Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 9, číslo 4/2007 **15. duben 2007**

4/2007

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1262 registrovaných odběratelů)

Obsah : str.

Poznámka:
omlouváme se za zpoždění v distribuci tohoto čísla, které bylo zapříčiněno výpadkem HW serveru v hostingovém centru ….

A. Rodina speciálních blokových šifer DN a hašovacích funkcí nové generace HDN typu SNMAC
Část II. - Dodatky

RNDr. Vlastimil Klíma, nezávislý konzultant,
v.klima@volny.cz, http://cryptography.hyperlink.cz

Pokračování článku z e-zinu Crypto-World 3/2007.
Dodatek A: Teorie SP sítí a jejich odolnost proti DC a LC
Dodatek B: Definice volitelných prvků speciální blokové šifry DN(512,8192)
Dodatek C: Popis volitelných prvků HDN(512, 8192)
Dodatek D: Zdrojové kódy DN(512, 8192) a HDN(512, 8192)
Dodatek E: Testovací hodnoty DN(512, 8192) a HDN(512, 8192)

Dodatek A: Teorie SP sítí a jejich odolnost proti DC a LC

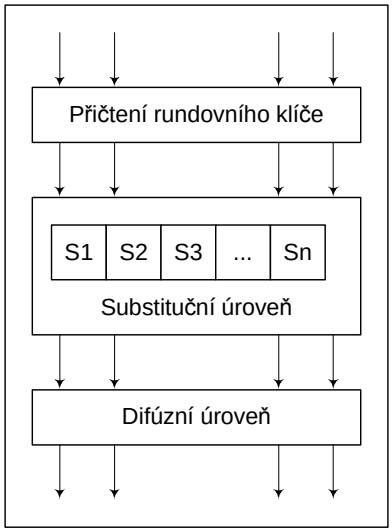
V této kapitole uvedeme nejprve výsledky teorie SP sítí, které budeme používat ke konstrukci funkcí Φ a Π. Poté uvedeme pravidla tvorby stavebních prvků (parametrů) ve funkci Φ a pravidla tvorby stavebních prvků (parametrů) ve funkci Π. Využijeme definicí a vět z [Ho00], odkud je převzata většina této kapitoly.

DC, LC a SPN

Nejznámější útoky na blokové šifry jsou diferenciální analýza DC ([BiSh91a], [BiSh91b], [Bi94]) a lineární kryptoanalýza LC ([Ma93], [Ma94]).

V diferenciální kryptoanalýze blokové šifry o několika rundách se používají diferenciální charakteristiky jednotlivých rund. Jsou to pravděpodobnosti, že nějaké konkrétní diference na vstupu dané rundy budou převedeny na nějaké konkrétní diference na výstupu této rundy.

Jako hodnota odolnosti blokové šifry proti DC byla brána maximální hodnota součinu diferenciálních charakteristik všech rund. Ukázalo se však, že nemusí být nezbytné fixovat hodnoty vstupních a výstupních diferencí ve vnitřních rundách blokové šifry a že lepším ukazatelem odolnosti je tzv. diferenciál [LaMa91]. Je to pravděpodobnost, že nějaká diference na vstupu (celé) blokové šifry se projeví jako určitá diference na výstupu (celé) blokové šifry, nezávisle na tom, jaké jsou vnitřní diference v jednotlivých rundách.



Obr.A.1: Jedna runda SPN sítě

Podobně se u odolnosti proti LC přešlo od pojmu lineární charakteristiky k pojmu lineární obal [Ny94]. Samozřejmě je mnohem obtížnější vypočítat hodnotu diferenciálu a lineárního obalu pro více rund blokové šifry.

V [NyKn92] K.Nyberg a L.R. Knudsen ukázali, že pravděpodobnost diferenciálu r-rundovního schématu je omezena číslem $2p^2$, jestliže maximální pravděpodobnost diferenciálu rundovní funkce je p a $r \geq 4$. Pokud je rundovní funkce bijektivní, je to pouze p^2. V substitučně permutačních sítích provádí difúzní úroveň lavinovitý efekt ve smyslu diferencí i lineárních aproximací, proto byl zaveden pojem

větvícího čísla [Da95]. Tento pojem je velmi důležitý, neboťmohou existovat šifry s S-boxy odolnými proti LC a DC, ale fatálně slabé, pokud mají malou hodnotu větvícího čísla. V [Ho00] se dokazuje odolnost SPN proti DC a LC, pokud má maximální hodnotu větvícího čísla.

V sítích Φ a Π budeme používat vždy maximální difúzní úroveň, tj. maximální hodnotu větvícího čísla. Naše důkazy odolnosti Φ a Π proti DC a LC budou založeny na dvou hlavních větách z [Ho00]. Předtím zavedeme označení.

Označení

V tomto příspěvku uvažujeme SPN s mn-bitovou rundovní funkcí, která používá n S-boxů $(S_1, ..., S_n)$. Každý S-box je bijekcí na množině $\{0, 1\}^m$, S_i: $\{0, 1\}^m \rightarrow \{0, 1\}^m$, i = 1, ..., n.

Definice 1. Lineární a diferenciální pravděpodobnost S-boxu

Diferenciální a lineární pravděpodobnost (bijektivního) S-boxu S: $\{0, 1\}^m \rightarrow \{0, 1\}^m$ definujeme pro libovolná $\Delta x, \Delta y, \Gamma x, \Gamma y \in \{0, 1\}^m$ jako

$DP^S(\Delta x \rightarrow \Delta y) = \#\{x \in \{0, 1\}^m \mid S(x) \oplus S(x \oplus \Delta x) = \Delta y \} / 2^m$,

$LP^S(\Gamma x \rightarrow \Gamma y) = [\#\{x \in \{0, 1\}^m \mid \Gamma x \bullet x = \Gamma y \bullet S(x) \}/2^{m-1} - 1]^2$, kde

$\Gamma x \bullet x$ je parita $\Gamma x \oplus x$.

Definice 2. Maximální diferenciální a lineární pravděpodobnost S-boxu

Maximální diferenciální a lineární pravděpodobnost (bijektivního) S-boxu S: $\{0, 1\}^m \rightarrow \{0, 1\}^m$ definujeme jako

$\mathbf{DP^S}$ = max $DP^S(\Delta x \rightarrow \Delta y)$, kde maximum se bere přes všechna $\Delta x \neq 0$, $\Delta x \in \{0, 1\}^m$, $\Delta y \in \{0, 1\}^m$

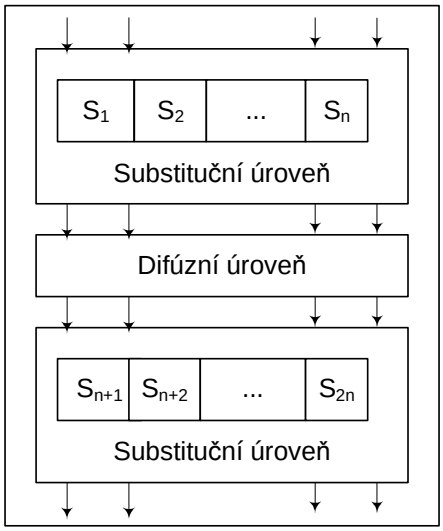
$\mathbf{LP^S}$ = max $LP^S(\Gamma x \rightarrow \Gamma y)$, kde maximum se bere přes všechna $\Gamma x, \Gamma y \neq 0$, $\Gamma x \in \{0, 1\}^m$, $\Gamma y \in \{0, 1\}^m$.

S-box se nazývá silný, pokud jsou tato čísla malá. SPN se nazývá silnou, pokud jsou tato čísla malá pro všechny S-boxy. Pro SPN označme

p = max DP^S,

q = max LP^S,

kde maximum se bere přes všechny S-boxy S, použité v SPN.



Obr.A.2: Funkce SDS

Funkce SDS. SDS je funkce se třemi úrovněmi: substitucí (S), difúzní úrovní (D) a substitucí (S), viz obrázek. Označme vstupní a výstupní diferenci SDS jako $\Delta x \in \{0, 1\}^{nm}$, $\Delta x \ \Delta x \neq 0, \in \{0, 1\}^{nm}$, $\Delta y = y \oplus y^* = D(x) \oplus D(x^*)$, a vstupní a výstupní masku SDS jako $\Gamma x \in \{0, 1\}^{nm}$, $\Gamma y \in \{0, 1\}^{nm}$, $\Gamma y \neq 0$ (mezi Γx a Γy existuje lineární vztah, detaily viz [RiDa97]).

Minimální počet diferenciálně a lineárně aktivních S-boxů. Minimální počet diferenciálně a lineárně aktivních S-boxů funkce SDS definujeme následovně:
$n_d(D) = \min (Hw(\Delta x) + Hw(\Delta y))$, kde minimum se bere přes všechna $\Delta x \neq 0$,
$n_l(D) = \min (Hw(\Gamma x) + Hw(\Gamma y))$, kde minimum se bere přes všechna $\Gamma y \neq 0$.

Maximální difúzní úroveň. Difúzní úroveň nazýváme maximální, jestliže minimální počet diferenciálně (nebo ekvivalentně lineárně) aktivních boxů je roven n + 1. Je známo, že maximální difúzní úroveň lze konstruovat z MDS (maximum distance separable) kódu RS typu (2n, n, n + 1) [Ho00]. Je-li generátor tohoto kódu matice v echelonové formě $[I_{nxn} \ B_{nxn}]$, pak $D: GF(2^m)^n \rightarrow GF(2^m)^n : x \rightarrow Bx$ je maximální difúzní úroveň [RiDa97].

Hlavní věty

V příspěvku předpokládáme, že rundovní klíče, které jsou xorovány na data v každé rundě, jsou nezávislé a stejnoměrně náhodné. Za tohoto předpokladu nemá přičtení klíče v rundovní funkci žádný vliv na počet aktivních S-boxů. Věta 1 dává horní odhad pro diferenciál funkce SDS jako celku, jestliže difúzní úroveň je maximální.

Věta 1. Horní odhad pro diferenciál funkce SDS [Ho00]**.** Předpokládejme, že rundovní klíče, které jsou xorovány na vstupní data v každé rundě, jsou nezávislé a stejnoměrně náhodné. Jestliže difúzní úroveň D je maximální (tj. $n_d = n + 1$), pak pravděpodobnost každého diferenciálu, funkce SDS je omezena hodnotou p^n.

