Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 11, číslo 1/2009 **15.leden 2009**

1/2009

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1306 registrovaných odběratelů)

Obsah :

Příloha: ---

A. Novoroční perlička o luštění šifrových zpráv

Mgr. Karel Šklíba (karel.skliba@crypto-world.info)

Již 29 let trpím zcela nevinnou zábavou. Vypisuji a označuji si pasáže v literatuře, nikoliv odborné, ale v beletrii, ve kterých se vyskytnou zmínky o problematice šifrování. Úplnou lahůdku pak pro mne představují ta díla, kde jsou popisovány metody luštění nějakého šifrového systému. V létě minulého roku jsem v jednom mimopražském antikvariátu náhodou zalistoval knihou, jejíž vazba svou ošuntělostí napovídala stáří nejméně předválečnému. Stejnou náhodou jsem knihu ihned zpočátku otevřel v místě, kde se nacházel popis luštění šifrovaného dopisu. Zjistil jsem, že v regálu se nachází ještě dvojče této knihy – asi druhý díl. Protože cena obou knih byla ryze symbolická, obě jsem zakoupil jako přírůstek do své „sbírky“. Ukázalo se, že se jedná o dva detektivní romány Vladimíra Neffa, vydané v letech 1933, resp. 1934, a že oba mají podtitul detektivka proti všem pravidlům. Podtitul obou knih skutečně nelhal. Sám autor v doslovu ke druhé a s tímto hrdinou určitě poslední knize uvedl, že jeho cílem byla detektivka česká, která není plná krvežíznivosti a vražd, jak je zvykem u importovaných detektivek chvatně a hanebně překládaných, jež kazí naši domácí mentalitu. Jeho mottem bylo „Není-li vraždy, je jistě veselost spíše namístě“. Knihy jsem přečetl rychle a dosti letmo, neboť nad většinou zápletek bylo nutno spíše kroutit hlavou. Nuda to ale nebyla, trochu to mohlo připomínat styl Saturnina. Nebo příhody Mr. Beana? Nejspíš jako příhody z cirkusu Monty Python. Ale to už jsem si zapřeháněl.

První kniha se jmenuje Nesnáze Ibrahima Skály a obsahuje skvostnou kapitolu o postupu luštění šifrovaného dopisu. Druhá kniha se jmenuje Papírové panoptikum a je volným

pokračováním prvního detektivního románu. V této knize je již šifrová problematika bohužel pominuta. Pátá kapitola z první knihy však myslím stojí za reprodukování, proto zde uvádím její podstatnou část v doslovném znění:

Jak Ibrahim rozluštil šifrovaný dopis

Rozpaky se mne, totiž autora, zmocňují a proto váhám s trapnou chvílí, kdy budu nucen vyrukovati s obsahem toho trapného, proklatého šifrovaného dopisu.

Jeho obsah je totiž nesmírně hloupý a budu proto vydán posměchu a utrhání. Eventuelní čtenář totiž okamžitě prokoukne můj plytký trik a na první pohled pozná, do jakého nesmyslu se Ibrahim svým luštěním šifrovaného dopisu pustil. Proto oddálím tu strašnou chvíli tím, že dám naposledy vystoupiti Ibrahimově služce Marii.

- Tak já teda du, mladej pane. Když chtěj, abych na hodinu šla, tak já du. Maj se dobře a vzpomenou si někdy na mne. Já to s nima myslila dycky do- do-.

…….

Z vedlejšího pokoje bylo ještě dlouho slyšet neurčité vlykavé zvuky, jaké vydávají staré ženy na pohřbu. Marie se patrně pomalu a důstojně ubírala ke dveřím. Nad klikou uronila slzy nejtrpčí a nejdelší. Ibrahim trna poslouchal, jak v předsíni váhavě zavrzal proutěný košík. Při konečném bouchnutí dveří mu spadl nesmírný kámen ze srdce.

Nový život.

Hladově se vrhl k šifrovanému dopisu.

Teď začala pro autora chvíle hanby.

Usmolený papírek byl popsán na obou stranách. Na jedné straně stálo tužkou velikými tiskacími písmenami:

NE PAS OUBLIER ANNI VERSAIRE DE DODE !!!!!!!!

A na druhé obyčejným písmem:

Renard argenté ????????

Moták zřejmě složitý, zlověstný a významný. První strana svou řadou kategorických vykřičníků zřejmě nasvědčovala, že obsahuje příkaz nebo důležité sdělení. A otazníky druhé strany prozrazovaly, že obsahuje úpěnlivou otázku, v nejvyšší tísni kladenou. Jak ale odkrýt podstatu těchto slov barbarsky pokroucených? Jak najít k nim klíč?

Upozorňuji eventuelního čtenáře, že teď bude následovat podrobný popis, jak si Ibrahim při svém těžkém úkolu počínal. Kdo se nezajímá o vědecké luštění šifrovaných dopisů, nechť přímo přeskočí ke konci kapitoly, kde najde brilantní výsledek Ibrahimových snah.

Měl tušení, že pro větu psanou tiskacími písmenami je jiný klíč než pro druhou. Proto si rozdělil svůj úkol na dvě části:

NE PAS OUBLIER ANNIVERSAIRE DE DODE

V motáku se nejčastěji vyskytovala samohláska E, šestkrát a A třikrát. Dobrá, to už bylo něco. Vybral si namátkou jednu stránku do češtiny přeloženého Hraběte Monte Christa a pracně spočítal, kolikrát se tu jednotlivá písmena vyskytují. Rekordu dosáhlo A číslem šedesát devět a E číslem padesát jedna. Ostatní bídně pokulhávala za těmito závratnými čísly. Jedině L se k nim přiblížilo počtem třicet jedna, ale to bylo hlavně tím, že na stránce se jedenáctkrát vyskytovalo cizokrajné jméno Villefort, jež pokaždé samo o sobě dvě L zkonsumovalo.

A teď pozor. Sledujte Ibrahimovu neúprosnou logiku, jež se ostatně nebezpečně podobá logice Zlatého Chrobáka.

Jelikož se v šifrovaném dopise nejčastěji vyskytovalo písmeno E a na stránce opravdového rozumného románu písmeno A, dalo se bezpečně soudit, že skutečný význam písmeny E je A. Podle tétéž úvahy pak skutečný význam A je E. A tak se počal Ibrahimovi rýsovati následující tekst:

. A . E . . . . . A . E . . . . A . . E A . A . . . A

Teď byla ale veškerá logická vodítka tak poněkud vyčerpána. Ostatní písmena, jako P, B, L, V, vyskytovala se v motáku jen jednou a O dvakrát. Výjimku ouze N a L počtem tři. Ibrahim učinil zoufalý pokus. V Monte Christovi se po A a E nejčastěji vyskytovalo L a proto nahradil D v tekstu písmenou L. Mohl sice zrovna tak dobře zvolit N, ale nebesa mu přála a on se rozhodl pro to pravé.

