Crypto-World

Informační sešit GCUCMP
ISSN 1801-2140

Ročník 16, číslo 8-9/2014 **15. září**

8-9/2014

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1393 registrovaných odběratelů)

POSLEDNÍ ČÍSLO

Obsah :

Příloha: CFP_MKB2014.pdf http://crypto-world.info/casop16/CFP_MKB2014.pdf

A. Ukončení vydávání e-zinu Crypto-World
Pavel Vondruška

Vážení čtenáři,

před 15ti lety (7.9.1999) vyšlo prvé číslo e-zinu Crypto-World.

Prvé číslo bylo rozesláno 25ti zájemcům. V následujících letech jejich počet rychle rostl. Počet registrovaných čtenářů se postupně rozrostl až na dnešních 1393. Mimochodem všech 25 čtenářů prvého čísla je stále mezi registrovanými odběrateli.

V době vzniku nebylo tolik dostupných zdrojů z oblasti kryptografie jako nyní, a tak si pravděpodobně i díky tomu e-zin získal poměrně rychle své čtenáře.

E-zin vycházel dlouhých třináct let každý měsíc. Pak přešel do režimu dvouměsíčníku. Toto číslo je již 153 v pořadí.

Pro zájemce bylo také uspořádáno 13 originálních soutěží v luštění šifrových úloh.

Po několik let byl také na našem webu Crypto-Worldu provozován vysoce navštěvovaný přehled zajímavostí a novinek ("News").

E-zin byl po celou dobu přísně „nekomerční“ záležitostí a vyhýbal se PR článkům a reklamám.

Jenže to vše jej již historie.

Zvážil jsem své časové a zdravotní možnosti a rozhodl jsem se, že <u>toto číslo bude poslední.</u>

Na přání kolegy z bývalé redakce ještě dodám, že není vyloučeno, že někdy v budoucnu vyjde nějaké mimořádné číslo nebo se vytvoří redakce, která by chtěla navázat na práci, která byla vykonána.

Z tohoto důvodu prozatím ponechávám databázi odběratelů aktivní a nebude automaticky pro rozeslání tohoto čísla smazána.

Pokud tedy chcete, aby byla váš e-mail z databáze vyjmut, zašlete jednoduše e-mail na adresu ezin@crypto-world.info s předmětem rusim odber Crypto-Worldu!
Ke zrušení registrace můžete také použít formulář na http://crypto-world.info/ .
V takovém případě prosím nezapomenout v žádosti uvést e-mailovou adresu, na kterou byla informace ke stažení e-zinu rozesílána!

Děkuji všem čtenářům za zájem a podporu e-zinu a někdy nashledanou!

B. Poděkování autorům

Pavel Vondruška

Všem 115ti autorům, kteří do e-zinu přispěli svým článkem, patří velké poděkování. Na závěr tohoto článku si dovoluji pro připomenutí jejich jmen otisknout kompletní abecední přehled. **Děkuji jim touto cestou za jejich hodnotné příspěvky**, které bez nároku na honorář poskytli pro publikování v našem e-zinu.

Zejména také děkuji svým nejbližším kolegům, kteří dlouhodobě jako členové redakční rady pomáhali nekomerčnímu projektu e-zinu Crypto-World a sami také přispívali řadou článků.

Zvláštní poděkování patří V.Klímovi za jeho téměř „on-line“ přenos ze „zákulisí“ hashovacích funkcí a hledání SHA-3, Jardovi Pinkavovi, který poskytl řadu článků zabývajících se standardy a neúnavně po řadu let provozoval na našem webu Crypto-Worldu vysoce navštěvovaný přehled zajímavostí a novinek ("News").

Poděkování patří mé ženě - Libuši, Jakubovi Vránovi a Dušanu Drábikovi, kteří po řadu let neúnavně pomáhali s jazykovou korekturou přijatých článků.

Poděkování za řadu pěkných článků patří Karlovi Šklíbovi, Petru Tesařovi, Jozef Krajčovičovi, Jozefu M. Kollarovi a Tomaši Rosovi. Poděkování patří i mému synovi Pavlovi, který již od gymnaziálních let spravoval web a připravil prostředí pro řešení a hodnocení soutěžních úloh.

Děkuji vám - bez vás by nebyl e-zin tím, čím byl a nemohl by po tak dlouho dobu existovat!

Abecední přehled všech autorů, kteří přispěli alespoň jednou svým článkem do e-zinu Crypto -World 9/1999 – 9/2014 a kterým tímto děkuji a vzpomínám na spolupráci a perfektní spolupráci:

E.Antal, R.Barczi, P.Barreto, T.Beneš, M.Bond, D.Bosáková, D.Brechlerová, V.Brtník, L.Caha, L.Cechlár, R.Cinkais, D.Cvrček, J.Daemen, V.David, J.Dočkal, D.Doležal, L.Dostálek, M.Drahanský, J.Dušátko, L.Fojtová, M.Forišek, D.Gligoroski, O.Haděrka, J.Hajný, R.Haubert, P.Hellekalek, J.Hobza, M.Hojsík, M.Hlaváč. M.Hornák J.Hrubý, J.B.Hurych, V.J.Jákl, J.Janečko, M.Janošová, P.Javorka, J.Jeřábek, M.Jókay, M.Kákona, M.Kaláb, J.Kadlec, M.Kesely, M.Kolařík, V.Klíma, J.Klimeš, J.Knížek, J.Kobelka, M.Kolařík, J.Kollár, J.Krajčovič, J.Krhovják, P.Komárek, M.Kuchař, P.Kuchař, M.Kumpošt, R.Kümmel, L.Langhammer, Z.Loebl, J.Matejka, P.Matiaško V.Matyáš, I.Mokoš, O.Mikle, J.Mírka, S.J.Murdoch, J.Němejc, O.Nezhyba, A.Olejník, F.Orság, R.Palovský, J.Polák, V.Plátěnka, J.Pinkava, M.Pivoluska, B.Preneel, B.Procházková, J.Prokeš, J.Pulec, I.Pullman, L.Rašek, R.Rexa, V.Rijmen, T.Rosa, P.Rybár, B. Rudolf, J.Růžička, A.Řezníčková, Z.Říha, D.Schmidt, T.Sekera, V.Smejkal, L.Smolík, L.Soukup J.Strelec, J.Souček, L.Stachovcová, V.Sudzina, J.Suchý, O.Suchý, P.Sušil, M.Šedivý, J.Šiška, K.Šklíba, M.Švagerka, P.Švenda, P.Tesař, M.Till, J.Ulehla, A.Uścińska, P.Veselý, P.Vondruška, V.Vondruška, J.Vábek, J.Vorlíček, M.Vozňák, J.Vrána, P.Wallenfels, P.Zajac, I.Zderadička.

