny druhy k dispozici. Šifry 2. stupně byly podle závažnosti užívání označovány jako Tajné (služební tajemství) nebo Přísně tajné. Pracoviště ŠO i jeho pracovníci podléhaly zvláštnímu bezpečnostnímu režimu a jeho hrubá porušení se řešily soudně. Šifranti všech stupňů byli pověřeni zpracovávat znalecké posudky ze svého oboru. Málokdo si dovolil překročit utajovací režim, a pokud se tak stalo, do smrti toho litoval. Přesto jsem několik posudků musel zpracovat, bylo to hlavně při ztrátách spisů či předpisů.

K tajným věcem (dokumentům, utajovaným zbraním ap.) měli přístup i třeba vybraní občanští pracovníci. S Přísně tajnými [PT] a Přísně tajnými zvláštní státní důležitosti [PTZD] věcmi však směli pracovat jen k tomu zvlášť prověřené, určené a sledované osoby. Podobně to bývá organizováno ve všech státech, tedy i armádách.

Přímými nadřízenými ŠO byli náčelník daného štábu (NŠ) a také náčelník nadřízeného nebo zvlášť určeného ŠO. Několik roků byla šifrová služba podřízena Náčelníkovi spojovacího vojska. Pracoviště ŠO byla téměř u všech druhů vojsk, tedy i u svazků letectva a PVOS, Raketových vojsk a dělostřelectva, u Pohraniční stráže, Železničního vojska, atd. Pracovníci ŠO se navzájem se souhlasem nadřízeného ŠO mohli zastupovat a odborně si pomáhat. Například ve službě na ŠO sušické motostřelecké divize jsem spolupracoval s ŠO tamní brigády Pohraniční stráže, anebo u 1. td ve Slaném jsem spolupracoval s ŠO rádiového praporu v Kladně, u KVS Liberec jsem spolupracoval s ŠO KVS Ústí n. L. nebo Hradce Králové, ale protože jsem tam byl šifrantem jediný, musel jsem si vycvičit náčelníka 1. oddělení k zastupování v akutních případech. Každé ŠO muselo zabezpečovat svou službu (včetně školení a kontrol) i pro určené jednotky rozmístěné v jeho teritoriu a k němu si museli náčelníci dotyčných jednotek pro šifrovky na vyzvání přijet a stejně je i vrátit (nesměly se posílat poštou ani kurýrem, došlo by tím k ohrožení bezpečnosti šifry 1. stupně).

Pokračování v e-zinu Crypto-World 6/2010

D. Tajemství ukryté v 11-ti pohlednicích

Marta Janošová, 261281@mail.muni.cz, studentka Filosofické fakulty Masarykovy univerzity

Už jako malá holčička jsem často chodila s rodiči do antikvariátů. Obchůdky s antikvárním zbožím jsem vnímala jako tajemné místo, kde člověk může objevit nejrůznější poklady a to od starých knih s překrásnými ilustracemi třeba od Zdeňka Buriana až po novější knihy za levný peníz. Mýlí se však ten, kdo si myslí, že v antikvariátech mají pouze knížky, není tomu tak. Antikvariát je totiž místo, kde můžete zakoupit mapy, překrásné grafiky, fotografie ze začátku dvacátého století, bankovky, pohlednice a mnoho dalšího. Je to totiž ten druh obchodu, který se vždycky liší, nikdy nenarazíte na dva totožné antikvariáty a i v tom je určité kouzlo.

Když jsem byla malá, tak jsem měla slabost pro pohlednice a to od starých až po nové s líbivými obrázky. Postupem času jsem zjistila, že staré pohledy jsou často mnohem zajímavější, než ty nové, neboť člověk se z nich dozví mnohem více věcí. Dobové pohlednice nám ilustrují, jak lidé dříve žili, jaké nosili oblečení, jak vypadaly města a vesnice atd.

Avšak i v první polovině století měli lidé pohlednice pro „potěšení“, pohlednice s milostnou tématikou, s tématikou svátků jako jsou například Vánoce, jmenin a narozenin. Tyto pohlednice jsou často zajímavé především svým obsahem, například když mládenci psali zamilovaná psaníčka svým dívkám a naopak nebo když si příbuzní sdělovali jak se kdo má a co dělá anebo také když si ženy do pohlednic psaly recepty. Proto není správné tato psaní hned zavrhovat, neboť mnohdy mohou ukrývat velmi pestré a spletité lidské osudy. Díky pohledům, které jsem nakoupila před pár lety v antikvariátu, jsem měla možnost jeden takový pozoruhodný lidský příběh poznat.

Když mi bylo asi 18, tak jsem navštívila antikvariát, ve kterém prodávali pohledy a to s nejrůznější tématikou. Při jejich prohlížení mě zaujalo několik, které si mezi sebou psali voják a jeho dívka a to v letech 1929 – 1931. Psaníčka mladých milenců jsou velmi často sama o sobě velmi zajímavá, ale tyto byly opravdu výjimečné – části jejich obsahů byly totiž psány šiframi. Musím přiznat, že mě to velmi zaujalo, vždycky jsem měla kladný vztah k šifrování (asi mě velmi ovlivnily dobrodružné filmy s hledáním pokladů, kde často hrdinové musejí rozluštit tajné zprávy pomocí nějakého klíče, aby získali ukrytý poklad), ale přesto všechno jsem se nikdy nenaučila ani morseovku.