Tekst teď vypadal takto:

. A . E . . . . . A . E . . . . A . . E . . ALAL . LA

A teď nezbývalo Ibrahimovi, než se dát vést instinktem a zkoušet. Začátek motáku, podle A a E soudě, mohl by být palec, kábel, zajetí, pánev, kanec, papež, daleko, kámen, datel, házeti, Marek, vánek, pačes, pálení, rakev a řada jiných hamižných a nedůstojných slov. Ibrahim jich vyzkoušel s neuvěřitelnou trpělivostí třicet osm, než přišel na to pravé, a to slovo ZAJETÍ. Stálo ho to tři hodiny úmorné práce, ale výsledek byl překvapující. To kýžené slovo bylo jedno z prvních, která ho vůbec napadla a které, jak tomu obyčejně bývá, v hříšné slepotě zavrhl, aby se k němu zkroušeně vrátil.

N se podle toho rovnalo Z, O se rovnalo I a celý tekst podle těchto údajů doplněn vypadal takto:

ZAJETÍ . . . . A . EZZ . . A . . E . . ALAL . LA

Skupina Z . . A . . E mohla znamenat ZPRAVTE. Toto ovšem napadlo Ibrahima až po dalších třech hodinách úmorného zkoušení. Ale proč ne? Vždyť šifrovaný dopis nejenom že sám zpravuje, nýbrž může být i rozkazem k dalšímu zpravování. Podle toho pak I rovná se P, R rovná se V a (Ibrahim zajásal) S **rovná se** T, což nezvratně nasvědčuje, že první slovo, totiž zajetí, bylo voleno správně, neboť tam také S **rovná se** T.

Tekst pomalu nabýval srozumitelných obrysů.

ZAJETÍ . . . PAVEZZPRAVTEPVALALILA

Přítomnost druhého Z před slovem zpravte Ibrahima neznepokojovala. Jednalo se o zjevné přepsání.

A tak vyluštěná část tekstu, náležitě zčeštěna, vypadala takto:

Zajetí . . . pave, zpravte P. Vála. Lila.

Nakousnuté slovo –pave znamenalo samozřejmě v Opavě, čili bližší místní určení toho zajetí. Ano, ale v dešifrovaném tekstu se písmena V shodovala s písmenou R původního znění. Proto Ibrahim s odporem usoudil, že pisatel v chronické neznalosti pravopisu místo V užil F a tak výsledek luštění vypadal takto:

Zajetí . f Opavě. Zpravte P. Vála. Lila.

Význam posledního puntíku Ibrahim ovšem odkrýti nemohl. Bylo to bezpochyby počáteční písmeno jména zajatého.

Spokojil se s tím, že je blíže určil. To počáteční písmeno bylo samozřejmě jiné než všechna písmena, která se v dopise vyskytovala. Mohlo to být jedině B, C, D, G, H, K, M, N, Ř, S, Š, X, Y, Ž. Podle takových matných faktů se ovšem přesné jméno zajatého zjistiti nedá, ba ani počáteční písmeno jeho jména. Ibrahim si tedy vybral mnoho napovídající tajemné písmeno X a tak konečný výsledek byl tento: Zajetí Xovo f Opavě. Zpravte P. Vála. Lila.

Blažené hodino vykonané práce! Blažená hodino, odměno chvil trpkého úsilí, blažená hodino zdárného výsledku, blažená hodino radosti čisté a zdravé atakdále. Veliké atakdále! Jasný symbole věcí, jež v našem podvědomí klidně dřímají a jež nás napadnouti nechtějí.

Ibrahim byl bez sebe radostí. Dešifrovaná věta neznamenala mnoho, ale byl si jist, že mu pomůže odkrýti věci veliké a tajné.

- Kdo by to do Opavy řekl, pomyslil si.

Zbývala druhá část záhadného motáku:

Renard argenté????????

Když nahradil jednotlivá písmena těmi písmeny, jejichž význam odkryl v první části motáku, vypadalo to takto:

V A Z E V L V . A Z . . A ????????

Ať to Ibrahim kroutil jak chtěl, významu se dopíditi nemohl a tak byl nucen potvrditi svou první teorii, že písmena tiskací a obyčejná se luští dvěma odlišnými klíči. Druhý klíč ale pro přílišnou krátkost věty najíti nemohl a tak byl nucen se spokojiti větou první. Ta ale již sama o sobě byla obrovskou odměnou jeho strašlivé mravenčí píle.

Eventuelní čtenář mne jistě bude obviňovat z nelogičnosti, řekne, že muž jako Ibrahim, muž požívavší výhody akademického vzdělání, požívavší dobrodiní vysokého školení, musil mít alespoň slabé zdání o francouzštině.

Lituji. Myji si ruce. Ibrahim znal z tohoto jazyka jen jedno slovo a sice monsieur a i to vyslovoval monsjé. Abych mu neubližoval, znal ještě madame a sauce tartare, ale ani jedno z těchto slov se na lístku nevyskytovalo a tak neměl ani nejmenšího zdání, že se jedná o naprosto nevinný francouzský tekst. A vůbec, tak docela nevinný nebyl, jak se eventuelní čtenář v následujících kapitolách dozví. A vůbec já za hloupost svého hrdiny nemůžu. A vůbec, není u nás řada nadějných mladých mužů, kteří mluví hanebně česky, o němčině ani nemluvě a přitom se horlivě učí arabštině nebo esperantu?

Zde končí 5. kapitola knihy a i popis toho, kam až vedou slepé uličky v luštitelském nadšení. A Vladimír Neff to excelentně vykreslil, včetně své mírné ironie k luštitelům Hrdina Ibrahim se teprve po dalších pěti kapitolách dozví, že zlosyn jménem Rikitiki si ve své mateřštině poznamenal Nezapomenout na Dodiny narozeniny!!!!!!!!Stříbrná liška???????? A připadal si jako Donkyšot, ten středověký gentleman, kterého pobláznily knížky, který chtěl něco podle nich zažít, s někým bojovat, s někým se rvát a bojoval s mlýny.

Použitá literatura:

[1] Neff Vladimír: Nesnáze Ibrahima Skály, A. Neubert Praha 1933

[2] Neff Vladimír: Papírové panoptikum, A. Neubert Praha 1934

B. Mohutné multikolize a multivzory hašovacích funkcí BLENDER-n

RNDr. Vlastimil Klima, nezávislý kryptolog, Praha,
(http://cryptography.hyperlink.cz, v.klima@volny.cz)

Abstrakt
Blender-n [1] je jeden z 51 kandidátů na hašovací funkci SHA-3, které postoupily do prvního kola mezinárodní soutěže na nový hašovací standard. V tomto příspěvku prezentujeme multikolizní a multivzorový útok na hašovací funkci Blender-n pro všechny velikosti výstupu n = 224, 256, 384 a 512. Složitost útoku a požadavky na paměť pro nalezení 2^{2n} (multi)vzorů (a multikolizí) algoritmu Blender-n jsou řádově pouze 10 krát větší než nalezení kolize náhodné hašovací funkce s n/2 výstupními bity.