C. Příspěvek k luštění šifry Cryptorbit

RNDr. Bohuslav Rudolf, email: b.rudolf@centrum.cz

1. Úvod

V posledním dvojčísle Crypto-Wordu byla v článku RNDr. Vlastimila Klímy a Ing. Martina Kákony popsána šifra Cryptorbit, dále první kroky k jejímu luštění a výzva k hledání elegantnějšího přístupu.

V tomto krátkém textu popisujeme přístup, který sice do značné míry vychází ze zmíněného článku, ale je doveden (jak se alespoň domníváme) až do návodu k praktickému luštění.

Má dvě části. V obou jsou studovány útoky se znalostí otevřeného textu. Předpokládáme při nich, že útočník má pro luštění k dispozici několik jemu známých dvojic (otevřený text, šifrový text) a jeho (naším) cílem je rekonstrukce klíče nebo alespoň dalších otevřených textů.

První část má spíše studijní význam. Je v ní studována zjednodušená verze šifry. Toto zjednodušení spočívá v zanedbání přenosových bitů mezi jednotlivými bajty, které vznikají při sčítání dvou čtyřbajtových slov bajt po bajtu. Luštění se tím zjednodušilo a vedlo k překvapivému výsledku. Tím byla existence tříd ekvivalentních klíčů takto redukované šifry. Luštíme-li takto redukovanou šifru, není nutné rekonstruovat její konkrétní klíč, ale postačí zjistit, do které třídy ekvivalence její klíč patří.

Druhá část využívá zkušenosti získané v první části k luštění původní šifry. V rovnicích, které jsme v první části využili k vyluštění redukované verze šifry, se při přechodu k plné šifře objeví dříve zanedbané přenosové bity. Ty pro danou třídu ekvivalence mírně modifikují proces šifrování. Třídy ekvivalence redukované šifry se v případě plné šifry změní na „třídy klíčů s blízkým účinkem“.

Řešení rovnic odvozených pro plnou šifru, v nichž se již vyskytují přenosové bity, ale nemusí být jednoznačné. V poslední kapitole je vysvětlen mechanismus vzniku takové nejednoznačnosti. Z tvaru rovnic pro vyšší iterace ale usuzujeme na to, že jejich aplikací by se případné nejednoznačnosti vzniklé v počátečních iteracích měly zmírňovat, případně eliminovat.

Autor příspěvku pracoval na těchto výsledcích po kouskách ve chvilkách volného času, a proto prosí o shovívavost, pokud se někde dopustil chyby, nebo pokud se někde odchýlil od přesného schématu šifry.

2. Označení

Označení slov, jejich bajtů a jejich indexů:

- Slova budeme označovat velkými písmeny.
- Každé slovo obsahuje 4 bajty, které budeme označovat malými písmeny.
- Pozici bajtu ve slově budeme vyznačovat horním indexem, takže například: $X = (x^3, x^2, x^1, x^0)$.
- Dolní index si vyhradíme pro označení čísla iterace. Iterace se provádějí při výpočtu bajtů hesla nebo při výpočtu bajtů šifrového textu apod.

Klíč šifry

Klíč šifry obsahuje

- „heslový klíč“ Z dlouhý 1024 bajtů $Z = (z_0, z_1, z_2, \ldots, z_{1023})$
- čtyři 32-bitová slova A, N, B, M pro započtení zpětné vazby, kde: $A = (a^3, a^2, a^1, a^0)$, $N = (n^3, n^2, n^1, n^0)$, $B = (b^3, b^2, b^1, b^0)$, $M = (a^3, a^2, a^1, a^0)$.

Označení otevřeného a šifrového textu

- Symbolem p_j budeme značit j-tý bajt otevřeného textu.
- Symbolem c_j budeme značit j-tý bajt šifrového textu.

Označení slov zajišťujících zpětnou vazbu

- Zpětnou vazbu z šifrového textu zajišťuje řetězec slov $X_0, X_1, X_2, X_3, \ldots$.
- Zpětnou vazbu z otevřeného textu zajišťuje řetězec slov $Y_0, Y_1, Y_2, Y_3, \ldots$.
- Bajty j-tého slova zpětné vazby označujeme takto: $X_j = (x_j^3, x_j^2, x_j^1, x_j^0)$, obdobně: $Y_j = (y_j^3, y_j^2, y_j^1, y_j^0)$,

Vztak k označení v původním článku

- Heslový klíč je v původním článku značen jako N3, jeho j-tý bajt jako N3[j], takže z_j = N3[j].
- Slovo A je v původním článku značeno jako N1.
- Slovo N je v původním článku značeno jako N2.
- Slovo B je v původním článku značeno jako N4.
- Slovo M je v původním článku značeno jako N5.
- J-tý bajt otevřeného textu p_j je v původním článku značen jako PT[j].
- J-tý bajt šifrového textu c_j je v původním článku značen jako CT[j].