Důsledek. Věta 1 říká, že $DP^{SDS}(\Delta x \rightarrow \Delta y) \leq p^n$ pro každé $\Delta x \in \{0, 1\}^{nm}$, $\Delta x \neq 0$, $\Delta y \in \{0, 1\}^{nm}$. Odtud vyplývá, že
$\mathbf{DP^{SDS}} = \max DP^{SDS}(\Delta x \rightarrow \Delta y) \leq p^n$,
kde maximum se bere přes všechna $\Delta x \neq 0$, $\Delta x \in \{0, 1\}^{nm}$, $\Delta y \in \{0, 1\}^{nm}$.

Podobný odhad platí pro lineární obal funkce SDS.

Věta 2. Horní odhad pro lineární obal funkce SDS [Ho00]**.** Jestliže difúzní úroveň D je maximální (tj. $n_l(D) = n + 1$ nebo ekvivalentně $n_d(D) = n + 1$), pak pravděpodobnost každého lineárního obalu funkce SDS je omezena hodnotou q^n.

Důsledek 1. Věta 2 říká, že $LP^{SDS}(\Gamma x \rightarrow \Gamma y) \leq q^n$ pro každé $\Gamma x \in \{0, 1\}^{nm}$, $\Gamma y \neq 0$, $\Gamma y \in \{0, 1\}^{nm}$. Odtud vyplývá, že
$\mathbf{LP^{SDS}} = \max LP^{SDS}(\Gamma x \rightarrow \Gamma y) \leq q^n$,
kde maximum se bere přes všechna $\Gamma x \in \{0, 1\}^{nm}$, $\Gamma y \neq 0$, $\Gamma y \in \{0, 1\}^{nm}$.

Dále budeme hovořit pouze o diferenciálech, podobná tvrzení platí vzhledem k podobnosti vět 1 a 2 i o lineárních obalech. Věty 1 a 2 jsou významné, neboť odhadují velikost diferenciálu a lineárního obalu. Tyto odhady bylo dosud obtížné obdržet u klasické blokové šifry. Tam se tyto odhady nahrazovaly součiny rundovních charakteristik.

Důsledek 2. Síť SDS můžeme vůči S-boxu chápat jako větší S-box, tzv. "XS"-box. Maximální diferenciál (lineární obal) boxu XS je pomocí Věty 1 (2) odhadnut pomocí

maximálních diferenciálů (lineárních obalů) malých boxů S, z nichž je sestaven jako SDS síť. Z XS-boxů lze sestavovat větší XXS-boxy atd. Tento princip využijeme ke konstrukci a důkazu vlastností sítí Φ a Π.

Dodatek B: Definice volitelných prvků speciální blokové šifry DN(512,8192)

V této kapitole uvedeme konkrétní volbu volitelných parametrů pro funkci DN(512, 8192) o počtu velkých rund $\rho = 1, ..., 10$. Volíme $r = 16$, $c = 64$.

Poměrně velká mohutnost klíče (8192 bitů) je umožněna tím, že funkce F provádí zpracování těchto dat (paralelně) po sloupcích. Při použití DN v hašovací funkci dostáváme funkci HDN(512, 8192), který má 512 bitový kód a zpracovává bloky zpráv o délce 7680 bitů (7680 = 8192 - 512). Popis volitelných prvků HDN(512, 8192) je uveden v následující kapitole.

Substituční boxy, které použijeme ve funkci DN, jsou substituční boxy, které pochází z algoritmu Whirlpool. Původní verze blokové šifry W ve Whirlpoolu, zaslaná do projektu NESSIE, obsahovala (pseudo)náhodně vygenerovaný S-box 8x8, který tudíž neměl žádné speciální algebraické vlastnosti, tento S-box byl pak zaměněn za S-box generovaný ze dvou malých S-boxů 4x4 z důvodu rychlejší HW realizace.
Zdroje:
(a) Poslední verze popisu - odpovídá vybranému algoritmu NESSIE a ISO normě ISO/IEC 10118-3 (změněný S-box a změněná matice MDS):
Paulo S.L.M. Barreto and Vincent Rijmen: The WHIRLPOOL Hashing Function, (Revised on May 24, 2003)
http://planeta.terra.com.br/informatica/paulobarreto/whirlpool.zip
(b) Předposlední verze popisu (změněný S-box) ze 7.3.2003
https://www.cosic.esat.kuleuven.be/nessie/updatedPhase2Specs/WHIRLPOOL/Whirlpool-tweak2.zip
(c) Originální verze popisu ze září 2000 (původní S-box)
https://www.cosic.esat.kuleuven.be/nessie/workshop/submissions/whirlpool.zip

Funkce F: originální S-box algoritmu Whirlpool

Originální S-box algoritmu Whirlpool byl generován (pseudo)náhodně do té doby, než splňoval tyto podmínky (https://www.cosic.esat.kuleuven.be/nessie/workshop/submissions/whirlpool.zip, September 3, 2000):
(a) $\delta \leq 8*2^{-8}$,
(b) $\lambda \leq 16 * 2^{-6}$,
(c) $\nu = 7$,
(d) žádné pevné body,
(e) v množině hodnot (x xor S(x)) pro všechna x se žádná hodnota neobjevuje více než dvakrát.
Zvolený S-box měl tyto parametry
(a) $\delta = 8*2^{-8} = 2^{-5}$,
(b) $\lambda = 16 * 2^{-6} = 2^{-2}$,
(c) $\nu = 7$,

(d) žádné pevné body,
(e) v množině hodnot (x xor S(x)) pro všechna x se žádná hodnota neobjevuje více než dvakrát. Nazýváme ho **originální S-box** algoritmu Whirlpool. Použijeme ho ve funkci F, protože je méně strukturovaný než druhý S-box z algoritmu Whirlpool.

```
unsigned char SubsF[256] = {
0x68, 0xd0, 0xeb, 0x2b, 0x48, 0x9d, 0x6a, 0xe4,
……
0xb8, 0x7b, 0x89, 0x30, 0xd3, 0x7f, 0x76, 0x82
};
```

Obr.B.1: Originální S-box algoritmu Whirlpool

Počet rund ρ

V definici F volíme z realizačních důvodů všechny S-boxy stejné, a to s parametry $p = DP^S = 2^{-5}$ a $q = LP^S = 2^{-2}$. Použijeme originální pseudonáhodný S-box algoritmu Whirlpool, který není generován algebraicky. Z tohoto důvodu má bohužel nižší odolnost proti lineární kryptoanalýze (q). Abychom tuto odolnost učinili dostatečně vysokou i s rezervou, jsme nyní nuceni volit počet rund ρ zbytečně vysoký. **Volíme ρ = 10 místo postačujících 6**. Jakmile bude k dispozici veřejně generovaný S-box s lepšími vlastnostmi, bude možné ho použít ve funkci DN s nižším počtem rund (doporučujeme ρ = 6).

Deset rund F tvoří pět po sobě zařazených SDS sítí, spojených maticemi MDS typu 16x16. Uvnitř SDS sítě je difúzní úroveň zajištěna také maticí MDS typu 16x16. Využijeme toho, že pomocí Věty 1 a 2 můžeme odhadnout DP^{SDS} a LP^{SDS} pro jednu SDS. Máme $p_{SDS} \leq 2^{-80}$ a $q_{SDS} \leq 2^{-32}$.

Poměrně nízký odhad $LP^{SDS} \leq 2^{-32}$ je způsoben nepříliš vhodnou lineární charakteristikou použitého boxu ($q = 2^{-2}$). S-box ve funkci F je však možné volit s lepší charakteristikou, například $q = 2^{-6}$ jako u AES nebo s očekávaným koeficientem $q = 2^{-4}$ pro náhodně generované S-boxy.

Pro S-box AES máme $q = 2^{-6}$ a dostali bychom zcela dostatečný odhad $LP^{SDS} \leq 2^{-96}$. Pro koeficient $q = 2^{-4}$ bychom obdrželi také dostatečně dobrý odhad $LP^{SDS} \leq 2^{-64}$. V obou těchto případech by z hlediska odolnosti F proti LC postačovaly tři SDS sítě za sebou, tj. 6 velkých rund (ρ = 6).

Odolnost funkce F proti diferenciální kryptoanalýze je pak zajištěna podobným způsobem a postačují také tři SDS sítě za sebou, tj. 6 velkých rund (ρ = 6).

Rundovní konstanty RConstF

Ukázali jsme, že různé rundovní konstanty způsobují afinní modifikaci každého S-boxu. Rundovní konstanty ve funkci F volíme z důvodu efektivní SW a HW realizace jako konstanty, které se dají průběžně tvořit: RConstF[i][j] = ((CONSTA * (i+1)) mod 2^{32} ⊕ ((CONSTB * (j+1)) mod 2^{32}), kde CONSTA = 0xfedc1357, CONSTB = 0x84736251. Tyto konstanty jsou pouze čtyřbajtové (prvních 12 bajtů je nulových) a navzájem různé.

Těleso GF(2^8)

Těleso GF(2^8) je uvažováno s ireducibilním polynomem $q(x) = x^8 + x^4 + x^3 + x^1 + x^0$. Násobení v tomto tělese je v programovém kódu realizováno pomocí tabulek Logtable a Alogtable, které jsou stejné jako v algoritmu AES.

Matice MDS 16 x 16

Z důvodu snadné SW a HW realizace volíme ve funkci F pouze jednu matici MDS 16 x 16. Matice MDS typu 16x16 byla zvolena na základě [PlDi05] a [Ro06] následujícím postupem.

Budeme pracovat v tělese GF(2^8) s ireducibilním polynomem $q(x) = x^8 + x^4 + x^3 + x^1 + x^0$.

Základem je matice G Vandermondova typu 16x32, $G = (g_{i,j})_{i = 0...15,\ j = 0..31}$, kde volíme 32 různých prvků $a_0, a_1, a_2, ..., a_{31}$, přičemž $a_0 = 1$. Volíme $a_1 = 12$, $a_2 = 13$, ..., $a_{31} = 42$, tj. $a_j = (j + 11)$ pro všechna j = 1, ..., 31. Definujeme $g_{i,j} = a_j^i$, kde i = 0, ...,15, j = 0, ..., 31. Máme

$$G = \begin{matrix} 1 & 1 & 1 & ..... & 1 & 1 \\ 1 & 12 & 13 & & 41 & 42 \\ 1 & 12^2 & 13^2 & & 41^2 & 42^2 \\ 1 & ... & & (a_j)^i & & ... \\ 1 & ... & & & & ... \\ 1 & 12^{15} & 13^{15} & ... & 41^{15} & 42^{15} \end{matrix}$$

Označíme levou polovinu matice G jako G1 a pravou jako G2, tj. G = (G1, G2). Matici G = (G1, G2) upravujeme elementárními úpravami na tvar G = (I , F), kde I je identická matice typu 16x16 a F je matice typu 16x16. F je výsledná matice MDS typu 16x16.