Všechny předchozí útoky na Blender-n byly založeny na triku (Joux, [2]) s využitím mnoha zpráv. Naše útoky využívají jednu zprávu, u níž konstruujeme několik pevných bodů. Stavový registr kompresní funkce Blenderu má osm slov. Vhodnou volbou slov zprávy donutíme polovinu tohoto registru vrátit se do původního stavu. Potom nalezneme kolizi ve zbytku registru se složitostí $2^{n/4}$. Tato kolize vytvoří pevný bod v posloupnosti stavů stavového registru. Využíváme 10 těchto pevných bodů a pomocí nich konstruujeme kolidující zprávy, vedoucí k předepsané hašovací hodnotě.

Dosud známé útoky [4, 5] na Blender-n měly složitost nejméně $2^{n/2}$. Náš 2^{2n}-multikolizní a multivzorový útok má složitost pouze $10*2^{n/4}$.

1 Přehledný popis algoritmu Blender-n

Pro jednoduchost se budeme zabývat pouze algoritmem Blender-256. Útoky na ostatní varianty jsou analogické.

Hašovací funkce Blender je iterovaná hašovací funkce. Používá w-bitová slova (w = 32 pro Blender-256, w = 64 pro Blender-512), stavový registr A o osmi w-bitových slovech, dva bity přenosu (carry c1, c2) a hašovací registr H, který má také osm w-bitových slov. Na počátku jsou stavový registr a carry bity vynulovány a počáteční hodnota registru A je nastavena na konstantu $A^0 = (a0^0, a1^0, a2^0, a3^0, a4^0, a5^0, a6^0, a7^0) = H_{init}$. Registr H obsahuje průběžnou hašovací hodnotu, která je definována jako součet (modulo 2^{32} po slovech) slov stavů stavového registru A, tj. $H^t = \sum_{t=1,...,K} A^t$. Nový stav A je funkcí starého stavu a slova zprávy. Takže máme $(A^{t+1}, c1^{t+1}, c2^{t+1}) = f(A^t, c1^t, c2^t, W^t)$, kde f je kompresní funkce a W^t slovo zprávy.

Před hašováním se zpráva zarovná na bajty a doplní na celistvý počet bloků o 16 slovech. Stručně řečeno "doplněk" je tvořen "výplňovými bajty" (filling), které se skládají z prvních 13 bajtů zprávy, eventuálně opakovaných do potřebné délky, dále z délky zprávy v bitech, přičemž tato délka se kóduje binárně a jen do nezbytného počtu bajtů a dále následuje délka délky zprávy (to je jeden bajt, jež obsahuje počet bajtů, v nichž byla zakódována délka zprávy) a poté nakonec dvě slova kontrolního součtu.

Ta jsou vypočítána takto:
checksum1 = non($\sum_{t=1,...,K} W^t$),
checksum2 = $\sum_{t=1,...,K}$ (nonW^t).

Abychom se vyhnuli technickým detailům, uvažujeme pouze zprávy, které mají celočíselný počet slov, stejných 13 prvních bajtů, stejnou délku a dokonce i stejné kontrolní součty. Je důležité poznamenat, že kontrolní součty i aktualizace registru H a registru A jsou počítány pomocí w-bitových slov, zejména pomocí sčítání modulo 2^w.

Zde uvádíme část původního popisu hašování - odstavec 2.6.2, [1]:

Algoritmus Blender-256 používá 32-bitové proměnné a0, ..., a7, H0, ..., H7, dva bity přenosu c1 a c2. To vytváří stav algoritmu od rundy k rundě. Dále se využívají pomocné 32-bitové proměnné T, T1 a T2 a celé číslo r.

Před hašováním jsou proměnné a naplněny hodnotou (H_{init}): a0 = 6a09e667, ...(cut)..., a7 = 5be0cd19. Když je připravena posloupnost 32-bitových slov word W^t , počítá se:

1. hodnoty T1,T2:
[c1,T1] = (a5 ⊕ W^t) + (a1 ⊕ rotl(a3, 8)) + c1
[c2,T2] = (a0 ⊕ rotr(W^t, 8)) + (a4 ⊕ rotr(a2, 8)) + c2

2. rotační faktor:
r = 8 – (c1 + c2)

3. Rotují se T1,T2:
T1 = rotl(T1, r)
T2 = rotr(T2, r)

4. Vypočte se následující stav:
T = rotr(a0, 7)
a0 = a1 ⊕ T2
a1 = a2 ⊕ T1
a2 = a3 ⊕ T2
a3 = a4 ⊕ T1
a4 = a5 ⊕ T2
a5 = a6 ⊕ T1
a6 = a7 ⊕ T2
a7 = T ⊕ T1

5. Aktualizuje se hašovací hodnota:
H0 = H0 + a0
H1 = H1 + a1
H2 = H2 + a2
H3 = H3 + a3
H4 = H4 + a4
H5 = H5 + a5
H6 = H6 + a6
H7 = H7 + a7

Těchto pět kroků definuje jednu rundu algoritmu. Po zpracování všech slov je hašovací hodnota vyčtena z registru H:
H0 || H1 || H2 || H3 || H4 || H5 || H6 || H7.

2 Stavový registr

Hašování má vnitřní stav, který je dán hodnotami (A, c1, c2, H). Nejprve vytvoříme kolize ve stavovém registru A, potom v registru H. Pro jednoduchost budeme hovořit o registru A, i když budeme mít na mysli i stav bitů c1, c2.

Stavový registr má osm slov, ale vhodnou volbou 256 slov zprávy W^t ho přinutíme, aby ve skutečnosti měl pouze 4 měnící se slova po každých 256 krocích. Označme $A^0 = (a0^0, a1^0, a2^0, a3^0, a4^0, a5^0, a6^0, a7^0) = H_{init}$ počáteční stav registru A.

Základní útok

Runda 0:

Z hodnot A^0 vypočítáme první slovo zprávy W^0 tak, že $\mathbf{T2^0 = 0}$. Tomu odpovídá právě jedna volba W^0, což můžeme vidět z rovnice $T2 = (a0 \oplus rotr(W^t, 8)) + (a4 \oplus rotr(a2, 8)) + c2$. Připomeňme, že registr A rotuje svá slova o jednu pozici doleva a v posledním slově navíc rotuje bity o 7 pozic vpravo:

$A^1 = ($ **$a1^0$** $, a2^0 \oplus T1^0,$ **$a3^0$** $, a4^0 \oplus T1^0,$ **$a5^0$** $, a6^0 \oplus T1^0,$ **$a7^0$** $, rotr(a0^0,7) \oplus T1^0)$.

Runda 1:

Podobně jako v rundě 0 nyní volíme slovo zprávy W^1 tak, že $\mathbf{T1^1 = 0}$. Opět máme právě jedinou volbu, což vidíme z rovnice $T1 = (a5 \oplus W^t) + (a1 \oplus rotl(a3, 8)) + c1$.