Pohledů s šiframi jsem v antikvariátu objevila celkem 11, zakoupila jsem je a doma jsem se jimi kochala. Obsah byl velmi zajímavý, ale přerušovaný šifrovaným textem. Moc mě mrzelo, že nevím, co kódy znamenají a toužila jsem tomu přijít na kloub. Jelikož jsem chtěla mít v obsahu aspoň trochu jasno, když jsem nemohla porozumět šifrám, tak jsem si seřadila pohledy podle data. Poté, co jsem toto učinila, jsem si všimla, že zašifrovaný text nebyl vždy složitý jako na některých pohledech. Všimla jsem si, že zpočátku používali poměrně jednoduché znaky, které byly často prokládány normálními písmenky. V ten moment mi svitla naděje, že přece jen budu moci šifrám porozumět a pustila jsem se do jejich luštění.

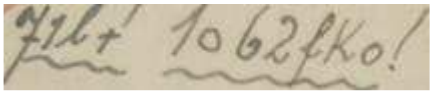
Na úvod bych vám ráda představila dvojici mladých lidí, která si takto psala. Slečna se jmenovala Josefína Halmová a bydlela v Boleradicích (vesnice mezi Hustopečemi a Klobouky u Brna) a její milý byl František Kaisler - vojín, který se účastnil kursu specialistů na vojenském leteckém učilišti v Prostějově.

Jméno slečny mi velmi pomohlo, protože se z něj skládaly šifry pohledu nejstaršího data. Rozluštění tedy nebylo příliš složité, protože se šifrovými znaky teprve začínali a vymýšleli si je. Jako příklad bych mohla uvést třeba, že písmeno T nahradili číslem 3, protože trojka začíná písmenem T, pak I a J nahradili číslem 1, protože se tato písmena číslici 1 podobají. Postup nahrazení písma čísly, na které dané číslo začíná, použili u více písmen, například číslo 9 značilo písmeno D, písmenko O nahrazují číslem 8 a P zase číslem 5. Některé znaky podobnou logiku nemají, ale jsou založeny zase na jiném principu, například A nahradili znamínkem +, někdy i písmenem x. Toto pravděpodobně učinili z toho důvodu, že písmeno A má spojovací funkci a znaménko plus také spojuje čísla a čte se jako „a“, tudíž je to vcelku logické. Některé znaky se postupem jejich dopisování dále utvářely a měnily, takže ne vždy byl šifrovací znak zachován po celou dobu jejich psaní.

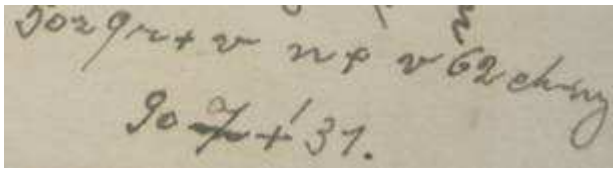
První, nejstarší, pohled byl psán 11. 6. 1929 v Brně. Pohled byl adresován Josefce Halmové do Boleradic a psal jej její milý – František Kaisler. Avšak většina pohledů byla psána Josefkou Františkovi. Pohledy psané Josefínou byly často mnohem více obsáhlejší a také v nich bylo mnohem více šifer, což je konkrétně pro milovníky šifer jen a jen dobře.

Šifry byly psány ze začátku opravdu velmi jednoduše, takže si šlo význam sdělení velmi snadno domyslet. Těchto pár znaků mi velmi pomohlo k rozluštění textu všech pohledů. Obávám se totiž, že bez nich by se mi to možná ani nepodařilo, proto se prvnímu pohledu budu věnovat více, neboť byl pro celé dešifrování klíčový.

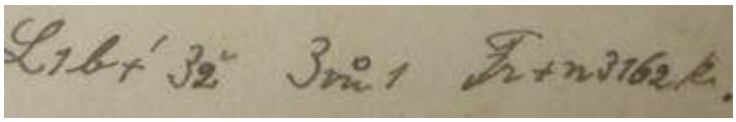
Př:



Překlad: Milá Josefko!

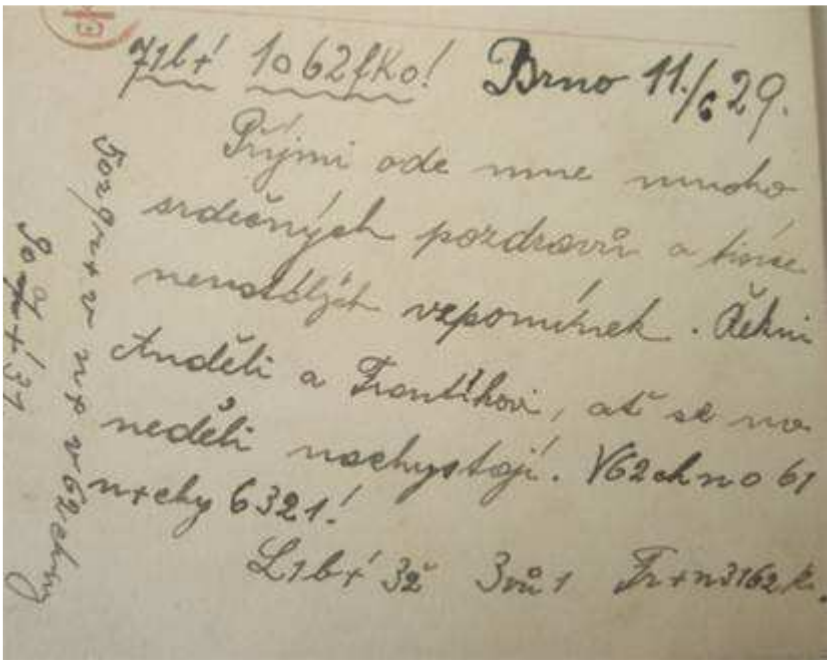


Překlad: Pozdravuj všechny domácí.