Elementární úpravy jsou prováděny na řádcích matice G a jedná se o tyto úpravy:

- výměna řádků,
- násobení nebo dělení řádku nenulovým prvkem tělesa,
- přičtení nenulového násobku nějakého řádku k jinému řádku.

Jako výslednou matici MDS použijeme transponovanou F (hexadecimálně):

```
4A 7B BA CF 84 8D B7 C6 72 9F 24 B2 7A 40 B1 CD,
…...
34 F0 19 66 6A 6D 73 08 22 16 11 9B 33 F4 5D E2.
```

Závěrečná permutace

U DN(512, 8192) je závěrečná permutace tvořena pouze cyklickým posunem v rámci řádků pole RK:

```
v řádku  0 jde o cyklický posun doprava o  0 pozic
v řádku  1 jde o cyklický posun doprava o  0 pozic
v řádku  2 jde o cyklický posun doprava o 16 pozic
v řádku  3 jde o cyklický posun doprava o 32 pozic
v řádku  4 jde o cyklický posun doprava o 32 pozic
v řádku  5 jde o cyklický posun doprava o 32 pozic
v řádku  6 jde o cyklický posun doprava o 16 pozic
v řádku  7 jde o cyklický posun doprava o  0 pozic

v řádku  8 jde o cyklický posun doprava o  0 pozic
v řádku  9 jde o cyklický posun doprava o  0 pozic
v řádku 10 jde o cyklický posun doprava o 16 pozic
v řádku 11 jde o cyklický posun doprava o 32 pozic
v řádku 12 jde o cyklický posun doprava o 32 pozic
v řádku 13 jde o cyklický posun doprava o 32 pozic
v řádku 14 jde o cyklický posun doprava o 16 pozic
v řádku 15 jde o cyklický posun doprava o  0 pozic
```

a toto se dále se periodicky opakuje až do řádku číslo 159.

Funkce B: Generovaný S-box algoritmu Whirlpool

Generovaný S-box aktualizovaného algoritmu Whirlpool je S-box generovaný ze dvou malých S-boxů 4x4 z důvodu rychlejší HW realizace. Je popsán ve zprávě pro NESSIE

7.3.2003 a pozdějších (24.5.2003, kde je též upravena matice MDS), a je součástí výsledného vybraného algoritmu Whirlpool v projektu NESSIE a zároveň je převzat do normy ISO. Tento S-box má charakteristiky $p = 2^{-5}$ a $q = 14*2^{-6}$ a použijeme ho ve funkci B.

```
unsigned char SubsB[256] = {
0x18,0x23,0xc6,0xE8,0x87,0xB8,0x01,0x4F,
......
0xcc,0x42,0x98,0xA4,0x28,0x5c,0xF8,0x86
};
```

Obr.B.2: Generovaný S-box aktualizovaného algoritmu Whirlpool

Permutace SMLPerm

Rodina funkcí DN používá pro každou z transformací T1 obecně jinou dílčí permutaci SMLPerm, která je permutací na množině čísel 0, ... c -1. DN(512, 8192) používá pouze čtyři různé permutace na množině čísel 0, ..., 63 (dekadicky):

```
23,14,49,32,41, 8,50,18,46,16,15,57,55,27,43, 2,
60, 7,22,42,38,26,53,12, 9,62,37,28, 0,36,51,20,
17,39, 4,56,59, 3,47,31, 6,25,45,48,24,58,11,33,
29,13,40,61, 1,19,63,34,52,35, 5,30,44,54,10,21,

17,42,57, 6,62, 8,24,12, 3,21,55,51,44,34,39,31,
36, 2,25,58, 7,47,53,14,49, 9,16,30,33,60,22,40,
41,37,50,15, 1,45,19,63,35,10,59,52,27,20, 4,28,
13,56,23,46,48,32,26,18,61,43,29,54, 5,11, 0,38,

10,15, 4, 1, 5, 0,14,11, 2, 8, 7,13, 6, 9, 3,12,
26,31,20,17,21,16,30,27,18,24,23,29,22,25,19,28,
42,47,36,33,37,32,46,43,34,40,39,45,38,41,35,44,
58,63,52,49,53,48,62,59,50,56,55,61,54,57,51,60,

10, 5,12, 2, 7, 9, 0,15, 1,11, 4,14, 8, 3,13, 6,
26,21,28,18,23,25,16,31,17,27,20,30,24,19,29,22,
42,37,44,34,39,41,32,47,33,43,36,46,40,35,45,38,
58,53,60,50,55,57,48,63,49,59,52,62,56,51,61,54.
```

Tento blok čtyř permutací se opakuje ještě třikrát v rámci každé velké rundy a každá velká runda používá tutéž sadu SMLPerm. Jejich hodnoty jsou odvozeny tak, aby příslušné matice MDS (XMDS, XXMDS, XXXMDS) realizovaly maximální difúzní úroveň a jinak nepravidelně (ručně).

Matice MDS 4x4

Pro DN byla z důvodu snadné realizace zvolena jedna matice MDS typu 4x4, a to matice z algoritmu AES.

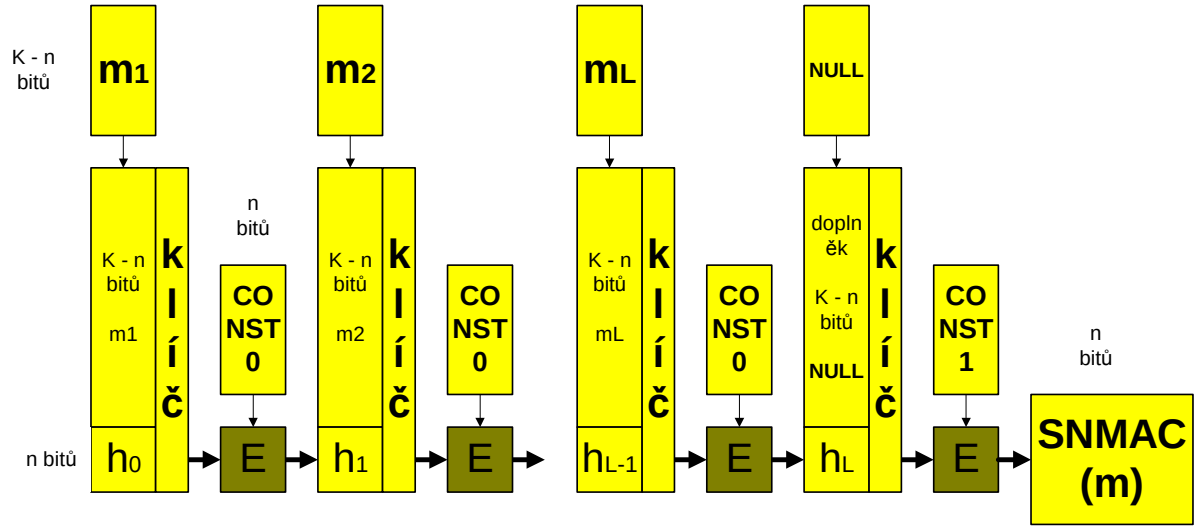
$$M = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Rundovní konstanty RConstB

Rundovní konstanty ve funkci B volíme z důvodu efektivní SW a HW realizace jako konstanty, které se dají průběžně tvořit, přičemž jejich prvních 60 bajtů je nulových. Poslední 4 bajty jsou jako 32bitová čísla tvořena vzorcem RConstB[i][j] = (CONSTC*(16*i + j + 1)) mod 2^{32}, kde CONSTC = 0x24687531. Nejnižší bajt 32bitového čísla je 61. bajtem konstanty, nejvyšší 64. bajtem. Hodnoty volitelných prvků jsou také vidět také v přiloženém programu.

Dodatek C: Popis volitelných prvků HDN(512, 8192)

Při použití DN(512, 8192) v hašovací funkci podle konstrukce SNMAC [Kl06] dostáváme funkci HDN(512, 8192), která má 512 bitový kód a zpracovává bloky zpráv o délce 7680 bitů (7680 = 8192 - 512).



Obr. C.1: Definice HDN(512, 8192) jako SNMAC, založená na speciální blokové šifře DN(512, 8192)

Definice. Hašovací funkce HDN(512, 8192) je hašovací funkce typu SNMAC, založená na speciální blokové šifře DN(512, 8192). Má n bitový hašovac kód (n = 512), K bitový klíč (K = 8192) a zpracovává bloky dat o délce K - n bitů (K - n = 7680). Používá kompresní funkci f a závěrečnou úpravu g, kde

f: $\{0, 1\}^K \rightarrow \{0, 1\}^n : X \rightarrow E_X(Const_0)$,

g: $\{0, 1\}^n \rightarrow \{0, 1\}^n : X \rightarrow E_{X \,||\, NULL}(Const_1)$,

a E je DN(512, 8192).

$Const_0$ a $Const_1$ jsou různé konstanty a NULL je řetězec K - n nulových bitů.

Hašování zprávy m má tři kroky.

Krok 1. Doplnění

Zprávu m, kterou hašujeme, nejprve doplníme bitem 1, nejmenším (i nulovým) počtem bitů 0 a 128bitovým číslem Č (které vyjadřuje délku m v bitech) tak, aby její délka byla L násobkem čísla K - n, kde L je přirozené číslo. Orientace bitů a bajtů je stejná jako u standardu SHA-512, tj. jako poslední bajt posledního bloku m_L se ukládá nejnižší bajt čísla Č. Tuto doplněnou zprávu rozdělíme na L bloků o délce K - n bitů, $m = m_1 \,||\, \ldots \,||\, m_{L-1} \,||\, m_L$. Doplnění je stejné jako u hašovací funkce SHA-512.

Krok 2. Iterace
$h_i = f(h_{i-1} \| m_i)$, i = 1, ..., L,
kde h_0 je konstantní inicializační hodnota (IV).
Krok 3. Závěrečná úprava
SNMAC(m) = $g(h_L)$.

$Const_0$, $Const_1$ a h_0 (IV)
U rodiny hašovacích funkcí bychom mohli konstanty $Const_0$, $Const_1$ a h_0 (IV) volit jakkoliv náhodně a odlišné. Z důvodu snadné realizace volíme konstanty tak, aby se daly vytvářet za chodu schématu. Konkrétní hodnoty jsou k dispozici v [Kl07].