3. Šifra Cryptorbit

Základní operace šifry

Šifra používá tyto operace:

- Operace + je sčítání na slovech modulo 2^{32}. Vstupem jsou dvě 32-bitové slova, výstupem je slovo téhož typu.
- Operace ++ je přičtení modulo 256 daného bajtu k nejméně významnému bajtu slova, (přičemž ignorujeme případný přenos do významnějšího bajtu). Vstupem je 32-bitové slovo a bajt, výstupem je slovo téhož typu.
- Operace $\oplus$ je XOR bajtů. Vstupem jsou dva bajty, výstupem je bajt.

Popis šifrování a dešifrování

- Šifruje se 1024 bajtů na začátku souboru a dále podle stejného postupu 1024 bajtů na konci souboru.
- Jde o proudovou šifru s dvojí zpětnou vazbou. Jedna zpětná vazba (označená X) je z šifrového textu, druhá (označená Y) je z otevřeného textu.
- Šifrovací rovnice (se známými x^0_j a y^0_j) má tvar:

$$c_j = p_j \oplus z_j \oplus x^0_j \oplus y^0_j.$$

Rovnice pro iterativní výpočet zpětné vazby z šifrového textu a z otevřeného textu:

$$X_j = (X_{j-1} + N)^{<<<8} ++ (c_{j-1} \oplus x^0_{j-1})$$

$$Y_j = (Y_{j-1} + M)^{<<<8} ++ p_{j-1}.$$

Počáteční podmínky pro výpočet zpětné vazby z šifrového textu a z otevřeného textu:

$$X_{-1} = A, \quad c_{-1} = 0, \quad Y_{-1} = B, \quad p_{-1} = 0,$$

4. Přechod k redukované šifře

Podstata přechodu

- Operaci + mod 2^{32} nahradíme sčítáním navzájem si odpovídajících bajtů.
- Jinými slov: Budeme ignorovat přenosové bity do významnějšího bajtu vzniklé při sčítání slov.
- Značení nové operace ale ponecháme +.

Zjednodušení iterativních rovnic pro výpočet zpětné vazby

Iterativní rovnice pro zpětnou vazbu ze šifrového textu přejdou na tvar:

$$x^3_j = x^2_{j-1} + n^2,$$
$$x^2_j = x^1_{j-1} + n^1,$$
$$x^1_j = x^0_{j-1} + n^0,$$
$$x^0_j = x^3_{j-1} + n^3 + (c_{j-1} \oplus x^0_{j-1}).$$

Iterativní rovnice pro zpětnou vazbu z otevřeného textu přejdou na tvar:

$$y^3_j = y^2_{j-1} + m^2,$$
$$y^2_j = y^1_{j-1} + m^1,$$
$$y^1_j = y^0_{j-1} + m^0,$$
$$y^0_j = y^3_{j-1} + m^3 + p_{j-1}.$$

5. Několik prvních iterací – zpětná vazba z šifrového textu

Inicializace: $x^3_{-1} = a^3, \quad x^2_{-1} = a^2, \quad x^1_{-1} = a^1, \quad x^0_{-1} = a^0.$

Postupným dosazováním do iterativních rovnic zpětné vazby dostaneme rovnice pro jednotlivé iterace. Upřesněme postup zmíněného „postupného dosazování“: Nejprve získáme rovnice nulté iterace dosazením inicializačních vztahů. Potom postupujeme tak, že rovnici pro j-tou iteraci získáme dosazením z rovnic pro předchozí tj. j – 1 iteraci do iterativních rovnic.

Získané rovnice přepíšeme pomocí substituce:

$$\alpha_0 = a^3 + n^3 + a^0.$$
$$\alpha_1 = a^2 + n^2 + n^3$$
$$\alpha_2 = a^1 + n^1 + n^2 + n^3$$
$$\sigma_N = n^3 + n^2 + n^1 + n^0.$$
$$\alpha_3 = a^0 + \sigma_N$$
$$\alpha_4 = \alpha_0 + \sigma_N$$

Na tvar:

$$x^0_0 = \alpha_0$$
$$x^0_1 = \alpha_1 + (c_0 \oplus \alpha_0).$$
$$x^0_2 = \alpha_2 + (c_1 \oplus x^0_1).$$
$$x^0_3 = \alpha_3 + (c_2 \oplus x^0_2).$$
$$x^0_4 = \alpha_4 + (c_3 \oplus x^0_3),$$
$$x^0_5 = x^0_1 + \sigma_N + (c_4 \oplus x^0_4),$$

Obecně pro $j \geq 4$ platí: $x^0_j = x^0_{j-4} + \sigma_N + (c_{j-1} \oplus x^0_{j-1}),$

6. Několik prvních iterací – zpětná vazba z otevřeného textu

Inicializace: $y^3_{-1} = b^3$, $y^2_{-1} = b^2$, $y^1_{-1} = b^1$, $y^0_{-1} = b^0$.