Překlad: Líbá Tě Tvůj František.

Pohled vcelku:



Ústředním motivem většiny pohledů je zamilovaná dvojice a byly pravděpodobně vytvořeny během dvacátých let.

(Přeložené šifry jsou vyznačené kurzívou) Pohled byl psán 11. 6. 1929 v Brně.

Milá Josefko!

Příjmi ode mne mnoho srdečných pozdravů a tisíce neustálých vzpomínek. Řekni Anděli a Frantíkovi, ať se na něděli nachystají. *Všechno si nachystej!*

Líbá Tě Tvůj František

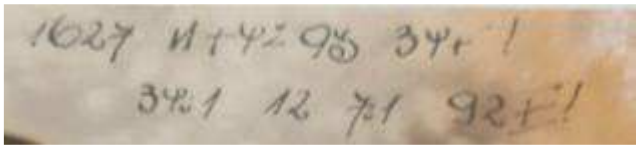
Pozdravuj všechny domácí.

Bohužel z daného textu nelze odvodit více, třeba co přesně si Josefína měla nachystat a také co přesně se mělo v neděli konat. Dále, proč byl František v Brně, zda to bylo spojeno s jeho vojenskou službou nebo byl v Brně z úplně jiných důvodů. Některá tajemství musí prostě zůstat navždy skryta.

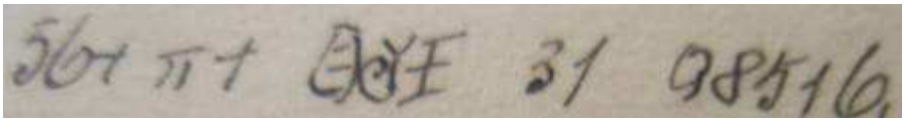
Šifry se postupem času stávaly čím dál více propracovanější a díky tomu byl i obsah pohledů tím více zajímavější. Vybrala jsem proto pár pohledů, které rozhodně stojí za pozornost.

Následující pohled patří k těm, které byly na šifry i na zajímavý obsah nejbohatší a z toho důvodu se budu jednotlivým šifrám věnovat detailněji, než u dalších pohledů. Myslím si, že na základě vyobrazených šifrových textů by každý mohl rozluštit, a to bez větších problémů, šifry v dalších pohledech, které si Josefka a František mezi sebou psali. Pohled psala Josefka Františkovi a to 8. 12. 1929 v Boleradicích.

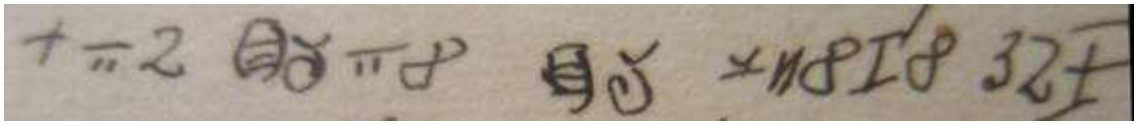
Ukázky konkrétních šifer v pohledu:



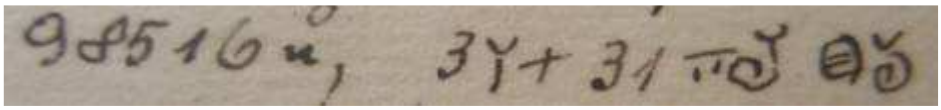
Překlad: Jsem navždy Tvá!
Tvůj je můj dech!



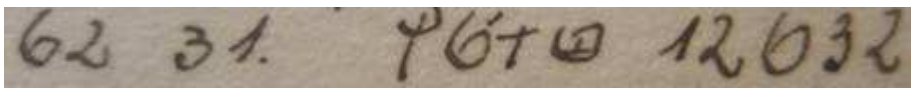
Překlad: Psala Bych Ti dopis,



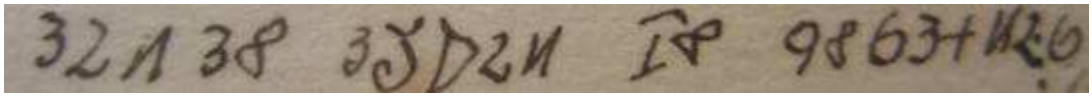
Překlad: ale bylo by mnoho těch



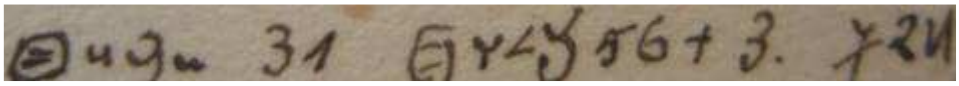
Překlad: dopisů, tratily by



Překlad: se Ti. Však ještě



Překlad: tento týden ho dostaneš.