Dodatek D: Zdrojové kódy DN(512, 8192) a HDN(512, 8192)

Zde uvádíme výběr funkcí, všechny jsou k dispozici na [Kl07].

```
/*=========================================================*/
/* Funkce ExpandRK vytvari pole rundovnich klicu RK[1..rho][0..r-1][0..c-1]
      ze vstupniho pole RK[0][0..r-1][0..c-1].
      Rundovni konstanty jsou RConstF;
*/
void ExpandRK(unsigned char RK[MAXRHO][r][c],int rho,int print)
{
      unsigned char i,j,x,m, temp[c];
      unsigned long templong;
      int k;

      //tvorba RK
 for(i=1;i<rho;i++)
 {
  for(j=0;j<c;j++)
  {
      templong = 0; for(m = 0;m < r; m++) templong ^= T[0][m][RK[i-1][m][j]];
      RK[i][4*0+0][j] = (unsigned char)( templong       ) & 0xFF;
      RK[i][4*0+1][j] = (unsigned char)( templong >>   8) & 0xFF;
      RK[i][4*0+2][j] = (unsigned char)( templong >>  16) & 0xFF;
      RK[i][4*0+3][j] = (unsigned char)( templong >>  24) & 0xFF;

      templong = 0; for(m = 0;m < r; m++) templong ^= T[1][m][RK[i-1][m][j]];
      RK[i][4*1+0][j] = (unsigned char)( templong       ) & 0xFF;
      RK[i][4*1+1][j] = (unsigned char)( templong >>   8) & 0xFF;
      RK[i][4*1+2][j] = (unsigned char)( templong >>  16) & 0xFF;
      RK[i][4*1+3][j] = (unsigned char)( templong >>  24) & 0xFF;

      templong = 0; for(m = 0;m < r; m++) templong ^= T[2][m][RK[i-1][m][j]];
      RK[i][4*2+0][j] = (unsigned char)( templong       ) & 0xFF;
      RK[i][4*2+1][j] = (unsigned char)( templong >>   8) & 0xFF;
      RK[i][4*2+2][j] = (unsigned char)( templong >>  16) & 0xFF;
      RK[i][4*2+3][j] = (unsigned char)( templong >>  24) & 0xFF;

      templong = RConstF[i-1][j];
      for(m = 0;m < r; m++) templong ^= T[3][m][RK[i-1][m][j]];
      RK[i][4*3+0][j] = (unsigned char)( templong       ) & 0xFF;
      RK[i][4*3+1][j] = (unsigned char)( templong >>   8) & 0xFF;
      RK[i][4*3+2][j] = (unsigned char)( templong >>  16) & 0xFF;
      RK[i][4*3+3][j] = (unsigned char)( templong >>  24) & 0xFF;
  }
 }

  //Final permutation
  for(i=0;i<rho;i++)
```

```
  {
       x=2;
       for(k=48;  k<c; k++) temp[k-48]  = RK[i][x][k];
       for(k=c-1;k>=16;k--) RK[i][x][k] = RK[i][x][k-16];
       for(k=15;  k>= 0;k--) RK[i][x][k] = temp[k];
       x=3;
       for(k=0;k<32;k++)
       {temp[k] = RK[i][x][k];RK[i][x][k]= RK[i][x][k+32];RK[i][x][k+32]= temp[k];}
       x=4;
       for(k=0;k<32;k++)
       {temp[k] = RK[i][x][k];RK[i][x][k]= RK[i][x][k+32];RK[i][x][k+32]= temp[k];}
       x=5;
       for(k=0;k<32;k++)
       {temp[k] = RK[i][x][k];RK[i][x][k]= RK[i][x][k+32];RK[i][x][k+32]= temp[k];}
       x=6;
       for(k=48;  k<c; k++) temp[k-48]  = RK[i][x][k];
       for(k=c-1;k>=16;k--) RK[i][x][k] = RK[i][x][k-16];
       for(k=15;  k>= 0;k--) RK[i][x][k] = temp[k];

       x=10;
       for(k=48;  k<c; k++) temp[k-48]  = RK[i][x][k];
       for(k=c-1;k>=16;k--) RK[i][x][k] = RK[i][x][k-16];
       for(k=15;  k>= 0;k--) RK[i][x][k] = temp[k];
       x=11;
       for(k=0;k<32;k++)
       {temp[k] = RK[i][x][k];RK[i][x][k]= RK[i][x][k+32];RK[i][x][k+32]= temp[k];}
       x=12;
       for(k=0;k<32;k++)
       {temp[k] = RK[i][x][k];RK[i][x][k]= RK[i][x][k+32];RK[i][x][k+32]= temp[k];}
       x=13;
       for(k=0;k<32;k++)
       {temp[k] = RK[i][x][k];RK[i][x][k]= RK[i][x][k+32];RK[i][x][k+32]= temp[k];}
       x=14;
       for(k=48;  k<c; k++) temp[k-48]  = RK[i][x][k];
       for(k=c-1;k>=16;k--) RK[i][x][k] = RK[i][x][k-16];
       for(k=15;  k>= 0;k--) RK[i][x][k] = temp[k];
  }

}
/*=============================================================*/
/* Funkce DN.
Funkce DN se sklada z rho velkych rund, cislovanych 0..rho-1.
V kazde velke runde se za sebou (iterativne) provede r (=16) malych rund
(transformaci T1),
pricemz vysledek predchozi transformace T1 je vstupem nasledujici.
V i-te (i = 0 ... rho-1) velke runde je potreba r rundovnich klicu o c bajtech,
jsou to RK[i][0..r-1][0..c-1].

RK[0][0..r-1][0..c-1] je vstupem funkce DN.
Zbyvajici RK:
RK[   1][0..r-1][0..c-1]
RK[   2][0..r-1][0..c-1]
....
RK[rho-1][0..r-1][0..c-1]
se vytvori expanzni funkci ExpandRK z RK[   0][0..r-1][0..c-1].
Vstupem prvni male rundy je c bajtu pole indata.
Vystupem funkce DN je c bajtu vystupu z posledni male rundy posledni velke rundy,
ktere jsou ulozeny do pole outdata.
 */
void DN(unsigned char RK[MAXRHO][r][c],
                    int rho,
                    unsigned char indata[c],
                    unsigned char outdata[c],
                    int print)
{
unsigned char tempdata[64],tempdata2[64];

int i,j;
```

```
unsigned char k;
unsigned long temp;

ExpandRK(RK,rho,print);

Copy64(indata,tempdata);
for(i=0;i<rho;i++)
{
  for(j=0;j<r;j+=2)
  {
    for(k=0;k<c;k+=4)
    {
       temp  = N[0][tempdata[SMLPerm[j][k+0]]];
       temp ^= N[1][tempdata[SMLPerm[j][k+1]]];
       temp ^= N[2][tempdata[SMLPerm[j][k+2]]];
       temp ^= N[3][tempdata[SMLPerm[j][k+3]]];
       if (k==60) temp = temp ^ RConstB[i][j];
       tempdata2[k+0] = RK[i][j][k+0] ^ (unsigned char)( temp       ) & 0xFF;
       tempdata2[k+1] = RK[i][j][k+1] ^ (unsigned char)( temp >>   8) & 0xFF;
       tempdata2[k+2] = RK[i][j][k+2] ^ (unsigned char)( temp >>  16) & 0xFF;
       tempdata2[k+3] = RK[i][j][k+3] ^ (unsigned char)( temp >>  24) & 0xFF;
    }

    for(k=0;k<c;k+=4)
    {
       temp  = N[0][tempdata2[SMLPerm[j+1][k+0]]];
       temp ^= N[1][tempdata2[SMLPerm[j+1][k+1]]];
       temp ^= N[2][tempdata2[SMLPerm[j+1][k+2]]];
       temp ^= N[3][tempdata2[SMLPerm[j+1][k+3]]];
       if (k==60) temp = temp ^ RConstB[i][j+1];
       tempdata[k+0] = RK[i][j+1][k+0] ^ (unsigned char)( temp       ) & 0xFF;
       tempdata[k+1] = RK[i][j+1][k+1] ^ (unsigned char)( temp >>   8) & 0xFF;
       tempdata[k+2] = RK[i][j+1][k+2] ^ (unsigned char)( temp >>  16) & 0xFF;
       tempdata[k+3] = RK[i][j+1][k+3] ^ (unsigned char)( temp >>  24) & 0xFF;
    }
  }
}
Copy64(tempdata,outdata);
}
/*============================================================*/
// hasovani jednoho plneho bloku dat
static void Process_One_Block_HDN( HDN_CTX* ctx )
{
      /*
      Vstupem teto funkce je
      a) naplneni ctx->rk[0][0] inicializacni hodnotou
            nebo prubeznou hasovaci hodnotou (64 bajtu),
      b) naplneni ctx->rk[0][1..r-1] 960 bajty, ktere maji byt zpracovany
hasovanim.
      Cele pole RK je pote zpracovano funkci DN, jejiz 64 bajtovy vystup je jakozto
      prubezna hasovaci hodnota zkopirovan do ctx->rk[0][0], cimz prepise puvodni
hodnotu.
      */
      unsigned char outdata[c];
      DN(ctx->rk,ctx->rho,CONST0,outdata,0);
      Copy64(outdata,ctx->rk[0][0]);
}
/*============================================================*/
```

Dodatek E: Testovací hodnoty DN(512, 8192) a HDN(512, 8192)

Testovací příklady jsou definovány v [Kl07].

Testovací hodnoty DN

DN_abc_CONST0

Otevřený text: CONST0
Klíč:
rk[0][0] = IV,
rk[0][1][0] = 0x61; // 'a';
rk[0][1][1] = 0x62; // 'b';
rk[0][1][2] = 0x63; // 'c';
rk[0][1][3] = 0x80;
všechny ostatní bajty rk[0][][] jsou 0x00 až na poslední bajt (doplnění délky řetězce "abc", tj. 24 bitů = 0x18,): rk[0][15][63] = 0x18;
Šifrový text: viz pole DN_abc_CONST0[MAXRHO][c], kde je uložen výsledek (64 bajtů šifrového textu) pro počet rund 1 až 10.

DN_abc_CONST1

Otevřený text: CONST1
Klíč:
rk[0][0] = DN_abc_CONST0,
všechny ostatní bajty rk[0][][] jsou 0x00

Šifrový text: viz pole DN_abc_CONST1[MAXRHO][c], kde je uložen výsledek (64 bajtů šifrového textu) pro počet rund 1 až 10.