Postupujeme zcela analogicky k předchozímu případu zpětné vazby z šifrového textu. Takže použijeme substituci:

$\beta_0 = b^3 + m^3$.
$\beta_1 = b^2 + m^2 + m^3$.
$\beta_2 = b^1 + m^1 + m^2 + m^3$.
$\sigma_M = m^3 + m^2 + m^1 + m^0$.
$\beta_3 = b^0 + \sigma_M$,
$\beta_4 = \beta_0 + \sigma_M$,

A obdobně jako v předchozím případě dostaneme:

$y^0_0 = \beta_0$
$y^0_1 = \beta_1 + p_0$.
$y^0_2 = \beta_2 + p_1$.
$y^0_3 = \beta_3 + p_2$
$y^0_4 = \beta_4 + p_3$.
$y^0_5 = y^0_1 + \sigma_M + p_4$,

Obecně pro $j \geq 4$ platí: $y^0_j = y^0_{j-4} + \sigma_M + p_{j-1}$,

7. Útok se znalostí otevřeného textu na redukovanou šifru, získání informací o klíči

Předpokládejme, že máme množinu M nám známých několik dvojic
(P, C) = (otevřený text, šifrový text)
odpovídajících témuž klíči Z, A, N, B, M.

- Z této množiny M vyberme nějakou dvojici D = (P, C). Označme M* = M – D.
- Vytvořme množinu $\prod$ = D x M*, tedy množinu párů ((P, C), (P*, C*)), kde (P, C) = D a (P*, C*) $\in$ M*.
- Slova zpětné vazby z šifrového (otevřeného) textu odpovídající první dvojici v páru označíme X (Y) a druhé dvojici v páru označíme X* (Y*).
- V této fázi luštění nás zajímají pouze diference odpovídajících si hodnot uvnitř zvoleného páru, tedy: $\Delta P = P \oplus P^*$ a $\Delta C = C \oplus C^*$.
- Obdobně je definováno: $\Delta X = X \oplus X^*$, $\Delta Y = Y \oplus Y^*$ a $\Delta Z = Z \oplus Z^* = 0$.

Takže aplikací rovnice: $c_j = p_j \oplus z_j \oplus x^0_j \oplus y^0_j$ na vybraný pár (P, C), (P*, C*) dostáváme

$$x^0_j \oplus x^{*0}_j \oplus y^0_j \oplus y^{*0}_j = \Delta r_j,$$

kde: $$\Delta r_j = \Delta c_j \oplus \Delta p_j = p^0_j \oplus p^{*0}_j \oplus c^0_j \oplus c^{*0}_j.$$

V této rovnici pro každý pár z D x M známe hodnotu její pravé strany, kterou jsme označili Δr_j.

Nyní budeme do této rovnice postupně dosazovat. Netriviální výsledky začneme dostávat až od j = 1 výše.

První iterace j = 1

$$(\alpha_1 + (c_0 \oplus \alpha_0)) \oplus (\alpha_1 + (c^*_0 \oplus \alpha_0)) \oplus (\beta_1 + p_0) \oplus (\beta_1 + p^*_0) = \Delta r_1.$$

Tato rovnice pro daný pár obsahuje

- pět známých parametrů: c_0, c^*_0, p_0, p^*_0 a Δr_1
- tři neznámé parametry: α_0, α_1 a β_1.

K tomu dodejme, že:

- Takových párů s různými hodnotami známých parametrů: c_0, c^*_0, p_0, p^*_0 a Δr_1 můžeme získat několik.
- Podstatné je, že hodnoty neznámých parametrů α_0, α_1 a β_1 jsou pro všechny páry stejné.
- K nalezení hodnot α_0, α_1 a β_1 by nám tedy měly stačit 3 různé páry.

Poznámka: Hodnoty: α_0, α_1 umožňují pro dané c_0 rekonstruovat hodnotu x^0_1.

Druhá, třetí, čtvrtá a pátá iterace

Obdobným postupem získáme pro j = 2 z následující rovnice parametry: α_2 a β_2 (přitom x^0_1 a x^{*0}_1 známe z předchozí iterace). A α_2 a β_2 umožní pro daný pár rekonstruovat x^0_2 a x^{*0}_2):

$$(\alpha_2 + (c_1 \oplus x^0_1)) \oplus (\alpha_2 + (c^*_1 \oplus x^{*0}_1)) \oplus (\beta_2 + p_1) \oplus (\beta_2 + p^*_1) = \Delta r_2.$$

Z další rovnice pro j = 3 získáme α_3 a β_3.

$$(\alpha_3 + (c_2 \oplus x^0_2)) \oplus (\alpha_3 + (c^*_2 \oplus x^{*0}_2)) \oplus (\beta_3 + p_2) \oplus (\beta_3 + p^*_2) = \Delta r_3.$$

Z rovnice pro j = 4 určíme: $\alpha_4 = \alpha_0 + \sigma_N$, $\beta_4 = \beta_0 + \sigma_M$.

$$(\alpha_4 + (c_3 \oplus x^0_3)) \oplus (\alpha_4 + (c^*_3 \oplus x^{*0}_3)) \oplus (\beta_4 + p_3) \oplus (\beta_4 + p^*_3) = \Delta r_4.$$

Rovnice pro j = 5 má tvar:

$$(x^0_1 + \sigma_N + (c_4 \oplus x^0_4)) \oplus (x^{*0}_1 + \sigma_N + (c^*_4 \oplus x^{*0}_4)) \oplus$$
$$\oplus (y^0_1 + \sigma_M + p_4) \oplus (y^{*0}_1 + \sigma_M + p^*_4) = \Delta r_5.$$

Hodnoty α_0, α_1 umožňují pro daná c_0, c^*_0 rekonstruovat hodnoty x^0_1, x^{*0}_1 a hodnota β_1 umožňuje pro daná p_0, p^*_0 rekonstruovat hodnoty y^0_1, y^{*0}_1. Díky tomu získáme hodnotu σ_M.