Překlad: Budu Ti brzy psát. Jen*

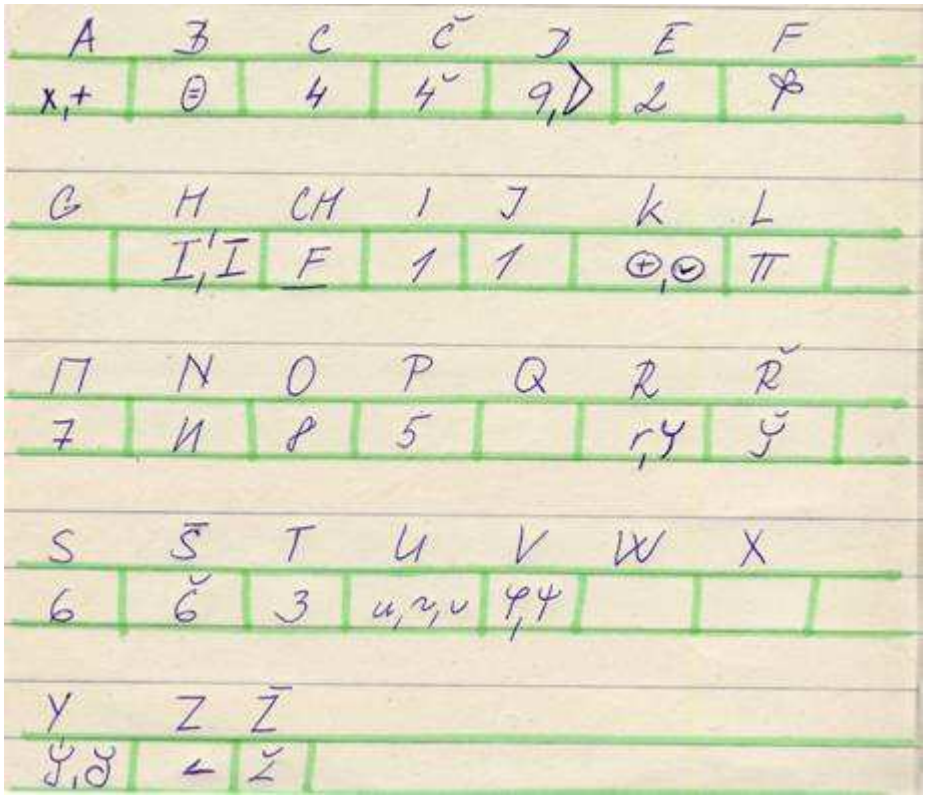
Překlad: Ty mi také brzy piš.

* Zde si můžete všimnout, že je v šifře chyba. Správně by místo čísla 7 mělo být číslo 1.

Co se týče diakritiky, tak někde byla dodržována, ale v mnoha případech tomu tak nebylo. Každopádně šifrám se dá rozumět i tak a to bez větších problémů.

Při luštění jsem si připravila převodovou tabulku (klíč) a do ní jsem si pak vpisovala znaky, které používali pro šifrování. Některé znaky prošly během jejich dopisování vývojem a tak často v klíči narazíte na více variant šifer. Někdy také použili pro jedno písmenko dva různé znaky a to dokonce v jednom pohledu, mohli jste si toho všimnout v příkladech šifer, které jsem uvedla výše. Chci ještě poznamenat, že některá písmena k sobě šifru nemají. Je to hlavně u těch písmen, která nejsou tak hojně používaná v běžné mluvě – např. X, Q atd.

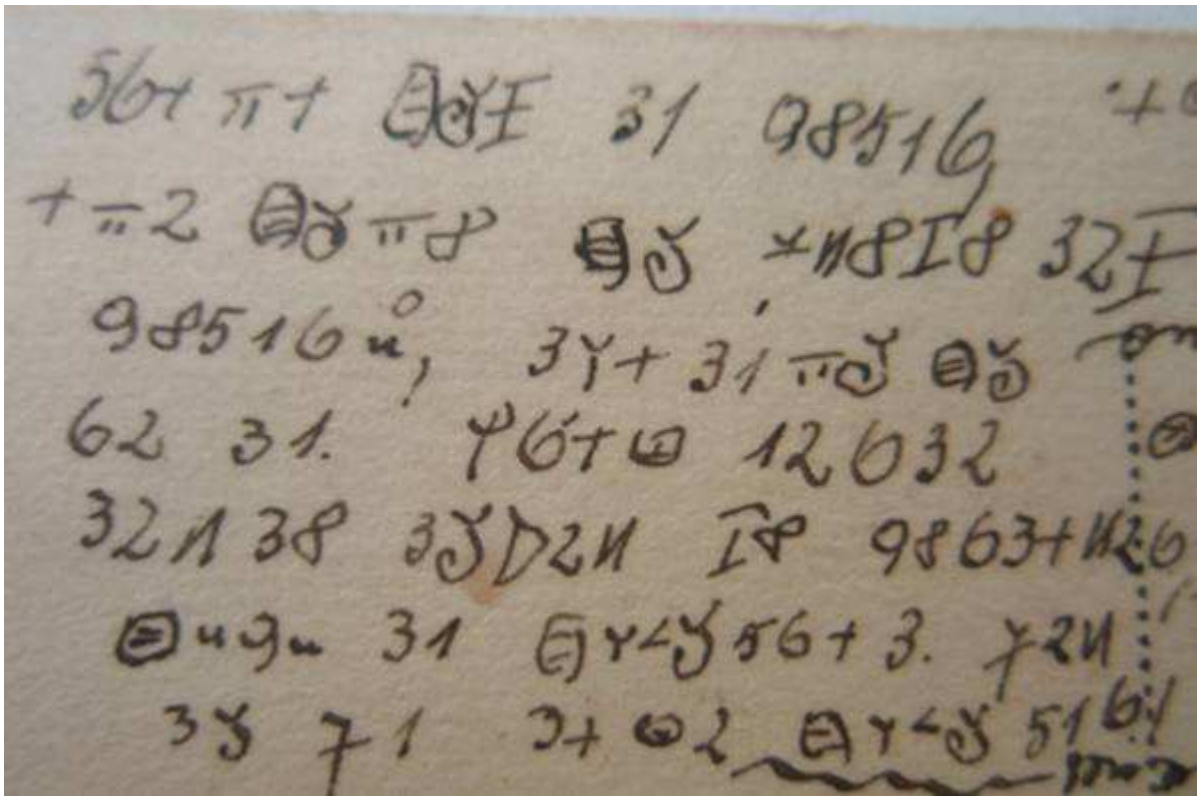
Klíč k šifrám:



Pohled vcelku:

*

* U druhého obrázku si můžete vyzkoušet dešifrování šifer, uvidíte, že to není nic těžkého. ☺ K dispozici vám může být klíč (viz výše).



Popis pohledu:

1) Nad hlavami dvojice je šifrou napsáno: *Jsem navždy Tvá! Tvůj je můj dech!*

2) Na této detailní fotce je zabrána růže a vedle ní ruka slečny, na které je šifrou napsáno: *Na té růžičce máš sladkou pusinku.* Všimněte si, že na růži je vyznačen křížek, který ukazuje místo, které Josefka pro Františka políbila.

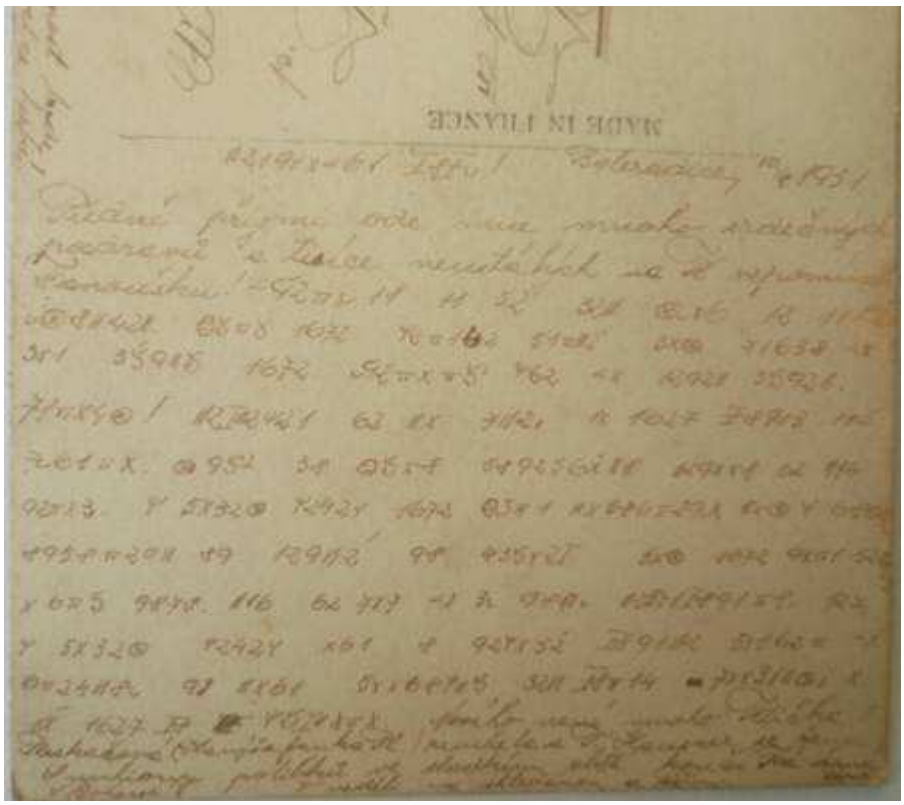
3) Pohled je adresován Vojínovi Františku Kaislerovi, který se účastnil kurzu specialistů na vojenském leteckém učilišti v Prostějově. Pod datem je obráceně napsáno: Teď budem drteť u nás. (Bohužel přesně nevím, co slovo „drteť“ znamená, je možné, že jsem to špatně přečetla.)

Drahý Frantíku!
Předně přijmi ode mne mnoho srdečných pozdravů a tisíce neustálých na Tě vzpomínek.
Mnohokrát Ti děkuji za dopis, kterým jsi mě potěšil, tím hlavně, že jsi již zdráv a že jsi to ode mne laskavě přijal. Ráda Ti vždy způsobím radost. Jsem ráda, že nemoc nebyla horší, však jsem měla veliký strach. Ten Tonda s tím J. K., co se podělali, nevím. Ale Jenda byl zpitý. T. mu něco řekl, co nevím a bylo to. Znáš Káňovy bijáky. Ale mlč! Vaši žádný dopis nedostali. Říkala jsem jim, aby Ti psali, prý Ti dnes pošlou buchtu. Frantíku, prosím Tě, k pilotům se nedávej! Aby ses také nezabil. Děkuji Ti za tu podobenku, jíž jsi mě též potěšil. Vaši měli včera dodírek. Nebyla jsem včera na nich ani jednou. Blaží mě pomyšlení, že nezrušila jsem slovo dané Tobě. Mluvíš v dopise o nějakém oplácení? Nemám strach, že mi to zůstaneš dlužen. Však Ty mi to jednou i z úroky splatíš. *Až mě pojmeš za svou choť!* Všichni domácí děkují za pozdrav a též Tě srdečně zdraví. *Ten balík jsem posílala já*, ale aby to nebylo zase roztrháno, tak adresu *napsal* Petr. *S miliony vroucích polibků končí věčně Tvá Josefka.*
Sbohem!
Na shledanou. Na Vánoce.