Megatest DN

Tento megatest naplní na počátku otevřený text i rundovní klíč RK[0][0..15][0..63] nulami.
Následuje blok operací pro i = 0:

- S tímto nastavením provedeme operaci zašifrování. Výsledkem (64 bajtů) přepíšeme otevřený text SBŠ.
- S tímto nastavením provedeme operaci zašifrování. Výsledkem (64 bajtů) přepíšeme rundovní klíč RK[0][0].
- S tímto nastavením provedeme operaci zašifrování. Výsledkem (64 bajtů) přepíšeme rundovní klíč RK[0][1].
- atd až
- S tímto nastavením provedeme operaci zašifrování. Výsledkem (64 bajtů) přepíšeme rundovní klíč RK na místě RK[0][15].

Nyní zopakujeme uvedený blok operací pro i =1, ..., 99, tj. provedeme celkem 100*17 = 1700 operací zašifrování. Výsledek poslední operace zašifrování je testovací hodnotou. Testovací hodnoty jsou uloženy v poli DN_mega[MAXRHO][c] , kde je uložen výsledek (64 bajtů šifrového textu) pro počet rund 1 až 10.

Testovací hodnoty HDN

Testovací hodnota HDN("abc")

Testovací hodnoty pro počet rund 1 až 10 jsou uloženy v poli HDN_abc. Musí být totožné s polem DN_abc_CONST1. Navíc je v programu kontrolováno, zda se při kompresi prvního bloku obdrží jako mezivýsledek pole DN_abc_CONST0.

Megatest HDN

V tomto testu se provede výpočet hodnoty pro stonásobné řetězené volání HDN. Funkce vypočte 64 bajtů výsledku HDN("abc") a uloží ho za řetězec "abc". Vznikne 3 + 64 bajtový vstup, který je zhašován. Výsledek se připojí za původní vstup 3 + 64 bajtů a zhašuje se tak 3 + 64 + 64 bajtů. To se opakuje celkem stokrát. Výstupem je tedy
HDN("abc" || HDN("abc") || HDN("abc" || HDN("abc")) || .....))))))...),
přičemž HDN se volá celkem stokrát, viz též program. Testovací hodnota je uvedena v poli HDN_mega pro počet rund 1 až 10.

Testovací program pro DN a HDN

Testovací modul main_test_definice_DN_a_HDN.c provede výpočet všech testovacích hodnot, uvedených výše pro funkce DN a HDN a na závěr test rychlosti, a to pro všechny hodnoty počtu rund 1 až 10.

Poznámka. Zdrojové kódy různých implementací DN a HDN jsou k dispozici na stránce http://cryptography.hyperlink.cz

B. Zachycené a šifrové telegramy dokazují, že demokraté se během voleb snažili podplácet!

Pavel Vondruška, Telefónica O2 Czech Republic a.s., (pavel.vondruska@crypto-world.info)

Titulky z novin:
Historicky nejtěsnější vítězství ve volbách! Rozdíl jednoho křesla! Nejtěsnější a nediskutovanější vítězství ve volbách! Jmenována komise, která má prověřit koupení hlasů voličů!

Že si na tyto novinové nadpisy nepamatujete a přitom jste naše volby a jejich výsledek a následné „koaliční tanečky“ sledovali ? Inu, to je v pořádku. Nejedná se o nadpisy z našci novin a už vůbec ne z loňského roku. Nadpisy souvisí z volbami, které v USA proběhly v předminulém století a to roku 1876.

Nejprve stručně k průběhu těchto zvláštních voleb:

Když byly při prezidentských volbách sečteny všechny hlasy při všeobecném hlasování , tj. při volbě elektorů, kandidát na prezidenta za demokratickou stranu vedl o 250 000 hlasů před svým republikánským soupeřem. Převaha ve volebním kolegiu tvořeného elektory, závisela na tom, která ze dvou protichůdných úředních zpráv o průběhu všeobecného hlasování na Floridě, Lousianě, Jižní Karolině a Oregonu bude uznána jako platná a správná. Kongres ustanovil zvláštní volební komisi, která přímým hlasováním 8:7 přiřkla všech 22 hlasů z uvedených států republikánskému kandidátovi. Tím získal tento kandidát většinu ve volebním kolegiu a 185:184 hlasy elektorů i prezidentské křeslo! Nový americký prezident tak získal většinu nejtěsnějším a nejdiskutovanějším způsobem v celých dějinách amerických voleb!!!
(Zájemci mohou najít detailní volební výsledky např. zde
http://www.uselectionatlas.org/USPRESIDENT/GENERAL/pe1876.html).

Těsné vítězství tak tehdy získal republikán Rutherford B.Hayes, poraženým byl demokrat Samuel Jones Tilden. To těsné vítězství se samozřejmě stalo diskutovaným tématem, zvláště po té, co poražení demokraté obvinili republikány z toho, že si koupili hlasy některých voličů. Zvláštní komise, kterou jmenoval Kongres však žádné důkazy nenašla.

Čas plynul a rozbouřená atmosféra volebních dnů se již pomalu uklidnila a na celou záležitost již pomalu veřejnost zapomněla. A pak se to stalo - v pondělí 7.října 1878 New York Tribune publikoval jednoho z velkých „sólokaprů“ americké žurnalistiky. Pod dvoupalcovým titulkem **„Zachycené šifrové telegramy“** úvodník tohoto listu publikoval otevřený text jednoho ze zachycených šifrových telegramů, které se týkaly voleb před dvěma lety. V následujících dnech noviny pokračovaly ve zveřejňování rozšifrovaných dalších a dalších telegramů. Jak již to bývá, ukázalo se, že zloděj křičel – chyťte zloděje. Z rozluštěných textů totiž vyplývalo, že to naopak byly demokraté, kteří se ve volbách roku 1876 snažili podplatit republikány.

V New York Tribune bylo postupně odhalen obsah na 400 zašifrovaných telegramů, které dokazovaly, že demokraté se snažili kupovat hlasy republikánů a i jinak ovlivnit výsledek prezidentských voleb ve svůj prospěch. Úspěch byl opravdu obrovský. Dokonce i list Sun (tradiční opora demokratů) smutně připustil, že „p.Tilden už nebude nikdy kandidátem na

úřad prezidenta za žádnou stranu“. Dokonce i autor životopisu Tildena uznal, že „*v důsledku zašifrovaných telegramů získali republikáni takovou výhodu, která jim vyhrála voly v roce 1880. Mnoho lidí bylo přesvědčeno, že milionář kandidující na prezidentský úřad dovolil sáhnout předákům své strany do svého měšce …*“.
Pro úplnost dodejme, že v následujících volbách roku 1880 republikáni v užších volbách přesvědčivě zvítězili (214:155 hlasům).

Vraťme se k šifrovým telegramům. Kde vzal list New York Tribune zašifrované telegramy a hlavně, jak získal odpovídající otevřené texty?

Telegramy nebyly zašifrovány pouze jedním systémem, ale celou řadu různých šifrových systémů. Byly použity nejrůznější klasické „ruční“ šifry, zejména se jednalo o různě složité substituce, transpozice a slovníkové či kódové zprávy. Kdo byl tím, kdo rozluštil tyto telegramy a umožnil americkým občanům poznat trpkou pravdu o volbách roku 1876?

Vše začalo podle hesla : „Kdo seje vítr, sklízí bouři“. Poradce neúspěšného kandidáta na prezidenta S.Tildena Manton Marble publikoval v demokratickém listu Sun článek o nepoctivých praktikách republikánů.

Republikánsky zaměřený list New York Tribune reagoval tím, že článek komentoval a publikoval i některé zašifrované telegramy demokratů.

Demokraté byli na oplátku rozhořčeni tím, jak novináři z Tribune spekulovali nad tím, proč bylo potřeba psát pokyny zašifrovaně…. Načež následovalo to, že do redakce Tribune z celé země věrní čtenáři, příznivci a stoupenci republikánů začali zasílat podezřelé telegramy, ke kterým se během voleb dostali…

Naprostou většinu z 29 275 telegramů, které si během voleb demokratičtí politici mezi s sebou vyměnili, totiž společnost Western Union spálila již v roce 1876. Provedla to proto, aby je nemusela předat vyšetřovací komisi, kterou po volbách ustanovil Kongres. Společnost k tomu nevedly cíle politické, ale chtěla tím prokázat, že u korespondence, která je jí svěřena existuje naprostá diskrétnost.

Přesto se díky různým lidem podařilo z této obrovské korespondence v redakci shromáždit 400 kusů zašifrovaných telegramů.

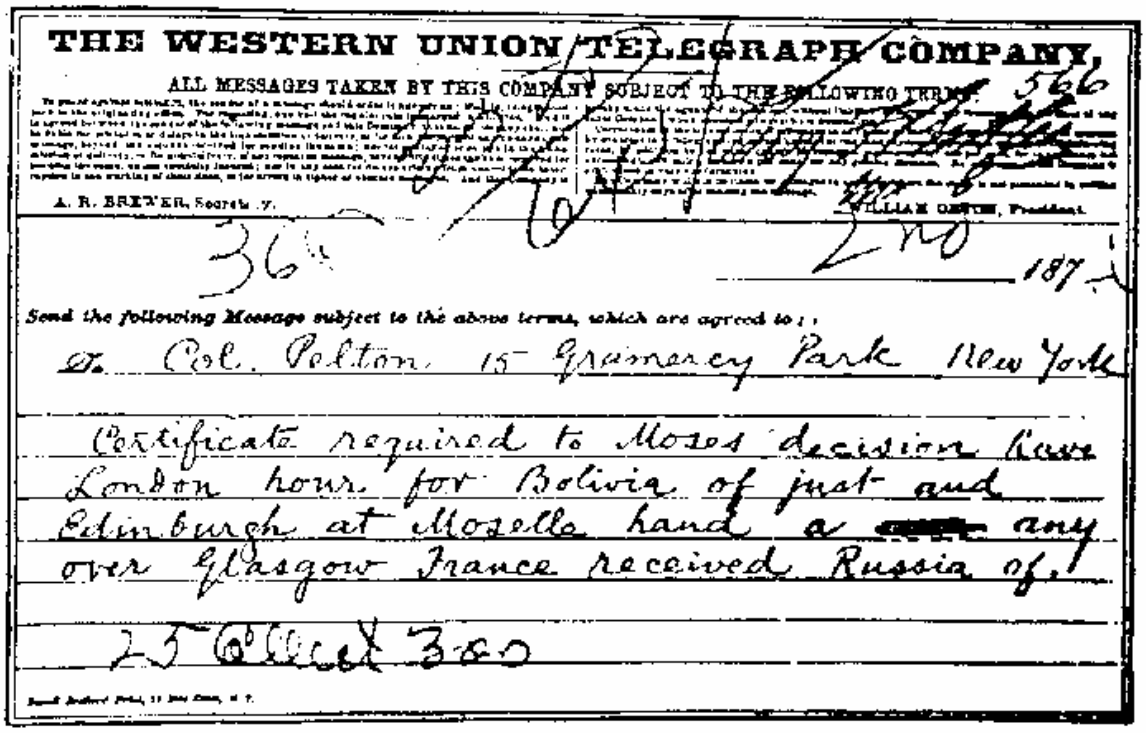
Šéfredaktor listu New York Tribune se rozhodl pokusit tyto šifrové telegramy vyluštit. Tedy přesněji začal shánět někoho, kdo by byl schopen tuto složitou práci provést. Těmito luštiteli se stali John R.G.Hassard, William M.Grosvenor a Edward S.Holden.
Všichni tři pracovali zcela nezávisle a každý z nich vyluštil několik set telegramů. Nevyluštěny zůstaly pouze tři telegramy ….