Takže nyní známe α_0, α_1, α_2, α_3, $\sigma_N = \alpha_4 - \alpha_0$, β_1, β_2, β_3, β_4, σ_M, $\beta_0 = \beta_4 - \sigma_M$, a ty nám stačí k rekonstrukci zpětné vazby pro libovolný známý šifrový text a známý klíč Z.

8. Dokončení útoku a ekvivalentní klíče redukované šifry

Rekonstrukce heslové části klíče Z

Předpokládejme, že pomocí postupu popsaného v předchozí kapitole jsme nalezli hodnoty parametrů:

$$\alpha_0, \alpha_1, \alpha_2, \alpha_3, \beta_0, \beta_1, \beta_2, \beta_3, \sigma_N, \sigma_M.$$

Z nich a z rovnic zpětné vazby:

$x^0_0 = \alpha_0$,	$y^0_0 = \beta_0$,
$x^0_1 = \alpha_1 + (c_0 \oplus \alpha_0)$,	$y^0_1 = \beta_1 + p_0$.
$x^0_2 = \alpha_2 + (c_1 \oplus x^0_1)$,	$y^0_2 = \beta_2 + p_1$.
$x^0_3 = \alpha_3 + (c_2 \oplus x^0_2)$,	$y^0_3 = \beta_3 + p_2$
$x^0_4 = \alpha_0 + \sigma_N + (c_3 \oplus x^0_3)$,	$y^0_4 = \beta_4 + p_3$.

můžeme pro známou dvojici (P, C) rekonstruovat hodnoty:

$$x^0_0, y^0_0, x^0_1, y^0_1, x^0_2, y^0_2, x^0_3, y^0_3, x^0_4, y^0_4.$$

Hodnoty: x^0_j, y^0_j pro $j \geq 5$ pro tuto dvojici (P, C) pak můžeme postupně rekonstruovat na základě znalosti hodnot σ_N, σ_M, x^0_{j-4}, y^0_{j-4}, x^0_{j-1} a rovnic:

$$x^0_j = x^0_{j-4} + \sigma_N + (c_{j-1} \oplus x^0_{j-1}), \qquad y^0_j = y^0_{j-4} + \sigma_M + p_{j-1}.$$

Takto jsme pro tuto dvojici (P, C) dostali celou zpětnou vazbu a můžeme vypočíst bajty z_j klíče Z, a to z rovnice:

$$z_j = p_j \oplus c_j \oplus x^0_j \oplus y^0_j.$$

Rekonstrukce neznámého otevřeného textu

Nabízí se iterativní postup na základě rovnice: $p_j = z_j \oplus c_j \oplus x^0_j \oplus y^0_j$, znalosti hodnot parametrů: α_0, α_1, α_2, α_3, β_0, β_1, β_2, β_3, σ_N, σ_M a výše uvedených rovnic zpětné vazby.

V j-té iteraci nejprve využijeme hodnoty p_{j-1}, x_{j-1}, případně x_{j-4}, y_{j-4} vypočtené v předchozích krocích pro výpočet hodnot x_j, y_j, a ty pak dosadíme do rovnice pro výpočet p_j.

Ekvivalentní klíče

Jak jsme viděli, v případě redukované šifry k rekonstrukci otevřeného textu postačí znalost Z a 10 bajtů: α_0, α_1, α_2, α_3, β_0, β_1, β_2, β_3, σ_N, σ_M omezujících tvar zpětné vazby. Klíč A, N, B, M sloužící pro výpočet zpětné vazby ale má 16 bajtů. To znamená, že v průměru ke každému klíči existuje $2^{6x8} = 2^{48}$ s ním ekvivalentních klíčů redukované šifry.

9. Přechod k původní šifře

Vyjádření vstupů do výpočtu přenosových bitů mezi bajty na sousedních pozicích

Výpočet přenosového bitu do bajtu na j-té pozici má 3 vstupy: dva z nich jsou sčítané bajty na j – 1 pozici a třetí je přenosový bit ze sčítání dvojice bajtů na pozici j – 2 do pozice j – 1. Správně bychom měli zavést funkci S(•, •, •) na dvojici bajtů x, y a bitu s definovanou vztahem:

$$S(x, y, s) = \lfloor (x + y + s) / 256 \rfloor.$$

Místo toho zavedeme dvouhodnotovou relaci S(•, •) pouze na dvojici bajtů x, y definovanou vztahem:

$$S(x, y) = \lfloor (x + y + s) / 256 \rfloor,$$

kde $s \in \{0; 1\}$, takže S(x, y) pro danou hodnotu bajtů x a y nabývá 1 nebo 2 hodnot. Pro nás bude podstatné, že rovněž :

$$S(x, y) \in \{0; 1\}.$$

10. Rovnice pro výpočet zpětné vazby původní šifry

Iterativní rovnice pro zpětnou vazbu ze šifrového textu přejdou na tvar:

$$x^3_j = x^2_{j-1} + n^2 + S(x^1_{j-1}, n^1)$$
$$x^2_j = x^1_{j-1} + n^1 + S(x^0_{j-1}, n^0)$$
$$x^1_j = x^0_{j-1} + n^0,$$
$$x^0_j = x^3_{j-1} + n^3 + S(x^2_{j-1}, n^2) + (c_{j-1} \oplus x^0_{j-1}).$$

Iterativní rovnice pro zpětnou vazbu z otevřeného textu přejdou na tvar:

$$y^3_j = y^2_{j-1} + m^2 + S(y^1_{j-1}, m^1),$$
$$y^2_j = y^1_{j-1} + m^1 + S(y^0_{j-1}, m^0),$$
$$y^1_j = y^0_{j-1} + m^0,$$
$$y^0_j = y^3_{j-1} + m^3 + S(y^2_{j-1}, m^2) + p_{j-1}.$$