4) Tento obrázek jsem již detailněji rozebrala výše, zde však máte šifry vcelku – nerozkouskované po jednotlivých řádcích.

Poslední pohled, který jsem pro vás vybrala je zároveň poslední ze série 11 pohledů, které si mezi sebou psali Josefka s Františkem. Na pohledu je především zajímavé to, že František už nebyl na vojně, ale pracoval v Brně v Králově poli a také, že je téměř celý napsaný pomocí šifer.

Pohled vcelku:



1) Celkový záběr na obrázek. Tento obrázek je jedinečný v tom, že na něm (jako na jediném ze všech 11 pohledů) není dvojice zamilovaných mladých lidí, ale pouze jediná postava a to mladá slečna držící v rukou květiny. Obrázek na přední straně pohledu je dobarvován.

2) Pohled je adresován Františkovi Kaislerovi do Králova Pole v Brně na ulici Budovcova č.2, kde František pracoval jako zahr. (pravděpodobně zahradní :o)) příručí u pana Kaliny. Nad adresou je obráceně napsáno: Ta zahradní slavnost bude 6. září. Bude to velice pěkné. Tento pohled byl vyroben ve Francii.

3) Pohled byl napsán 10. 8. 1931 v Boleradicích.

Obsah pohledu:

Nejdražší hochu!
Předně přijmi ode mne mnoho srdečných pozdravů a tisíce neustálých na Tě vzpomínek.
Fanoušku! *Sděluji Ti, že ten kurs je již ukončen. Byly jsme velice pilné, tak místo za tři týdny jsme udělaly vše za jeden týden. Miláčku! Nehněvej se na mne, já jsem chodit již musela. Když to bylo podepsáno, nedalo se nic dělat. V pátek večer jsme byly naposled a pak v sobotu odpoledne od jedné do čtyřech. Pak jsme daly peníze a šly domů. Nic se nám za tu dobu nepřihodilo, jen v pátek večer asi o deváté hodině přišel za slečnou do naší pracovny ten holič Martínek a já jsem ho vyhnala.*
Nového není mnoho. Tetička Pleskačová (?) zemřela a T. Hausner se žení.
S miliony polibků ve sladkém obětí končí Tvá věrná Pepička.
Sbohem
V neděli na shledanou se těším.

Pokud vás tento článek zaujal a rádi byste si prohlédli více pohledů a přečetli i více o nich, tak je najdete na mém blogu http://www.inflow.cz/blogs/marta. Je zde podrobně popsán každý z 11 pohledů, věnovala jsem se zde také ostatním souvisejícím věcem, jako například místu, kde František studoval a třeba Boleradicím – vesnici, ve které oba žili. Dozvíte se zde také o mé návštěvě jmenované vesnice a také i o tom jak to s Josefínou a Františkem dopadlo, zda se vzali a zda měli spolu děti. Přeji vám příjemný zážitek ze čtení, který snad budete mít, pokud se rozhodnete navštívit můj blog.

E. Chcete si zaluštit? Díl 5.

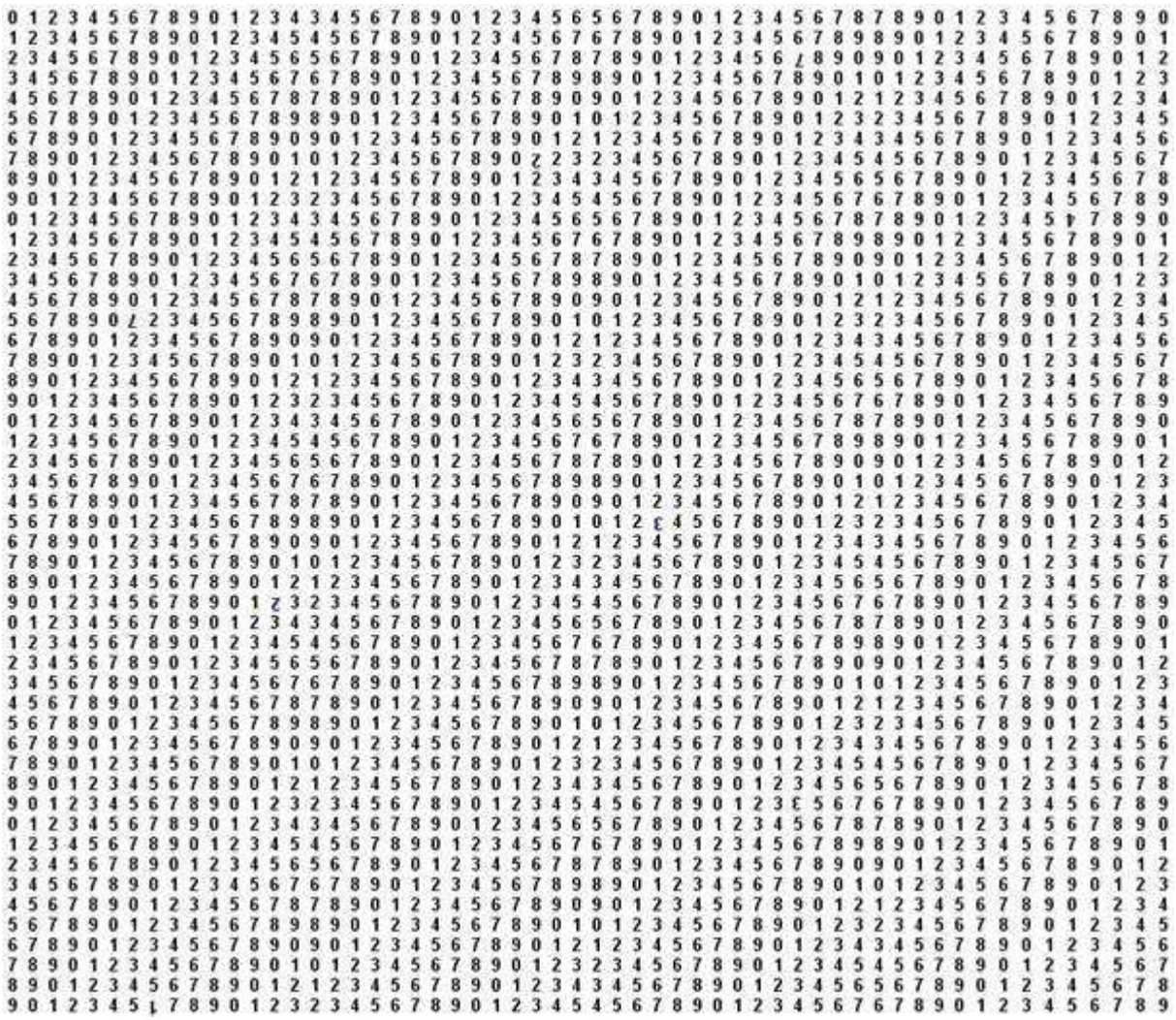
Martin Kolařík (marram.mail@gmail.com)