Kdo byli tito pánové, dobrovolní amatérští luštitelé ?

John R.G.Hassar (1836-1888), redaktor listu New York Tribune 42 let, proslavil se především reportáží o premiéře Wagnerova cyklu Prsten Nibelungů.
Byl znám jako významný popularizátor Wagnerovy hudby v Americe. Zemřel na tuberkulózu (http://www.famousamericans.net/johnrosegreenehassard/).

Redaktor William M.Grosvenor (1835-1900), 43 let, nadaný šachista, lingvista a matematik redaktor hospodářské rubriky novin New York Tribune. V občanské válce velel pluku složenému z černochů. Stal se známým odhalením tzv. whisky-gangu, kdy pomocí statistických metod prokázal, že palírny lihu v St. Louis šidí stát na daních.
(http://www.tamu.edu/pvamu/library/hyman13.htm , Card 85)

Posledním byl 31-letý matematik z observatoře válečného námořnictva, Edward S.Holden (1846-1914). Založil Astronomickou společnost Pacifiku. Později se stal známým astronomem a vědcem. Jeho jménem je pojmenován jeden z kráterů na Marsu.
(http://www.nationmaster.com/encyclopedia/Edward-S.-Holden).


THE WESTERN UNION TELEGRAPH COMPANY,

ALL MESSAGES TAKEN BY THIS COMPANY SUBJECT TO THE FOLLOWING TERMS

Send the following Message subject to the above terms, which are agreed to:

Certificate required to Moses decision Knox London hour for Bolivia of just and Edinburgh at Mozelle hand a any over Glasgow France received Russia of.

Na obrázku je jeden z šifrových telegramů, ve kterém se nabízí za hlasy voličů za Floridu 200 000 USD.

Ukážeme si na třech jednoduchých příkladech, jaké šifry byly tehdy vlastně použity.

Příklad 1 (slovníkový kód – dohodnutá kniha)

Demokraté jako jeden ze šifrových systémů během volební kampaně používali např. slovníkový kód, dohodnuté knihy byly pro komunikaci mezi různými subjekty pochopitelně různé.

Takovýto telegram pak vypadal např. takto (uveden skutečný text jednoho z telegramů) :

BY VIZIER ASSOCIATION INNOCUCUS TO NEGLIGENCE CUNNING MINUTELY PREVIOUSLY READMIT DOLTISH TO PURCHASED AFAR ACT WITH CUNNING AFAR SACRISTY UNWRIGHED AFAR POINTER ...

V uvedeném příkladě byl odesílatel a příjemce dohodnut na knize English Dictionary, vydání Londýn 1876.

Při šifrování se postupovalo v tomto konkrétním případě takto:
- šifrant vyhledal slovo v dohodnutém slovníku (knize)
- poznamenal si pořadí slova na stránce
- vzal slovo o čtyři stránky knihy vepředu, které má na stránce stejné pořadí
- toto slovo zapsal jako kódový ekvivalent

Při dešifrování se postupovalo takto (ukážeme na prvním slově zašifrovéného telegramu textu BY):
- dešifrant vyhledal slovo BY v dohodnuté knize
- toto slovo našel na straně 30 a bylo na 29 pozici
- nalistoval o čtyři stránky dozadu na stránku 34
- odpočítal 29 slov a získal prvé slovo zprávy - CERTIFICATE

Postupně tak získal celý otevřený text (uvádím již pouze překlad):
Osvědčení bude vydáno jednomu demokratovi. Musíte koupit republikánského elektora, aby bylo možno jednat s demokratem a zajistit hlas a vyhnout se nesnázím. Složte 10 000 dolarů v můj prospěch u Kountze Brothers, Twelve Wall Street. Čekám na odpověď. J.N.H.Patrick.

Právě tento telegram byl jedním z těch, které prokazatelně dokumentovali, že demokraté se snažili koupit republikánského elektora a to za 10000 USD. Mimochodem z této nabídky, ale ve skutečnosti sešlo, nastalo totiž zpoždění v doručení telegramu….

Příklad 2 – Digrafická substituční šifra (šifrová abeceda tvořena číslicemi)

Jedná se o speciální druh substituční šifry, kdy každý znak abecedy otevřeného textu je nahrazen dvojicí znaků šifrové abecedy. Speciální význam sehrály tyto šifry při vyjádření znaků abecedy otevřeného textu pomocí číslic. Tedy v případě, kdy šifrová abeceda byla tvořena číslicemi od 0 do 9. Zpravidla se pro vyšší bezpečnost s takto získaným šifrovým textem dále pracovalo, využívala se transpozice šifrového textu nebo jiná úprava, viz např. přičítání hesla, následná transpozice nebo zlomkové šifry.

V případě některých telegramů byla demokraty použita digrafická šifra, kde každý znak byl vyjádřen dvojicí čísel. K následnému přešifrování takto získaného textu však již nedocházelo. Jednalo se tedy vlastně jen o klasickou jednoduchou substituci, kdy znaky šifrové abecedy byly dvojice čísel. Díky tomu bylo luštění velmi jednoduché a systém (na rozdíl od předchozího) lze označit za velmi, velmi slabý a svědčí jen o tom, že americký kontinent v této disciplíně za tehdejší Evropou značně pokulhával….

Zde je jeden z takovýchto telegramů:

S. PASCO AND E. M. L'ENGLE
84 55 84 25 93 34 82 31 31 75 93 82 77 33 55 42 93 20 93 66 77 66 33 84 66
31 31 93 20 82 33 66 52 48 44 55 42 82 48 89 42 93 31 82 66 75 31 93
DANIEL

Luštitelé měli k dispozici dokonce více takto zašifrovaných telegramů. Snadno tak pomocí frekvence šifrových znaků zjistili význam jednotlivých dvojic čísel :

```
20 = D   33 = N   44 = H   62 = X   77 = G   89 = Y
25 = K   34 = W   48 = T   66 = A   82 = I   93 = E
27 = S   39 = P   52 = U   68 = F   84 = C   96 = M
31 = L   42 = R   55 = O   75 = B   87 = V   99 = J
```

Výsledek lze zapsat do následující převodové tabulky

```
        1  2  3  4  5  6  7  8  9  0
       ------------------------------
2 .                K     S        D .
3 .   L     N  W               P    .
4 .      R     H           T       .
5 .      U        O                 .
6 .      X           A     F        .
7 .                B     G          .
8 .      I     C        V     Y     .
9 .         E        M        J     .
       ------------------------------
```

Otevřený text uvedeného telegramu tedy zní:

S. PASCO AND E. M. L'ENGLE
Cocke will be ignored, Eagan called in Authority reliable.
DANIEL

Zajímavé je, že nebyla pro převod otevřených znaků na šifrové ekvivalenty použitá tabulka o rozměrech 5x5, jak je u šifry tohoto typu obvyklé (tzv. tabulka Polybiova typu), ale o rozměrech 8x10. Tabulka o rozměrech 5x5 by dostatečně pokryla převod všech znaků abecedy otevřeného textu, při rozměrech 8x10 zůstává řada šifrových „znaků“ nevyužita. Určité opodstatnění použití takto velké tabulky by bylo využití dalších možností na převod (zašifrování) např. interpunkčních znaků (., ? /) , číslic nebo dokonce jmen osob, měst a případně dalších často používaných slov. Jinou možnou variantou by bylo možné využití „volných pozic“ pro převod četných znaků otevřeného textu. Např. E by mohlo mít šifrový ekvivalent mimo uvedených 93 ještě 22, 60, 73 , písmeno A mimo použité šifrové záměny 66 ještě navíc 21, 70, 97 atd. Tím by se stala šifra homofonní a luštění na základě frekvencí by se luštitelům (zvláště u krátkých telegramů) velmi výrazně ztížilo.

Příklad 3 – Digrafická substituční šifra (šifrová abeceda – písmena)

V případě některých telegramů byl demokraty použit jiný typ digrafické šifry. Tentokráte byl každý znak vyjádřen pomocí dvou písmen. Tak například písmeno O otevřeného textu bylo vyjádřeno pomocí AA .

Jakmile si to luštitelé uvědomí, pak při řešení stačí opět postupovat obdobně jako při luštění klasické jednoduché substituce.

Jedním z odeslaných a takto zašifrovaných telegramů byl např. tento:

GEO. F. RANEY, Tallahassee.
P P Y Y E M N S N Y Y Y P I M A S H N S Y Y S S I T E P A A E N S H N S P E N N S S
H N S M M P I Y Y S N P P Y E A A P I E I S S Y E S H A I N S S S P E E I Y Y S H N Y
N S S S Y E P I A A N Y I T N S S H Y Y S P Y Y P I N S Y Y S S I T E M E I P I M M E I
S S E I Y Y E I S S I T E I E P Y Y P E E I A A S S I M A A Y E S P N S Y Y I A N S S S E
I S S M M P P N S P I N S S N P I N S I M I M Y Y I T E M Y Y S S P E Y Y M M N S Y Y
S S I T S P Y Y P E E P P P M A A A Y Y P I I T
DANIEL

Digrafická šifra v tomto případě využívá pouze deset odlišných písmen. Text zprávy stačí rozdělit na dvojice a dále začít luštit pomocí klasických postupů. Při řešení si luštitel vystačí s využitím frekvenční analýzy a případně s hledáním předpokládaných slov.