11. Několik prvních iterací – zpětná vazba z šifrového textu

Připomeňme, jak vypadá inicializace:

$$x^3_{-1} = a^3, \quad x^2_{-1} = a^2, \quad x^1_{-1} = a^1, \quad x^0_{-1} = a^0, \quad c_{-1} = 0$$

Dosazením do výše uvedených iterativních rovnic dostáváme, jak vypadá nultá iterace:

$$x^3_0 = a^2 + n^2 + S(a^1, n^1)$$
$$x^2_0 = a^1 + n^1 + S(a^0, n^0)$$
$$x^1_0 = a^0 + n^0,$$
$$x^0_0 = a^3 + a^0 + n^3 + S(a^2, n^2).$$

Postupným dosazováním (z rovnic nulté iterace do rovnic první iterace, pak z první do druhé, atd.) dostaneme rovnice pro jednotlivé iterace, z nichž nás zajímají pouze tyto:

$$x^0_0 = a^3 + a^0 + n^3 + S(a^2, n^2).$$
$$x^0_1 = a^2 + n^2 + n^3 + (c_0 \oplus x^0_0) + S(a^1, n^1) + S(x^2_0, n^2).$$
$$x^0_2 = a^1 + n^1 + n^2 + n^3 + (c_1 \oplus x^0_1) + S(a^0, n^0) + S(x^1_0, n^1) + S(x^2_1, n^2).$$
$$x^0_3 = a^0 + \sigma_N + (c_2 \oplus x^0_2) + S(x^0_0, n^0) + S(x^1_1, n^1) + S(x^2_2, n^2).$$
$$x^0_4 = x^0_0 + \sigma_N + (c_3 \oplus x^0_3) + S(x^0_1, n^0) + S(x^1_2, n^1) + S(x^2_3, n^2)$$

Obecně pro $j \geq 4$:

$$x^0_j = x^0_{j-4} + \sigma_N + (c_{j-1} \oplus x^0_{j-1}) + S(x^0_{j-3}, n^0) + S(x^1_{j-2}, n^1) + S(x^2_{j-1}, n^2)$$

Na základě zkušenosti s redukovanou šifrou značme:

$\alpha_0 = a^3 + a^0 + n^3.$
$\alpha_1 = a^2 + n^2 + n^3$
$\alpha_2 = a^1 + n^1 + n^2 + n^3$
$\alpha_3 = a^0 + \sigma_N.$

$s^x_0 = S(a^2, n^2),$ $s^x_0 \in \{0, 1\}$
$s^x_1 = S(a^1, n^1) + S(x^2_0, n^2),$ $s^x_1 \in \{0, 1, 2\}$
$s^x_2 = S(a^0, n^0) + S(x^1_0, n^1) + S(x^2_1, n^2),$ $s^x_2 \in \{0, 1, 2, 3\}$
$s^x_3 = S(x^0_0, n^0) + S(x^1_1, n^1) + S(x^2_2, n^2),$ $s^x_3 \in \{0, 1, 2, 3\}$
$s^x_4 = S(x^0_1, n^0) + S(x^1_2, n^1) + S(x^2_3, n^2)$ $s^x_3 \in \{0, 1, 2, 3\}$
$s^x_j = S(x^0_{j-3}, n^0) + S(x^1_{j-2}, n^1) + S(x^2_{j-1}, n^2)$ $s^x_j \in \{0, 1, 2, 3\}$

Poznamenejme, že s^x_j je pro $j \geq 2$ vlastně dvojbitem.

Potom dostaneme:

Výchozí X-rovnice pro luštění

$x^0_0 = \alpha_0 + s^x_0,$ $s^x_0 \in \{0, 1\}$
$x^0_1 = \alpha_1 + (c_0 \oplus x^0_0) + s^x_1,$ $s^x_1 \in \{0, 1, 2\}$
$x^0_2 = \alpha_2 + (c_1 \oplus x^0_1) + s^x_2,$ $s^x_2 \in \{0, 1, 2, 3\}$
$x^0_3 = \alpha_3 + (c_2 \oplus x^0_2) + s^x_3,$ $s^x_3 \in \{0, 1, 2, 3\}$
$x^0_4 = \alpha_4 + (c_3 \oplus x^0_3) + s^x_4,$ $s^x_4 \in \{0, 1, 2, 3\}$
$x^0_j = x^0_{j-4} + \sigma_N + (c_{j-1} \oplus x^0_{j-1}) + s^x_j,$ $s^x_j \in \{0, 1, 2, 3\}$
kde: $\alpha_4 = x^0_0 + \sigma_N.$

12. Několik prvních iterací – zpětná vazba z otevřeného textu

Budeme postupovat obdobně jako v předchozím případě zpětné vazby z šifrového textu. Připomeňme nejprve, jak vypadá inicializace:

$$y^3_{-1} = b^3, \quad y^2_{-1} = b^2, \quad y^1_{-1} = b^1, \quad y^0_{-1} = b^0.$$

Dosazením do výše uvedených iterativních rovnic dostáváme, jak vypadá nultá iterace:

$y^3_0 = b^2 + m^2 + S(b^1, m^1),$
$y^2_0 = b^1 + m^1 + S(b^0, m^0),$
$y^1_0 = b^0 + m^0,$
$y^0_0 = b^3 + m^3 + S(b^2, m^2).$

Obdobně pak postupným dosazováním dostaneme rovnice pro jednotlivé iterace, z nichž nás zajímají pouze:

$y^0_0 = b^3 + m^3 + S(b^2, m^2)$.
$y^0_1 = b^2 + m^2 + m^3 + p_0 + S(b^1, m^1) + S(y^2_0, m^2)$.
$y^0_2 = b^1 + m^1 + m^2 + m^3 + p_1 + S(b^0, m^0) + S(y^1_0, m^1) + S(y^2_1, m^2)$.
$y^0_3 = b^0 + \sigma_M + p_2 + S(y^0_0, m^0) + S(y^1_1, m^1) + S(y^2_2, m^2)$.
$y^0_4 = y^0_0 + \sigma_M + p_3 + S(y^0_1, m^0) + S(y^1_2, m^1) + S(y^2_3, m^2)$.