Dostáváme

$A^2 = (a2^0 \oplus T1^0 \oplus T2^1,$ **$a3^0$** $, a4^0 \oplus T1^0 \oplus T2^1,$ **$a5^0$** $, a6^0 \oplus T1^0 \oplus T2^1,$ **$a7^0$** $, rotr(a0^0,7) \oplus T1^0 \oplus T2^1,$ **$rotr(a1^0,7)$** $)$.

.....atd....

Runda 256:

V předchozích rundách byly proměnné T2 a T1 voleny tak, aby neměly žádný vliv na hodnoty a1, a3, a5, a7. Proto se stavový registr po 256 rundách vrací na lichých pozicích do původního stavu:

$A^{256} = (a0^{256},$ **$a1^0$** $, a2^{256},$ **$a3^0$** $, a4^{256},$ **$a5^0$** $, a6^{256},$ **$a7^0$** $)$.

3 Kolize ve stavovém registru

Pro jednoduchost "vyplňování" uvažujme, že prvních 13 slov zpráv je konstantních. Dále můžeme také přidat libovolné množství w-bitových slov a řekněme, že tak zvolíme prvních 256 slov. Tuto část zprávy nazýváme první stacionární částí (S1).

Nyní začínáme ze stavu, který vznikne po zpracování S1. Použijeme metodu popsanou výše a konstruujeme posloupnost stavů A^{256*1}, A^{256*2}, A^{256*3}, ..., dokud neobdržíme kolizi v této posloupnosti. Tato kolize vytváří pevný bod (nebo též cyklus), protože z tohoto bodu můžeme jít opět na začátek cyklu (a opakovat ho kolikrát chceme) nebo pokračovat dále. Po prvním cyklu uděláme 256 rund s náhodně volenými slovy zprávy W^t (abychom přeťali determinismus). Potom opět pokračujeme metodou výše a vytváříme posloupnost stavů, dokud neobdržíme druhou kolizi ve stavech A registru.

Složitost nalezení každé uvedené kolize narozeninovým paradoxem je pouze $2^{n/4}$ (přesněji $2^{n/4+1}$ včetně bitů carry).

Označme S1 první stacionární část, C1 část mezi prvními kolidujícími body, S2 druhou stacionární část (256 náhodných kroků) a C2 část mezi druhými kolidujícími body.

Poznamenejme, že cyklus C1 (C2) můžeme procházet kolikrát chceme (budeme to využívat k tomu, abychom kontrolní součty a délku zprávy dotlačili do správných hodnot).

4 Příklad kolize s využitím dvou pevných bodů

Zde popíšeme, jak použít pouze dva pevné body ke konstrukci jednoduché kolize (v další kapitole využijeme 10 pevných bodů ke konstrukci mnoha vzorů, tj. i ke kolizi). Nyní definujeme dvě kolidující zprávy M1 a M2.

První zpráva jde přes S1, poté N1 krát přes cyklus C1, jednou přes S2 a jednou přes cyklus C2.

Druhá zpráva jde jednou přes S1, jednou přes cyklus C1, jednou přes S2 a N2 krát přes cyklus C2.

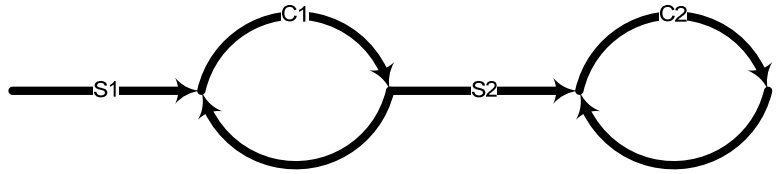
Označme L(S1), L(C1), L(S2), L(C2) počty rund, které odpovídají uvedeným částem S1, C1, S2, C2 posloupnosti stavů. Dále nechť L(M1), L(M2) je celkový počet rund při zpracování zpráv M1 a M2.

Hašovací hodnota je definována jako součet (zvlášť po slovech modulo 2^{32}) odpovídajících stavů A, obdržených při zpracování slov zprávy.

Označme S(S1), S(C1), S(S2) a S(C2) příspěvky A-stavů částí S1, C1, S2, C2 do celkové hašovací sumy. Nechť S(M1), S(M2) je celkový součet stavů, když se zpracuje celá zpráva M1 a M2.

Označme s(S1), s(C1), s(S2) a s(C2) součty slov zprávy v odpovídajících částech stavové posloupnosti.

Definujeme $N1 = 2^w * L(C2) + 1$, $N2 = 2^w * L(C1) + 1$. Potom M1 a M2 budou mít stejnou délku, kontrolní součty a hašovací hodnoty.



Délky

Délky zpráv ve slovech jsou

$L(M1) = L(S1) + Nl*L(C1) + L(S2) + 1*L(C2) = L(S1) + (2^w * L(C2) + 1)*L(C1) + L(S2) + L(C2) = L(S1) + L(C1) + L(S2) + L(C2) + 2^w * L(C2)*L(C1)$,

$L(M2) = L(S1) + 1*L(C1) + L(S2) + N2*L(C2) = L(S1) + L(C1) + L(S2) + (2^w * L(C1) + 1)* L(C2) = L(S1) + L(C1) + L(S2) + L(C2) + 2^w * L(C2)*L(C1)$,

tedy stejné $L = L(M1) = L(M2)$.

Kontrolní součty

Označme K délku zprávy ve slovech a X součet slov zprávy, $X = \sum_{t=1,...,K} W^t$. Potom máme (modulo 2^w)

$checksum1 = non(\sum_{t=1,...,K} W^t) = non\ X = 0xFF...FF - X = 1 - X$,

$checksum2 = \sum_{t=1,...,K} (nonW^t) = \sum_{t=1,...,K} (1 - W^t) = K - \sum_{t=1,...,K} W^t = K - X$.

Když zprávy mají stejné délky L(M1) a L(M2) a stejné součty všech slov X(M), pak také mají stejné checksum1 a checksum2.

Protože součet je počítán modulo 2^w, máme
$X(M1) = s(S1) + Nl*s(C1) + s(S2) + 1*s(C2) = s(S1) + (2^w * L(C2) + 1)*s(C1) + s(S2) + s(C2) = s(S1) + s(C1) + s(S2) + s(C2)$,

$X(M2) = s(S1) + 1*s(C1) + s(S2) + N2*s(C2) = s(S1) + s(C1) + s(S2) + (2^w * L(C1) + 1)*s(C2) = s(S1) + s(C1) + s(S2) + s(C2)$,

takže kontrolní součty zpráv M1 a M2 jsou stejné.

Průběžné hašovací hodnoty
M1 i M2 končí ve stejném posledním stavu - je to poslední stav cyklu C2. Vypočítejme h(M1) a h(M2).