Květnová dávka luštění. Za minulý měsíc jsem v geocachingu narazil na opravdu povedené způsoby ukrytí informací, bohužel se vždy jednalo o šifry, které člověk získá až přímo na místě, takže jejich zveřejněním bych prozrazoval to, co má zůstat překvapením. Proto jsem musel sáhnout do archívu a vybral jsem jiné povedené kousky, ale ty v terénu byly přeci jen o kousek lepší. Nechcete tedy přeci jen začít také „kešovat“. :)

SEDM SEGMENTU (http://coord.info/GC1J6DB)

Hra s pismeny (http://coord.info/GC239DX)

Prosecka sifra / Prosek code (http://coord.info/GC25A61)



Přeji úspěšné luštění a šťastný lov.

Martin

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

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

Problematika infrastruktury veřejných klíčů (PKI)

Kurz seznámí účastníky s principy fungování PKI z různých aspektů. Účastník se seznámí se základními principy asymetrických šifer, s prací s certifikáty, fungováním certifikačních autorit, s požadavky zákona o elektronickém podpisu na různé subjekty a aplikací tohoto zákona v praxi, bude seznámen s technickým a legislativním pohledem na důvěru v certifikáty a přehledem různých druhů útoků na PKI (od praktických po teoretické). Součástí budou některé jednoduché praktické dovednosti – zejména práce s certifikáty (generování, export, import, podpis) a CRL.

Garant: **Pavel Vondruška**

Cena Základní cena: 2 000,00 Kč
Základní cena včetně DPH: 2 400,00 Kč

Datum	Čas	Lektor	Volná místa	Přihlásit
17.06.2010	09:00–17:00	Pavel Vondruška	????	http://www.nic.cz/akademie/course/15/detail/

Cíl kurzu

Po absolvování kurzu bude účastník:

- rozumět principu asymetrických šifer
- znát základní informace k budování PKI a CA
- znát vybrané aspekty zákona o el. podpisu (typy certifikátů, podpisů, certifikačních autorit atd.)
- umět vygenerovat certifkát a zacházet s ním a 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)
   - typy poskytovatelů (kvalifikovaný, akreditovaný)
   - typy certifikátů (obyčejný, kvalifikovaný, systémový kvalifikovaný certifikát

3. Certifikační autority
   - přehledy poskytovatelů (ČR, SR)
   - jak pracují a co jej jejich úkolem

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 Entrust, Adobe
   - podpis MS prostředí

7. Elektronická fakturace, archivace, ISDS

8. Otázky bezpečnosti elektronických podpisů

9. Obecné otázky bezpečnosti
   - Bezpečnost RSA
   - Bezpečnost hashovacích funkcí

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

G. Call for Papers Mikulášská kryptobesídka

2. – 3. prosinec 2010, , Hotel Olympik Praha

http://mkb.buslab.org

BUSLab CEPIA TECHNOLOGIES UNS

Základní informace

Mikulášská kryptobesídka se koná letos již podesáté. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *2. prosince 2010* a (b) půldne prezentací příspěvků a diskusí v pátek *3. prosince 2010*. Pro workshop jsou domluveny zvané příspěvky:

- Danilo Gligoroski (NTNU, Norsko) na téma SHA-3 a BMW.
- Paul Leyland (Cepia Technologies, ČR) na téma GPU a kryptanalýzy.
- Tomáš Rosa (Raiffeisenbank a UK, ČR) na téma bezpečnosti RFID.
- Dan Cvrček (Apoideas, UK a VUT v Brně, ČR) na téma kryptografie v bankovnictví.
- Petr Hanáček (VUT v Brně, ČR) a Petr Švenda (MU, ČR) na téma kryptografie v bezdrátových senzorových sítích.

Podrobné informace, včetně pokynů k registraci, se budou průběžně objevovat na www stránkách workshopu: http://mkb.buslab.org.

Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Oba druhy návrhů mají požadovaný rozsah 5-15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER, nebo STANDARD TRACK.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a to tak, aby na uvedenou adresu přišly nejpozději do *30. září 2010*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2010 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *26. října*. Příspěvek pro sborník workshopu pak musí být dodán do *18. listopadu*.

Důležité termíny

Návrhy příspěvků:	30. září 2010
Oznámení o přijetí/odmítnutí:	26. října 2010
Příspěvky pro sborník:	18. listopadu 2010
Konání MKB 2010:	2. – 3. prosince 2010

Mediální partneři

Programový výbor

Otokar Grošek, STU Bratislava, SR
Vlastimil Klíma, KNZ, ČR
Jan Krhovják, Cepia Technologies, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Luděk Smolík, Siegen, SRN
Martin Stanek, UK, Bratislava, SR
Pavel Vondruška, Telefónica O2 & UK, ČR

H. KEYMAKER – studentská soutěž

v rámci workshopu Mikulášská kryptobesídka

2. – 3. prosinec 2010, Hotel Olympik, Praha
http://mkb.buslab.org

BUSLab

Mikulášská kryptobesídka se koná letos již podesáté. Je zaměřena na podporu úzké spolupráce odborníků se zájmem o teoretickou a aplikovanou kryptografii a další příbuzné oblasti informační bezpečnosti. Hlavním cílem je vytvořit prostředí pro neformální výměnu informací a nápadů z minulých, současných i budoucích projektů. Cítíme potřebu setkání expertů s jejich kolegy bez obchodních vlivů, starostí s (potenciálními) zákazníky, šéfy a dalšími rozptylujícími faktory. ;-)

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *2. prosince 2010* a (b) půldne prezentací příspěvků a diskusí v pátek *3. prosince 2010*. Pro workshop jsou domluveny zvané příspěvky:

- Danilo Gligoroski (NTNU, Norsko) na téma SHA-3 a BMW.
- Paul Leyland (Cepia Technologies, ČR) na téma GPU a kryptoanalýzy.
- Tomáš Rosa (Raiffeisenbank a UK, ČR) na téma bezpečnosti RFID.
- Dan Cvrček (Apoideas, UK a VUT v Brně, ČR) na téma kryptografie v bankovnictví.
- Petr Hanáček (VUT v Brně, ČR) a Petr Švenda (MU, ČR) na téma kryptografie v bezdrátových senzorových sítích.

KEYMAKER – Pokyny pro autory

Přijímány jsou příspěvky zaměřené především na oblasti kryptoanalýzy, aplikované kryptografie, bezpečnostních aplikací kryptografie, počítačové a komunikační bezpečnosti a dalších souvisejících oblastí. Návrhy se přijímají odděleně pro sekci KEYMAKER (studentská soutěž) a pro hlavní program workshopu. Příspěvek pro KEYMAKER má požadovaný rozsah 5 -15 stran A4 a připravenost pro anonymní hodnocení (bez jmen autorů a zjevných odkazů). Identifikační a kontaktní údaje prosím pošlete v těle e-mailu s příspěvkem jakožto přílohou a jasným označením KEYMAKER. Přijímány jsou články, bakalářské či diplomové práce, nebo jiná kvalitní ucelená díla, kde v případě rozsahu nad 15 stran požadujeme výtah podstatného obsahu v max. rozsahu 8 stran, s vlastní prací jako přílohou.

Mezi autory nejlepších příspěvků PV rozdělí *finanční odměny v celkové výši 150 tisíc Kč*. Oceněno bude min. 3 a max. 7 příspěvků. Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *30. října*. Příspěvek pak musí být prezentován na workshopu.

Šablony pro formátování příspěvků pro Word a LaTeX lze získat na www stránkách workshopu: http://mkb.buslab.org. Příspěvky mohou být napsané v češtině, slovenštině, nebo angličtině.

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu PDF, příp. RTF a to tak, aby na uvedenou adresu přišly nejpozději do *30. září 2010*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2010 – navrh prispevku KEYMAKER“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Důležité termíny

Návrhy příspěvků:	30. září 2010
Oznámení o přijetí/odmítnutí:	26. října 2010
Příspěvky pro sborník:	18. listopadu 2010
Konání MKB 2010:	2. – 3. prosince 2010

Mediální partneři

Programový výbor

Martin Drahanský, VUT v Brně, ČR
Otokar Grošek, STU Bratislava, SR
Petr Hanáček, VUT v Brně, ČR
Vlastimil Klíma, KNZ, ČR
Jan Krhovják, Cepia Technologies, ČR
Vašek Matyáš, FI MU, Brno, ČR – předseda
Luděk Smolík, Siegen, SRN
Martin Stanek, UK, Bratislava, SR
Pavel Vondruška, Telefónica O2 & UK, ČR

I. O čem jsme psali v květnu 2000 – 2009

Crypto-World 5/2005

Příloha : zpráva vysílaná radioamatérskou stanicí GB2HQ - nedele_30m.wav

Crypto-World 5/2006

Crypto-World 5/2007

Crypto-World 5/2008

Příloha:
1) Mikulášská kryptobesídka (4.-5.12.2008): CFP_MKB2008_May.pdf
2) Příloha k článku „Príklad útoku na podpisovaný dokument … “ : priklad.bmp

Crypto-World 5/2009

Příloha: Call for Papers Mikulášská kryptobesídka 2009 - CFP_MKB2009.pdf

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
Stálí přispěvatelé:	Vlastimil Klíma
	Pavel Vondruška
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
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/
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
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/