Obecně pro $j \geq 4$ platí::
$y^0_j = y^0_{j-4} + \sigma_M + p_{j-1} + S(y^0_{j-3}, m^0) + S(y^1_{j-2}, m^1) + S(y^2_{j-1}, m^2)$.

Označme:
$\beta_0 = b^3 + m^3$, $\beta_1 = b^2 + m^2 + m^3$,
$\beta_2 = b^1 + m^1 + m^2 + m^3$,
$\beta_3 = b^0 + \sigma_M$,
$\beta_4 = \sigma_M$,

$S(b^2, m^2) = s^y_0$,	$s^y_0 \in \{0, 1\}$
$S(b^1, m^1) + S(y^2_0, m^2) = s^y_1$,	$s^y_1 \in \{0, 1, 2\}$
$S(b^0, m^0) + S(y^1_0, m^1) + S(y^2_1, m^2) = s^y_2$,	$s^y_2 \in \{0, 1, 2, 3\}$
$S(y^0_0, m^0) + S(y^1_1, m^1) + S(y^2_2, m^2) = s^y_3$,	$s^y_3 \in \{0, 1, 2, 3\}$
$S(y^0_1, m^0) + S(y^1_2, m^1) + S(y^2_3, m^2) = s^y_4$,	$s^y_4 \in \{0, 1, 2, 3\}$
$S(y^0_{j-3}, m^0) + S(y^1_{j-2}, m^1) + S(y^2_{j-1}, m^2) = s^y_j$,	$s^y_j \in \{0, 1, 2, 3\}$

Potom dostáváme:

Výchozí Y-rovnice pro luštění

$y^0_0 = \beta_0 + s^y_0$,	$s^y_0 \in \{0, 1\}$
$y^0_1 = \beta_1 + p_0 + s^y_1$,	$s^y_1 \in \{0, 1, 2\}$
$y^0_2 = \beta_2 + p_1 + s^y_2$,	$s^y_2 \in \{0, 1, 2, 3\}$
$y^0_3 = \beta_3 + p_2 + s^y_3$,	$s^y_3 \in \{0, 1, 2, 3\}$
$y^0_4 = \beta_4 + p_3 + s^y_4$,	$s^y_4 \in \{0, 1, 2, 3\}$
$y^0_j = y^0_{j-4} + \sigma_M + p_{j-1} + s^y_j$,	$s^y_j \in \{0, 1, 2, 3\}$

kde: $\beta_4 = y^0_0 + \sigma_M$

13. **Útok se znalostí otevřeného textu na původní šifru**,

Rekonstrukce zpětné vazby

Pro jednotlivé iterace budeme postupovat obdobně jako v případě ignorovaných přenosových bitů mezi bajty. Kromě započtení přenosových bitů zachováváme označení, takže aplikací rovnice: $c_j = p_j \oplus z_j \oplus x^0_j \oplus y^0_j$ na vybraný pár dostáváme

$$x^0_j \oplus x^{*0}_j \oplus y^0_j \oplus y^{*0}_j = \Delta r_j,$$

kde: $$\Delta r_j = \Delta c_j \oplus \Delta p_j = p^0_j \oplus p^{*0}_j \oplus c^0_j \oplus c^{*0}_j.$$

Hlavním rozdílem proti předchozímu postupu bude to, že nyní vycházíme ze soustav rovnic uvedených v rámečcích a obsahujících přenosové (dvoj)bity.

První iterace

V tomto případě

$$x^0_1 = \alpha_1 + (c_0 \oplus x^0_0) + s^x_1, \qquad s^x_1 \in \{0, 1, 2\}$$

$$y^0_1 = \beta_1 + p_0 + s^y_1, \qquad s^y_1 \in \{0, 1, 2\}$$

$$s^x_1 = S(a^1, n^1) + S(x^2_0, n^2), \qquad s^y_1 = S(b^1, m^1) + S(y^2_0, m^2).$$

Z toho, že x^2_0, y^2_0 nezávisejí ani na otevřeném ani na šifrovém textu, dostáváme, že na nich nezávisejí ani s^x_1, s^y_1.

Takže:

$$(\alpha_1 + s^x_1 + (c_0 \oplus x^0_0)) \oplus (\alpha_1 + s^x_1 + (c^*_0 \oplus x^0_0)) \oplus$$

$$\oplus (\beta_1 + s^y_1 + p_0) \oplus (\beta_1 + s^y_1 + p^*_0) = \Delta r_1.$$

Označme: $$\alpha^s_1 = \alpha_1 + s^x_1, \qquad \beta^s_1 = \beta_1 + s^y_1$$

Pak dostáváme:

$$(\alpha^s_1 + (c_0 \oplus x^0_0)) \oplus (\alpha^s_1 + (c^*_0 \oplus x^0_0)) \oplus (\beta^s_1 + p_0) \oplus (\beta^s_1 + p^*_0) = \Delta r_1.$$

Tato rovnice pro daný pár obsahuje

- pět známých parametrů: c_0, c^*_0, p_0, p^*_0 a Δr_1
- tři neznámé parametry: x^0_0, α^s_1 a β^s_1.