Protože součty jsou počítány ze slov modulo 2^w, máme
$h(M1) = S(S1) + Nl*S(C1) + S(S2) + 1*S(C2) = S(S1) + (2^w * L(C2) + 1)*S(C1) + S(S2) + S(C2) = S(S1) + S(C1) + S(S2) + S(C2)$,

$h(M2) = S(S1) + 1*S(C1) + S(S2) + N2*S(C2) = S(S1) + S(C1) + S(S2) + (2^w * L(C1) + 1)*S(C2) = S(S1) + S(C1) + S(S2) + S(C2)$,

takže i tyto hodnoty jsou stejné.

Hašovací hodnoty
K oběma zprávám můžeme nyní přidat jakýkoliv suffix. Potom dokončíme hašování zpracováním společné části: tj. část "vyplnění", délka, délka délky a kontrolní součty.

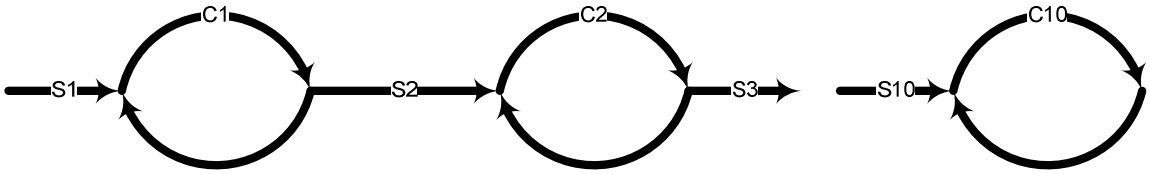
Složitost útoku a paměťové požadavky
Jak jsme viděli výše, všechny požadavky uvedeného útoku na Blender-n jsou řádově pouze $2^{n/4}$.

5 Multivzory

V této části popíšeme jinou metodu, která poskytuje velké množství multivzorů (tj. vytváří také multikolize).
Zvolme libovolnou hašovací hodnotu H. Vytvoříme zprávu M (velké množství zpráv M) tak, že h(M) = H, a to v následujících krocích:

1. Nastav první stacionární část na náhodnou hodnotu větší než 13. Použij proceduru z kapitoly 3 a najdi první kolizní cyklus C1. Následuje náhodná stacionární část S2 (mající malou náhodnou velikost) a druhý kolizní cyklus C2, stacionární část S3 (malá), ..., a končíme s S10 a cyklem C10. Označme A^{fin} finální stav stavového registru.
2. Nechť A^{fin} je finální stav všech uvažovaných zpráv. Poznamenejme, že A^{fin} je stav po zpracování všech slov zprávy (před zpracováním "doplňku").
3. Zvolme L jako bitovou délku zprávy, například kolem hodnoty $w*2^{n/2 + 8+w+\log(10)}$ (tj. $2^{n/2 + 8+w+\log(10)}$ w-bitových slov). Všechny uvažované zprávy budou mít tuto předepsanou délku.

4. Zvolme libovolnou hodnotu X jako budoucí součet všech slov zprávy. Všechny uvažované zprávy budou mít tento součet slov. Všechny zprávy budou mít také stejné "dokončení" (filling, délka, délka délky, kontrolní součty).
5. Nyní známe finální stav A^{fin} a hodnoty "dokončení", proto můžeme všechny tyto hodnoty zpracovat a obdržet hodnotu dH jejich příspěvku do hašovacího registru.
6. Nyní můžeme odstranit tento příspěvek z cílové hašovací hodnoty a příspěvek součtu slov z cílového součtu slov zprávy. Obdržíme "opravené" hodnoty H, L a X. Dále uvažujme, že L je vyjádřena přímo jako počet w-bitových slov zprávy.
7. Úlohou je najít zprávu (zprávy) s počtem slov L, součtem slov X, finálním stavem A^{fin} a hašovací hodnotou H.



Konstrukce multivzorů
Pro každé i = 1, ..., 10 označme

L(Ci) - délku cyklu Ci (ve w-bitových slovech),
s(Ci) - součet slov W^t, odpovídajících cyklu Ci
S(Ci) - součet stavů A^t, odpovídajících cyklu Ci

L(Si) - délku cyklu Si ve slovech,
s(Si) - součet slov W^t, odpovídajících stacionární části Si
S(Si) - součet stavů A^t, odpovídajících stacionární části Si

Vytvoříme velké množství zpráv M tak, že projdeme jednou stacionárními částmi S1, ..., S10 a mnohokrát a různě přes cykly C1, ..., C10. Pouze potřebujeme nastavit počty průchodů tak, aby součty slov, součty stavů a součty dílčích délek byly stejné a rovné předepsaným hodnotám. Pro každé i = 1, ..., 10 označme k_i počet průchodů cyklem Ci.

Potřebujeme řešit soustavu rovnic:

(H): $H = \sum_{i=1,...,10} k_i * S(C_i) \bmod 2^w$
(X): $X = \sum_{i=1,...,10} k_i * s(C_i) \bmod 2^w$
(L): $L = \sum_{i=1,...,10} k_i * L(C_i)$

Poznamenejme, že rovnice (H) je soustava osmi rovnic, protože X a $S(C_i)$ jsou vektory slov, (H) je jedna rovnice a (L) také. Máme 10 rovnic s 10 neznámými k_i. Kdyby (L) byla také modulární (mod 2^w), řešili bychom ji jednoduše Gaussovou eliminační metodou. Ale poslední rovnice obsahuje absolutní hodnoty, takže se jí budeme věnovat více.

Poznámka. Když zvolíme více cyklů (pevných bodů), budeme mít více stupňů volnosti v systému H-X-L (více rovnic než neznámých) a proto obdržíme mnohem více řešení. Přitom složitost příliš nenaroste - z násobícího koeficientu 10 bude 11. Zvýšení počtu cyklů můžeme také použít, pokud obdržený systém rovnic by byl lineárně závislý, a to nahrazením toho cyklu, který lineární závislost způsobuje, cyklem novým.

Řešení systému H-X-L

Označme dolní a horní část proměnné V jako $V^L = V \bmod 2^w$, $V^H = (V - V^L)/2^w = V >> w$. Poznamenejme, že
$S(C_i) = S(C_i)^L$ a $s(C_i) = s(C_i)^L$, zatímco $L(C_i) = L(C_i)^H * 2^w + L(C_i)^L$ a $k_i = k_i^H * 2^w + k_i^L$.