Vyřešením dostali luštitelé následující převodovou tabulku:

AA = O	EN = Y	IT = D	NS = E	PP = H	SS = N
AI = U	EP = C	MA = B	NY = M	SH = L	YE = F
EI = I	IA = K	MM = G	PE = T	SN = P	YI = X
EM = V	IM = S	NN = J	PI = R	SP = W	YY = A

Vyluštěný otevřený text zní:

GEO. F. RANEY, Tallahassee.
Have Marble and Coyle telegraph for influential men from Delaware and Virginia. Indications of weaking here. Press advantage and watch board.
DANIEL

Převodová tabulka použité digrafické šifry lze zapsat (obdobně jako v minulém případě) do tabulky o rozměrech 8x10 takto :

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

Poznámka k řešení příkladu 2 a 3:

Známý kryptolog William F. Friedman si uvědomil, že výběr „obsazených šifrových dvojic“ v tabulkách 8x10 uvedených příkladů dvě a tři je „shodný“!

Stačí totiž „zpřeházet“ řádky a sloupky tabulky s písmennými souřadnicemi a dostaneme shodnou tabulku jako se souřadnicemi číselnými:

		H	I	S	P	A	Y	M	E	N	T
		1	2	3	4	5	6	7	8	9	0
H	1	.									.
I	2	.				K		S		D	.
S	3	.	L		N	W				P	.
P	4	.		R		H			T		.
A	5	.		U			O				.
Y	6	.		X				A		F	.
M	7	.					B		G		.
E	8	.		I		C			V		Y	.
N	9	.			E			M			J	.
T	0	.										.

Je tedy pravděpodobné, že pro šifrování telegramů odpovídajících příkladu dva a tři byla ve skutečnosti použita jen jedna převodová tabulka, která měla uvedeny souřadnice číselné i textové a šifrant si mohl při převodu textu vybrat jednu z těchto nabízených možností.

Klíč sloužící k vytvoření a zapamatování takovéto tabulky - HIS PAYMENT, byl tak v případě korespondence, která se týkala pokusů o uplácení, více než symbolický.

Literatura

[1] Vondruška, P.: Dešifrované telegramy dokazují, že se demokraté snažili podplatit republikány při prezidentských volbách, Toulky zajímavými zákoutími kryptologie - 4.díl, Technet.idnes.cz, 2.11.2004
http://technet.idnes.cz/sw_internet.asp?r=sw_internet&c=A041101_5285844_sw_internet

[2] Vondruška, P.: Kryptologie, šifrování a tajná písma, edice OKO, Albatros 2006

[3] Kahn, D. : Codebreakers, Macmillan Co., New York, 1967

[4] LANAKI http://www.und.nodak.edu/org/crypto/crypto/lanaki.crypt.class/

[5] Friedman, William F. and Callimahos, Lambros D., Military Cryptanalytics Part I - Volume 1, Aegean Park Press, Laguna Hills, CA, 1985.

[6] http://www.uselectionatlas.org/USPRESIDENT/GENERAL/pe1876.html

[7] http://www.famousamericans.net/johnrosegreenehassard/

[8] http://www.tamu.edu/pvamu/library/hyman13.htm , Card 85

[9] http://www.nationmaster.com/encyclopedia/Edward-S.-Holden

C. Kircherovo šifrování aneb Dobrý voják Švejk

Moptivační (dubnová) ukázka z knihy
Jarsolava Hašek : Osudy dobrého vojáka Švejka
Díl : Slavný výprask, kapitola 1. : Přes Uhry

„Sie, Kadett," řekl hejtman Ságner, „dokud vám nedovolím mluvit, tak mlčte, poněvadž se vás nikdo na nic neptal. Ostatně vy jste zatraceně chytrý voják. Nyní vám předkládám zcela důvěrné informace, a vy si je zapisujete do svého zápisníku. Při ztrátě notesu očekává vás polní soud."

Kadet Biegler měl ještě ke všemu ten zlozvyk, že se vždy snažil každého přesvědčit nějakou výmluvou, že to myslí dobře.

„Poslušně hlásím, pane hejtmane," odpověděl, „že i při eventuelní ztrátě zápisníku nikdo nerozluští, co jsem napsal, neboť to stenografuji a mé zkratky nikdo po mně nepřečte. Užívám anglického systému stenografie."

Všichni se na něho podívali opovržlivě, hejtman Ságner máchl rukou a pokračoval ve své přednášce.

„Zmínil jsem se již o novém způsobu šifrování depeší v poli, a jestli vám snad bylo nesrozumitelným, proč právě vám byla odporučena z novel Ludvíka Ganghofera Die Sünden der Väter str. 161, jest to, pánové, klíč k nové šifrovací metodě, platné na základě nového nařízení štábu armádního sboru, ku kterému jsme přiděleni. Jak vám známo, je mnoho metod šifrování důležitých sdělení v poli. Nejnovější, které my používáme, jest číselná metoda doplňovací. Tím také odpadají minulého týdne doručené vám od štábu pluku šifry a poučení k jich odšifrování."

„Erzherzogs Albrechtsystem," zamumlal pro sebe snaživý kadet Biegler, „8922 = R, převzatý z metody Gronfelda."

„Nový systém jest velice jednoduchý," zněl vagónem hlas hejtmanův. „Osobně obdržel jsem od pana plukovníka druhou knihu i informace.

Máme-li například dostat rozkaz: ‚Auf der Kote 228, Maschinengewehrfeuer linksrichten,' obdržíme, pánové, tuto depeši: ‚Sache - mit - uns das - wir - aufsehen - in - die - versprachen - die - Martha - dich - das - ängstlich dann - wir - Martha - wir - den - wir Dank - wohl - Regiekollegium - Ende - wir versprachen - wir - gebessert - versprachen - wirklich - denke - Idee - ganz - herrscht - Stimme - letzten.' Tedy náramně jednoduché beze všech zbytečných kombinací. Od štábu po telefonu na batalión, batalión po telefonu na kumpanie. Obdržev velitel tuto šifrovanou depeši, rozluští ji tímto způsobem. Vezme Die Sünden der Väter, otevře si str. 161 a začne seshora hledat na protější straně 160 slovo Sache. Prosím, pánové. Poprvé jest Sache na str. 160 ve větním pořadí 52, slovem, tedy na protější straně 161 vyhledá se dvaapadesáté písmeno seshora. Všimněte si, že je to A. Dalším slovem v depeši je mit. Jest to na stránce 160 ve větním pořadí 7, slovo, odpovídající 7. hlásce na stránce 161, písmence u. Potom přijde uns, to jest, sledujte mě prosím bedlivě, 88. slovo, odpovídající 88. písmence na protější 161. straně, kterou jest f, a máme rozluštěno Auf. A tak pokračujeme, až zjistíme rozkaz: ‚Na kótě 228 řídit oheň strojních pušek nalevo: Velice důmyslné, pánové, jednoduché a nemožné rozšifrovat bez klíče: 161. str., Ludvík Ganghofer: Die Sünden der Väter."

Všichni mlčky prohlíželi si nešťastné stránky a nějak se nad tím povážlivě zamyslili. Panovalo chvíli ticho, až najednou vykřikl ustaraně kadet Biegler: „Herr Hauptmann, ich melde gehorsam: Jesus Maria! Es stimmt nicht ...“

A bylo to opravdu velice záhadné. Ať se namáhali jak chtěli, nikdo kromě hejtmana Ságnera nenašel na stránce 160 ona slova a na protější straně 161, kterou začínal klíč, jemu odpovídající písmeny.

„Meine Herren,“ zakoktal hejtman Ságner, když se přesvědčil, že zoufalý výkřik kadeta Bieglera odpovídá pravdě, „co se to jen stalo? V mém Ganghoferovi Die Sünden der Väter je to, a ve vašem to není?“

„Dovolte, pane hejtmane,“ ozval se opět kadet Biegler. „Dovoluji si upozornit, že román Ludvíka Ganghofera má dva díly. Račte se prosím přesvědčit na první titulní straně: ‚Roman in zwei Bänden’. My máme I. díl a vy máte II. díl,“ pokračoval důkladný kadet Biegler, „je proto nabíledni, že naše 160. i 161. stránka neodpovídá vaší. My tam máme zcela něco jiného. První slovo rozšifrované depeše má být u vás Auf, a nám vyšlo Heu!“
Všem bylo nyní zcela jasno, že Biegler není snad přece jen takový hlupák.

„Já mám II. díl ze štábu brigády,“ řekl hejtman Ságner, „a patrně se zde jedná o omyl. Pan plukovník objednal pro vás I. díl. Dle všeho,“ pokračoval tak, jako by to bylo přesné a jasné a on to věděl už dávno předtím, než měl svou přednášku o velmi jednoduchém způsobu šifrování, „spletli to ve štábu brigády. Neudali pluku, že jde o II. díl, a tak se to stalo.“
…

„Podivný případ, pánové,“ ozval se opět hejtman Ságner, jako by chtěl navázat rozmluvu, poněvadž to ticho bylo velice trapné. „V brigádní kanceláři jsou obmezenci.“

„Dovoluji si podotknout,“ ozval se opět neúnavný kadet Biegler, který opět se chtěl pochlubit svými rozumy, „že podobné věci důvěrného, přísné důvěrného rázu neměly by od divize jít kanceláří brigády. Předmět týkající se nejdůvěrnější záležitosti armádního sboru mohl by být oznámen přísně důvěrným oběžníkem jedině velitelům částí divizí i brigád, pluků. Znám systémy šifer, které byly používány ve válkách o Sardinii a Savojsko, v anglo-francouzské kumpanii u Sebastopolu, při povstání boxerů v Číně i za poslední rusko-japonské války. Systémy tyto byly předávány...“

„Nám starého kozla na tom záleží, kadete Bieglere,“ s výrazem opovržení a nelitosti řekl hejtman Ságner; „je jisto, že systém, o který šla řeč a který jsem vám vysvětloval, je nejen jeden z nejlepších, ale můžeme říct nedostižitelných. Všechna oddělení pro protišpionáž našich nepřátelských štábů mohou jíti na hrnec. Kdyby se rozkrájeli, nepřečtou naše šifry. Jest to něco zcela nového. Tyto šifry nemají předchůdce.“

Snaživý kadet Biegler významně zakašlal. „Dovoluji si,“ řekl, „pane hejtmane, upozorniti na knihu Kerickhoffovu o vojenském šifrování. Knihu tu může si každý objednat ve vydavatelstvu Vojenského naučného slovníku. Jest tam důkladně popsána, pane hejtmane, metoda, o které jste nám vypravoval. Vynálezcem jejím je plukovník Kircher, sloužící za Napoleona I. ve vojsku saském. Kircherovo šifrování slovy, pane hejtmane: každé slovo depeše se vykládá na protější stránce klíče. Metoda ta zdokonalena nadporučíkem Fleissnerem v knize Handbuch der militärischen Kryptographie, kterou si každý může koupit v nakladatelství Vojenské akademie ve Vídeňském Novém Městě. Prosím, pane hejtmane.“
Kadet Biegler sáhl do ručního kufříku a vytáhl knížku, o které mluvil, a pokračoval: „Fleissner udává týž příklad, prosím račte se všichni přesvědčit. Týž příklad, jak jsme slyšeli:
Depeše: Auf der Kote 228, Maschinengewehrfeuer linksrichten.