Přepišme H-X-L:
(H): $H = \sum_{i=1,...,10} k_i^L * S(C_i)^L \mod 2^w$
(X): $X = \sum_{i=1,...,10} k_i^L * s(C_i)^L \mod 2^w$
(LL): $L^L = \sum_{i=1,...,10} (k_i^H * 2^w + k_i^L) * (L(C_i)^H * 2^w + L(C_i)^L) \mod 2^w$
(LH): $L^H = (\sum_{i=1,...,10} (k_i^H * 2^w + k_i^L) * (L(C_i)^H * 2^w + L(C_i)^L)) >> w$

Poslední dvě rovnice jsou
(LL): $L^L = \sum_{i=1,...,10} k_i^L * L(C_i)^L \mod 2^w$
(LH): $L^H = (\sum_{i=1,...,10} (k_i^H * 2^w * L(C_i) + k_i^L * L(C_i)^H * 2^w + k_i^L * L(C_i)^L) >> w$
$= c^{1)} + \sum_{i=1,...,10} (k_i^H * L(C_i) + k_i^L * L(C_i)^H)$

Nyní můžeme najít řešení systému H-X-LL 10 lineárních rovnic s 10 neznámými k_i^L (mod 2^w):
(H): $H = \sum_{i=1,...,10} k_i^L * S(C_i)^L \mod 2^w$
(X): $X = \sum_{i=1,...,10} k_i^L * s(C_i)^L \mod 2^w$
(LL): $L^L = \sum_{i=1,...,10} k_i^L * L(C_i)^L \mod 2^w$

Potom nahradíme k_i^L ve zbývající rovnici (LH) a máme

(LH): $L^H = \sum_{i=1,...,10} (k_i^H * L(C_i) + k_i^L * L(C_i)^H) = \sum_{i=1,...,10} (k_i^H * L(C_i)) + CC$
kde CC je konstanta s hodnotou $\sum_{i=1,...,10} k_i^L * L(C_i)^H$.

Zbývá řešit jednu rovnici s 10 neznámými proměnnými k_i^H. Připomeňme, že se jedná o diofantickou rovnici s tím rozdílem, že hledáme její nezáporná řešení. Budeme jí řešit hrubou silou[2)].

Cykly C_i budou obsahovat kolem $2^{n/4}$ bodů. Body jsou stavy po zpracování 256 slov, takže konstanty $L(C_i)$ budou kolem $2^{n/4} * 2^8$ a CC kolem $10 * 2^w * 2^{n/4} * 2^8 \leq 2^{\log(10)+w+n/4+8}$. Hodnota L^H je kolem $2^{n/2+8+w+\log(10)}/2^w = 2^{n/2+8+\log(10)}$, takže hodnota $L^{rest} = L^H - CC$ bude také kolem $2^{n/2+8+\log(10)}$. Máme
(LH): $L^{rest} = \sum_{i=1,...,10} k_i^H * L(C_i)$.
Řekněme, že cyklus C_1 je nejmenší z cyklů. Nyní můžeme nastavit 9 proměnných k_i^H pro i = 2, ..., 10 libovolně a pak vypočítat k_1^H z rovnice (LH). Jestliže výraz $L^{rest} - \sum_{i=2,...,10} k_i^H * L(C_i)$ bude dělitelný $L(C_1)$, dostaneme jedno řešení. To se stane s pravděpodobností $1/L(C_1)$. Protože rozdíl mezi L^{rest} a $L(C_i)$ je ohromný, můžeme očekávat ohromný počet řešení, více než zhruba $((2^{n/2+8+\log(10)}/10) / 2^{n/4} * 2^8)^9 / L(C_1) \geq 2^{2n}$.

[1)] c je přenos z dolní části, může nabývat maximálně 10 hodnot, takže v dalším můžeme uvažovat, že c = 0.

[2)] jistě existují efektivnější metody

Každé řešení reprezentuje cestu z počátečního stavu, přes různý počet průchodů 10 pevnými body a končí v posledním známém jedinečném stavu. Proto všechny tyto zprávy mají stejnou předepsanou hašovací hodnotu.

Složitost nalezení 2^{2n} multivzorů (multikolizí) funkce Blender-n je zhruba 10 krát větší, než nalezení kolize náhodné hašovací funkce, ale s n/2-bitovým výstupem.

6 Závěr

Ukázali jsme 2^{2n}-multikolize a 2^{2n}-multivzory pro Blender-n pro všechny výstupní délky se složitostí zhruba $10*2^{n/4}$.

7 Literatura

[1] Colin Bradbury: BLENDER, A Proposed New Family of Cryptographic Hash Algorithms, http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/Blender.zip

[2] Antoine Joux: Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions, CRYPTO 2004, LNCS, Vol. 3152, pp. 306-316. Springer, 2004

[3] Vlastimil Klima: A near-collision attack on BLENDER, http://cryptography.hyperlink.cz/BMW/near_collision_blender.pdf

[4] Florian Mendel: Preimage Attack on Blender, http://ehash.iaik.tugraz.at/uploads/4/48/Blender-preimage.pdf

[5] Craig Newbold: Observations and Attacks On The SHA-3 Candidate Blender, http://ehash.iaik.tugraz.at/uploads/4/48/Blender-preimage.pdf

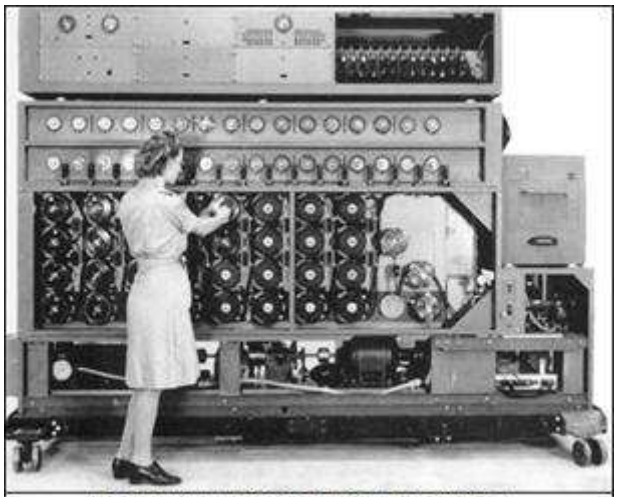
[6] Liangyu Xu: Semi-free start collision attack on Blender, http://ehash.iaik.tugraz.at/uploads/4/48/Blender-preimage.pdf

C. Proč se přestala používat bomba pro luštění Enigmy až v roce 1955?

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

Je všeobecně známo, že v nacistickém Německu byl pro šifrování na nižším stupni velení používán legendární šifrovací stroj *Enigma*. Měl pověst nerozluštitelného a velmi dokonalého šifrovacího stroje. Ve skutečnosti byl luštitelný a díky tomu spojenci získali neocenitelné tajné informace, které podle některých historiků významně ovlivnily průběh celé 2. světové války. O rozluštění jeho šifry se zasloužili především kryptologové Marian Rejewski, Alan Turing a Gordon Welchman.

Princip prolomení tohoto stroje objevil polský matematik Marian Rejewski těsně před počátkem války. Díky opakování klíče na začátku šifrového spojení objevil vztah mezi 1. a 4., 2. a 5. a 3. a 6. písmenem zprávy a na základě těchto vztahů vytvořil katalog typických řetězců pro dané konkrétní nastavení rotorů Enigmy. Nastavení rozvodné desky nemělo vliv na tvar těchto řetězců, a tedy bylo možné řešit problém hledání nastavení rotoru a propojení desky odděleně. Pro urychlení vyhledání správného klíče byl sestrojen stroj zvaný **bomba**, který dokázal prověřovat možná nastavení rotorů a tak najít to, které odpovídalo danému řetězci. Alan Turing během války myšlenku Rejewského zdokonalil a vytvořil vlastní bombu (původně tvořenou několika vzájemně propojenými šifrátory Enigma), která dokázala najít denní klíč pouze pomocí slova, které se ve zprávě nalézalo (tato slova bylo nutné uhodnout). Takto vylepšená elektromechanická bomba umožnila dešifrovat německou komunikaci, i když Němci přestali používat opakování denního klíče.


US NAVY 4 ROTOR BOMBE (NSA)

Koncem roku 1942 bylo v provozu v Bletchley parku 49 bomb. Bomby se též používaly v USA. Obecně se předpokládalo, že po skončení války byly tyto stroje postupně demontovány a přestaly se používat. V některých zdrojích se však objevila zmínka, že část bomb byla po skončení války umístěna na základně Dayton v Ohiu a že zde byly po nějakou dobu ještě používány.

Objevila se také řada méně či více pravděpodobných spekulací, proč tomu tak bylo. Vyjmenujme si některé:

- za druhé světové války bylo získáno velké množství telegramů, ne všechny se podařilo dešifrovat, po válce se NSA dala (z různých důvodů) do práce na dešifraci veškeré zachycené korespondence,
- spekulovalo se o tom, že někteří nacisté, kteří utekli do Jižní Ameriky, měli k dispozici Enigmu a používali ji k šifrovému spojení,
- Enigma se stala válečnou kořistí a státy, které nevěděly, že byla prolomena, ji zařadily mezi své kryptografické prostředky a po nějakou dobu po válce je používaly (mimochodem mezi tyto státy patřila i Česká republika…),

- některé státy třetího světa zakoupily po válce Enigmu a zařadily ji do své výzbroje (tajemství Enigmy nebylo dlouho po válce vyzrazeno a zařízení stále mělo pověst výborného šifrovacího stroje, po německé armádě zbyly stovky zařízení, které se takto mohly vyvézt a je jasné, že jejich vývozu nikdo ze západní zóny nebránil…)

V roce 2007 byl však odtajněn dokument, který alespoň částečně vnesl světlo do celé záležitosti. Dokument odtajnila NSA na základě žádosti 51630 FOIA (Freedom of Information Act) 20. 2. 2007 a byl publikován v Cryptologic Almanac [2].

(TS//SI) At the end of WW II, contrary to what one might believe, the use of Enigma did not cease in a bunker in Berlin in 1945. It lingered on to an insignificant demise in 1955. The East Germans continued to use the Enigmaequipment, but its role diminished, until by the early 1950s they were usingit only in Berlin.

(S//SI) Case notations were used to identify discrete communicationsentities so that one could follow and maintain continuity on a given set of communications. These designators were assigned according to a prescribed system. For instance, in GCPB 00101, the "GC" denoted East German, the "P" indicated Police, and the "B" meant that the mode of communications was Manual Morse. The "001" and "01" signify the number of the network and the net within the network. In this case we have only one net and that was the East

Approved for Release by NSA on
02-20-2007, FOIA Case # 51630

(S//SI) Then one day in 1956 Ellie Carmen Klitzke, chief of the East German cryptanalytic section located in A Building at Arlington Hall Station, notified Preston Welch that the effort on Enigma was to be terminated. Preston was the cryptanalyst in charge of developing "menus" to be run on the bombe. These menus were short passages of text, which he suspected werein the encrypted message. The menus were run on the bombe and, if the guess were correct, the bombe would yield the setting for that message so that it and other messages could be read.

Plyne z něj, že minimálně ještě jedna bomba pracovala během roku 1955. NSA ji používala k luštění policejní komunikace ve východní zóně Německa. Německá policie totiž ještě deset po válce Enigmu (zejména v Berlíně) pro své spojení používala.

Ani tato zpráva však dosud zcela plně nevysvětlila některé detaily. Například:

- Proč NSA používala k luštění Enigmy takovéto zastaralé a relativně pomalé zařízení? Vždyť v padesátých letech již mohla využít luštění na „skutečných“ programovatelných sálových počítačích, které měla k dispozici …

- Proč policie ve východní zóně používala Enigmu? Sověti znali tajemství Enigmy a mohli proto upozornit německou stranu nebo alespoň dát najevo, že použití tohoto zařízení je nevhodné ….

[1] Clin Burke : From the Archives: The Last Bombe Run 1955, Cryptologia, July 2008
[2] Cryptologic Almanach 50th Anniversary Series, FOIA Case 51630, 2-20-2007
[3] Simon Singh: Kniha kódů a šifer, DoKořán 2003

D. Senát schválil nový trestní zákoník

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

V našem e-zinu jsme se v minulých letech přípravě a znění trestního zákoníku již několikráte věnovali. Významnou byla zejména naše aktivita v roce 2005. Tehdy jsme mezi odbornou veřejností a čtenáři Crypto-Worldu uspořádali podpisovou akci, která měla upozornit na nebezpečí, které by vzniklo při schválení návrhu připraveného paragrafového znění trestního zákoníku. Hrozilo, že v případě jeho přijetí by mohl být za trestný čin považován i výzkum v oblasti kryptologie! Kolega Klíma se pak také osobně angažoval při návrhu nového upraveného paragrafového znění tohoto zákona.

Nakonec se nám podařilo za nezastupitelné pomoci vás - čtenářů Crypto-Worldu a organizace IURE prosadit v Parlamentu ČR změnu tehdejšího nevhodně formulovaného § 205 návrhu zákona. Sněmovna zákon přijala, ale Senát jej z politických důvodů zamítl. Sněmovna pak vrácený zákon také zamítla (to už se připravovaly parlamentní volby). Poznamenejme jen, že naše změna byla v Ústavně - právním výboru na právním semináři pochvalována jako příkladná dobře zdůvodněná odborná změna.

Podrobnosti lze najít v e-zinech z té doby Crypto-World 9/2005 a 10/20005.

[1] *Crypto-World 9/2005: Bude kryptoanalýza v Česku trestána vězením? (V. Klíma)*
[2] *Crypto-World 10/2005: Bude kryptoanalýza v Česku trestána vězením? - zřejmě už ne! (V.Klíma) + příloha (Obsahuje: Žádost a podpisy odborníků, Návrh Šámal, Návrh Smejkal, Návrh VK_IURE, překlad části úmluvy, průvodní dopis vk_iure, link psp, stenozáznam jednání PSP, tisk zpráva ČTK)*

V roce 2007 byl připraven a novou vládou navrhován trestní zákoník v novém znění. Po zkušenostech z roku 2005 jsme vydali preventivní výzvu našim čtenářům ke kontrole navrženého paragrafového znění. Zejména jsme se samozřejmě zaměřili na výklad paragrafů, které by mohl opět postavit vědecký výzkum v oblasti kryptografie a informační bezpečnosti do pozice trestní odpovědnosti a znemožňoval jej či jinak omezoval. Shromážděné připomínky byly zaslány na Ministerstvo spravedlnosti České republiky.