Klíč: Ludwig Ganghofer: Die Sünden der Väter Zweiter Band.
A podívejte se prosím dále: šifra ‚Sache mit uns das wir aufsehen in die versprachen die Martha...' a tak dále. Právě jak jsme před chvílí slyšeli."

Ve štábu armády si někdo z pánů generálů ulehčil práci. Objevil Fleissnerovu knihu o vojenském šifrování, a už to bylo hotovo.
Po celou tu dobu bylo vidět, že nadporučík Lukáš přemáhá jakési divné duševní rozčilení. Kousal se do pysku, chtěl něco říct, ale nakonec počal mluvit o něčem jiném, než bylo jeho prvním úmyslem.
…
„Nesmí se to brát tak tragicky," řekl s podivnými rozpaky, „během našeho pobytu v lágru v Brucku nad Litavou změnilo se již několik systémů šifrování depeší. Nežli přijedeme na frontu, tak zas budou nové systémy, ale myslím, že v poli není čas na luštění takových kryptogramů. Než by kdokoliv z nás rozluštil podobný šifrovaný příklad, dávno už by bylo po kumpanii, batalionu i po brigádě. Praktického významu to nemá!"

Hejtman Ságner velice nerad přikývl hlavou. „V praxi," pravil, „alespoň pokud se týče mých zkušeností ze srbského bojiště, neměl nikdo času na luštění šifer. Neříkám, že by šifry neměly významu při delším pobytu v zákopech, když se zakopáme a čekáme. Že se šifry mění, je také pravda."
Hejtman Ságner ustupoval na celé čáře: „Velkou část viny na tom, že se dnes od štábů na pozici čím dále tím méně používá šifer, je to, že naše polní telefony nejsou přesné a nereprodukují, zejména při dělostřeleckém ohni, jasné jednotlivé slabiky. Vy prostě neslyšíte ničeho a způsobuje to zbytečný chaos." Odmlčel se.

… Hejtman Ságner ustupoval na celé čáře: „Velkou část viny na tom, že se dnes od štábů na pozici čím dále tím méně používá šifer, je to, že naše polní telefony nejsou přesné a nereprodukují, zejména při dělostřeleckém ohni, jasné jednotlivé slabiky. Vy prostě neslyšíte ničeho a způsobuje to zbytečný chaos." Odmlčel se.
...
„Za chvíli," řekl dívaje se oknem, „jsme v Rábu: Meine Herren! Mužstvo zde dostane po patnácti dekách uherského salámu. Půl hodiny rast."
...
Nadporučík Lukáš první vyřítil se ze štábního vagónu a šel k vagónu, kde nalézal se Švejk.
...
„Švejku, pojďte sem," řekl, „nechte si vaše pitomé výklady a raději mně pojďte něco vysvětlit."

„Bezevšeho, poslušně hlásím, pane obrlajtnant." Nadporučík Lukáš odváděl Švejka a pohled, kterým ho sledoval, byl velice podezřívavý.
…
Nadporučík Lukáš během celé přednášky hejtmana Ságnera, která skončila takovým fiaskem, dopracoval se k jisté detektivní schopnosti, k čemuž nebylo třeba mnoho obzvláštních kombinací, neboť den před odjezdem hlásil Švejk nadporučíkovi Lukášovi: „Pane obrlajtnant, na batalióně jsou nějaký knížky pro pány lajtnanty. Vodnes jsem je z regimentskanclaje."
Proto když přešli druhé koleje, nadporučík Lukáš přímo se otázal, když zašli za vyhaslou lokomotivu, která čekala již týden na nějaký vlak s municí: „Švejku, jak to bylo tenkrát s těmi knížkami?"

„Poslušně hlásím, pane obrlajtnant, že je to moc dlouhá historie, a vy se vždy ráčíte rozčilovat, když vám všechno dopodrobna vypravuju.
...

Takhle bychom nebyli hotovi, Švejku," řekl nadporučík Lukáš, pokračuje ve výslechu, přičemž si předsevzal, že to nejpřísněji důvěrné musí být přirozeně úplně skryto, aby ten holomek Švejk nedělal zas z toho nějakou potřebu. „Znáte Ganghofera?"
„Čím má bejt?" otázal se Švejk se zájmem.
„Je to německý spisovatel, vy chlape pitomá," odpověděl nadporučík Lukáš.
...
Chtěl jsem jen vědět, zdali jste si všiml, že ty knížky, o kterých jste se vy mně sám zmiňoval, byly od Ganghofera. - Co je tedy s těmi knížkami?" vybouchl zlostně.
„S těmi, co jsem odnesl z regimentskanclaje na batalión?" otázal se Švejk. „Ty byly vopravdu vod toho sepsaný, vo kterým jste se mé ptal, jestli ho neznám, pane obrlajtnant. Já jsem dostal telefonogram přímo z regimentskanceláře. Voni totiž chtěli ty knížky poslat na batalionskanclaj, ale všichni tam byli pryč i s dienstführendrem, poněvadž museli bejt v kantýně, když se jede na front, a poněvadž žádnej neví, jestli bude ještě někdy sedět v kantýně.
...
Voni totiž ty knížky byly vo dvou dílech. První díl zvlášť, druhej díl zvlášť. Nikdy v životě jsem se tak tomu nezasmál, poněvadž jsem už v životě přečet mnoho knih, ale nikdy jsem nezačal číst něco vod druhýho dílu. A von mně tam ještě jednou říká: ‚Tady máte první díly a tady máte druhý díly. Kerej díl si mají číst páni oficíři, to už vědí.' Tak jsem si pomyslil, že jsou všichni vožralí, poněvadž když se má kniha číst vod začátku, takovej román, jakej jsem přines, vo těch Sünden der Väter, poněvadž znám taky německy, že se musí začít s prvním dílem, poněvadž nejsme židi a nečteme to pozpátku. Proto jsem se taky vás ptal, pane obrlajtnant, po telefonu, když jste se vrátil z kasina, a hlásil jsem vám to o těch knížkách, jestli snad teď na vojně je to převrácený a jestli se nečtou knihy v obráceným pořádku, napřed druhý a potom teprve první díl. A vy jste mně řek, že jsem vožralý hovado, když ani nevím, že v otčenáši je napřed ‚Otče náš' a potom teprve ‚amen'. - Je vám špatně, pane obrlajtnant?" otázal se se zájmem Švejk, když bledý nadporučík Lukáš zachytil se stupátka k vodojemu vyhaslé lokomotivy.
...
Jednou jsem koupil krvák vo Růžovi Šavaňů z Bakonskýho lesa a scházel tam první díl, tak jsem se musel dohadovat vo tom začátku, a ani v takovej raubířskej historii se neobejdete bez prvního dílu. Tak mně bylo úplně jasný, že je to vlastně zbytečný, kdyby páni oficíři začli číst napřed druhý díl a potom první, a jak by to vypadalo hloupě, kdybych u batalionu byl vyřídil to, co říkali v regimentskanclaj, že páni oficíři už vědí, kerej díl mají číst. Vono mně to vůbec s těma knížkama, pane obrlajtnant, připadalo strašně nápadný a záhadný. Já věděl, že páni oficíři vůbec málo čtou, a když je řvava válečná..."

Tak jsem tedy, pane obrlajtnant, vodnes do batalionskanclaje jenom ty první díly vod toho románu a druhej díl jsem nechal zatím v naší kompaniekanclaji. Měl jsem ten dobrej úmysl, až si páni oficíři přečtou první díl, že pak se jim vydá druhej díl, jako z knihovny, ale najednou přišlo to, že se jede, a telefonogram po celém batalionu, že všechno zbytečný se má dát do regimentsmagacínu. Tak jsem se ještě zeptal pana Vaňka, jestli druhej díl toho románu považuje za něco zbytečnýho, a von mně řekl, že vod doby těch smutných zkušeností v Srbsku, v Haliti a v Uhrách se žádný knihy pro zábavu nevozejí na front, a ty schránky v městech, aby se sbíraly vodložený noviny pro vojáky, ty že jsou jedině dobrý, poněvadž do novin se dá balit dobře tabák nebo seno, co vojáci kouřejí v dekunkách. Na batalióně už rozdali ty první díly vod toho románu a ty druhý díly jsme vodnesli do magacínu."

D. Úloha k luštění …

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

Pro ty čtenáře, kteří se již nemohou dočkat tradiční podzimní soutěže, jsem zařadil do tohoto dubnového čísla šifrový text a vypisuji soutěž v jeho prolomení.

K luštění této úlohy srdečně zvu všechny zájemce a to nejen z řad čtenářů e-zinu. Do soutěže není potřeba se nijak přihlašovat. V případě úspěchu stačí jednoduše na můj e-mail zaslat odpovídající otevřený text.

Pro prvého řešitele je připravena cena, kterou pro vítěze věnovalo nakladatelství Zoner Press. Jedná se o knihu Google Hacking (http://www.zonerpress.cz/kniha-google-hacking.html). Pro druhého v pořadí je připraveno tričko, které jako sponzorský dar věnoval portál soom.cz http://www.soom.cz/index.php?name=box&box=projects/triko/main .

Informaci o tom, že úloha již byla vyřešena a byly doručena alespoň dvě správná řešení naleznete v Crypto-News (http://crypto-world.info/news/index.php?sekce=s).

Správné řešení úlohy bude uvedeno v příštím čísle našeho e-zinu.

Soutěžní úloha 4/2007

```
04235 04006 04008 04210 04017 04009 04005 04003 04007
04220 04002 04004 04021 04004 04003 04321 04017 04001
04228 04009 04013 04009 04001 04002 04008 04002 04001
04046 04005 04002 04187 04001 04004 04201 04003 04009
04232 04018 04003 04193 04001 04007 04198 04020 04003
04170 04004 04006 04215 04018 04007 04221 04002 04002
```

Doporučená literatura:

[1] e-zin Crypto-World 4/2007, http://crypto-world.info/
[2] Vondruška, P.: Kryptologie, šifrování a tajná písma, edice OKO, Albatros 2006
http://crypto-world.info/oko/index.php

E. O čem jsme psali v dubnu 2000 – 2006

Crypto-World 4/2000

Crypto-World 4/2001

Crypto-World 4/2002

Crypto-World 4/2003

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a 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 sešity GCUCMP, 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:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
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@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.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/