[3] *Crypto-World 7/2007 (mimořádné vydání)*
Počítačová kriminalita v návrhu nového trestního zákoníku (2007),
Výzva ke kontrole navrženého paragrafového znění (V. Klíma)

Dlouhé období úprav trestního zákoníku bylo konečně v roce 2008 uzavřeno. Po té co byl zákoník schválen ve Sněmovně, byl podstoupen do Senátu. A zde jej senátoři 8. 1. 2009 také podpořili. Pokud jej podepíše prezident, nahradí zákoník současnou normu ze šedesátých let. Jeho účinnost je stanovena od 1. 1. 2010. Kodex mimo jiné zpřísňuje sankce u násilných trestných činů a naopak snižuje některé maximální sankce za hospodářské delikty. Nový trestní zákoník například rozlišuje trestný čin vraždy a úmyslného zabití, zvyšuje horní hranici trestu za týrání svěřené osoby z 8 na 12 let a zavádí některé nové trestné činy.

Pro zákoník v Senátu hlasovalo 74 ze 76 přítomných.

Text trestního zákoníku lze najít ve sněmovním tisku na adrese http://www.senat.cz/ .

A v jaké podobě byly nakonec schváleny paragrafy, o které jsme v roce 2005 svedli výše popsanou bitvu?

Jedná se o tyto následující paragrafy §§120, 230, 231 a 232 :

§ 120
Uvedení někoho v omyl a využití něčího omylu prostřednictvím technického zařízení

Uvést někoho v omyl či využít něčího omylu lze i provedením zásahu do počítačových informací nebo dat, zásahu do programového vybavení počítače nebo provedením jiné operace na počítači, zásahu do elektronického nebo jiného technického zařízení, včetně zásahu do předmětů sloužících k ovládání takového zařízení, anebo využitím takové operace či takového zásahu provedeného jiným.

§ 230
Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a
a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,
b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,
c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo
d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2
a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo
b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) způsobí-li takovým činem značnou škodu,
c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,
d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo
e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo
b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 231
Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává
a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo
b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,
bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.

(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 232
Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté
a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo
b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,
a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu.

Pro úplnost dále uvádíme výběr některých dalších paragrafů, které přímo či nepřímo upravují problematiku informačních technologií a to konkrétně porušení tajemství přenosu a ukládání zpráv (§§ 182,183) a šíření pornografie včetně nakládání a výroby dětské pornografie (§§ 191,183).

§ 182
Porušení tajemství dopravovaných zpráv

(1) Kdo úmyslně poruší tajemství
a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,
b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo
c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch
a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo
b) takového tajemství využije.

…

(5) Zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, který
a) spáchá čin uvedený v odstavci 1 nebo 2,
b) jinému úmyslně umožní spáchat takový čin, nebo
c) pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem,

bude potrestán odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti.

§ 183
Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

(1) Kdo neoprávněně poruší tajemství listiny nebo jiné písemnosti, fotografie, filmu nebo jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 v úmyslu získat pro sebe nebo pro jiného majetkový nebo jiný prospěch, způsobit jinému škodu nebo jinou vážnou újmu, anebo ohrozit jeho společenskou vážnost.

(3) Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,
b) spáchá-li takový čin vůči jinému pro jeho skutečnou nebo domnělou rasu, příslušnost k etnické skupině, národnost, politické přesvědčení, vyznání nebo proto, že je skutečně nebo domněle bez vyznání,
c) způsobí-li takovým činem značnou škodu, nebo
d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,
a) způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo
b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 191
Šíření pornografie

(1) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, v němž se projevuje násilí či neúcta k člověku, nebo které popisuje, zobrazuje nebo jinak znázorňuje pohlavní styk se zvířetem, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo písemné, fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo
a) nabízí, přenechává nebo zpřístupňuje dítěti, nebo
b) na místě, které je dětem přístupné, vystavuje nebo jinak zpřístupňuje,
bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

§ 192
Výroba a jiné nakládání s dětskou pornografií

(1) Kdo přechovává fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, bude potrestán odnětím svobody až na dva roky.

(2) Kdo vyrobí, doveze, vyveze, proveze, nabídne, činí veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě, anebo
kdo kořistí z takového pornografického díla,
bude potrestán odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na dvě léta až šest let nebo propadnutím majetku bude pachatel potrestán, spáchá-li čin uvedený v odstavci 2
a) jako člen organizované skupiny,
b) tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo
c) v úmyslu získat pro sebe nebo pro jiného značný prospěch.

E. Pozvánka na konferenci Trendy v internetové bezpečnosti

Odborná konference s názvem **Trendy v internetové bezpečnosti**, která má za cíl poukázat na nové výzvy v oblasti bezpečnosti na Internetu, v možnostech odhalení a mapování nových hrozeb i budoucích problémů, proběhne v prostorách Konferenčního centra City v Praze ve čtvrtek **26. února 2009 od 9:00**

Odbornou konferenci pořádají čtyři zpravodajské servery Root.cz, Lupa.cz, Měšec.cz, a Podnikatel.cz . Partnerem odborné konference je Česká spořitelna.

Kdy: 26. února 2009
Kde: Konferenční centrum City (Na strži 1702/65, Praha 4)
Další informace: http://konference.iinfo.cz/

Internetová bezpečnost je v posledních letech tématem číslo jedna. Množí se případy napadení bankovních systémů, odcizení citlivých dat či ohrožení samotných uživatelů. Cílem konference Trendy v internetové bezpečnosti je komplexní shrnutí aktuálních trendů v této oblasti, odhalení a zmapování nových hrozeb i budoucích problémů, se kterými se pravděpodobně instituce i uživatelé setkají.

Na konferenci přednesou své prezentace přední experti z oblasti elektronické bezpečnosti, bankovních služeb a telekomunikací.

Program konference bude rozdělen na dva samostatné bloky

- **Blok 1:** Bezpečnost z hlediska technologie
- **Blok 2:** Bezpečnost z hlediska bankovních služeb

Program je v současné době doplňován a jeho aktuální verze je k dispozici na stránkách konference http://konference.iinfo.cz/program/.

Zájemci o účast na konferenci se mohou registrovat prostřednictvím internetového formuláře na stránce http://konference.iinfo.cz/registrace/.

F. O čem jsme psali v lednu 2000 – 2008

Crypto-World 1/2000

Crypto-World 1/2001

Příloha:
trustcert.pdf (upoutávka na služby Certifikační Autority TrustCert)

Crypto-World 1/2002

Crypto-World 1/2003

Příloha : Crypto_p1.pdf
CEN Workshop Agreements (dokumenty vztahující se k elektronickému podpisu)

Crypto-World 1/2004

Crypto-World 1/2005

Příloha :
Speciál 2004 - přehled článků a prezentací členů redakce Crypto-World za rok 2004
(http://crypto-world.info/casop6/prehled_2004.pdf)

Crypto-World 1/2006

Crypto-World 1/2007

Crypto-World 1/2008

G. 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/