K tomu dodejme, že:

- Takových párů s různými hodnotami známých parametrů: c_0, c^*_0, p_0, p^*_0 a Δr_1 můžeme získat několik.
- Podstatné je, že hodnoty neznámých parametrů x^0_0, α^s_1 a β^s_1 jsou pro všechny páry stejné.
- K nalezení hodnot x^0_0, α^s_1 a β^s_1 by nám tedy měly stačit 3 různé páry.

Poznámky:

- Hodnoty: x^0_0, α^s_1 umožňují pro dané c_0 rekonstruovat hodnotu x^0_1.
- Hodnota: β^s_1 umožňuje pro dané p_0 rekonstruovat hodnotu y^0_1.
- Pro známé: x^0_1, y^0_1 lze pro dané p_0 a c_0 rekonstruovat hodnotu z_1.

Ukázka postupu pro další iterace na příkladu druhé iterace

V tomto případě

$$x^0_2 = \alpha_2 + (c_1 \oplus x^0_1) + s^x_2, \qquad s^x_2 \in \{0, 1, 2, 3\}$$

$$y^0_2 = \beta_2 + p_1 + s^y_2, \qquad s^y_2 \in \{0, 1, 2, 3\}$$

Dostáváme:

$$(\alpha_2 + (c_1 \oplus x^0_1) + s^x_2) \oplus (\alpha_2 + (c^*_1 \oplus x^{*0}_1) + s^{*x}_2) \oplus$$

$$\oplus (\beta_2 + p_1 + s^y_2) \oplus (\beta_2 + p^*_1 + s^{*y}_2) = \Delta r_2.$$

Páry (souborů) budeme vybírat tak, že první soubor páru zafixujeme a budeme měnit pouze druhý soubor v páru (získáme množinu D x M*). Pro takové páry budeme postupovat následovně:

Soubor rovnic pro takových N párů obsahuje

- Tři známé parametry: c_1, p_1, x^0_1 prvního souboru v párech.
- 4N známých parametrů: c^*_1, p^*_1, x^{*0}_1 a Δr_2.
- dva neznámé parametry: α_2, β_2, jejichž hodnoty jsou společné pro všechny páry,
- dva neznámé parametry: s^x_2, s^y_2 prvního souboru v párech.
- 2 N neznámých parametrů: s^{*x}_2, s^{*y}_2, jejichž hodnoty závisejí na druhém souboru v páru.

Další postup:

- To znamená, že máme celkem N bajtových rovnic pro 2 neznámé bajty a 2N + 2 neznámých přenosových dvoj-bitů s. Nejmenší kladné N, pro které platí, že $8\ N \geq 16 + 2\ (2N + 2)$, má hodnotu $N \geq 5$. Potřebujeme tedy nejméně pět známých párů, tedy alespoň šest dvojic (P, C).
- Pro N = 5 máme celkem 16 + 2 (10 + 2) = 40 neznámých bitů, které lze snadno určit hrubou silou.
- Tímto způsobem získáme nejen α_2, β_2, ale i parametry: s^x_2, s^y_2 pro všechny soubory v párech.

Poznámky:

- Hodnoty: x^0_1, α^s_2 umožňují pro dané c_1 rekonstruovat hodnotu x^0_2.
- Hodnota: β^s_2 umožňuje pro dané p_1 rekonstruovat hodnotu y^0_2.
- Pro známé: x^0_2, y^0_2 lze pro dané p_0 a c_0 rekonstruovat hodnotu z_2.

Třetí, čtvrtá, pátá a další iterace

V dalších iteracích se postupuje obdobně jako v případě druhé iterace.

Pro třetí iteraci dostáváme rovnici pro luštění:

$$(\alpha_3 + (c_2 \oplus x^0_2) + s^x_3) \oplus (\alpha_3 + (c^*_2 \oplus x^{*0}_2) + s^{*x}_3) \oplus$$

$$\oplus (\beta_3 + p_2 + s^y_3) \oplus (\beta_3 + p^*_2 + s^{*y}_3) = \Delta r_3.$$

Protože pro zvolenou množinu M párů známe: c_2, x^0_2, c^*_2, x^{*0}_2, p_2, c^*_2, Δr_3, můžeme obdobně jako v předchozím případě určit neznámé: α_3, β_3, a přenosové dvojbity s^x_3, s^{*x}_3, s^y_3, s^{*y}_3 pro celou M. Odtud dostáváme x^0_3, x^{*0}_3, y^0_3, y^{*0}_3 pro celou M.

Pro čtvrtou iteraci dostáváme:

$$(\alpha_4 + (c_3 \oplus x^0_3) + s^x_4) \oplus (\alpha_4 + (c^*_3 \oplus x^{*0}_3) + s^{*x}_4) \oplus$$

$$\oplus (\beta_4 + p_3 + s^y_4) \oplus (y^0_0 + \sigma_M + p^*_3 + s^{*y}_4) = \Delta r_4.$$

Z příslušné soustavy rovnic pro množinu M párů dostaneme hodnoty bajtů α_4 a β_4 a přenosových dvojbitů: s^x_4, s^{*x}_4, s^y_4 a s^{*y}_4. Protože platí: $\alpha_4 = x^0_0 + \sigma_N$, $\beta_4 = y^0_0 + \sigma_M$, a vzhledem ke tvaru dalších iterací, můžeme v budoucnu využít tuto rovnici k určení y^0_0 a σ_N, případně ke kontrole: x^0_0. Ze znalosti α_4, β_4 a přenosových dvojbitů s^x_4, s^{*x}_4, s^y_4 a s^{*y}_4 na množině M určíme hodnoty x^0_4, x^{*0}_4, y^0_4, y^{*0}_4 na M.

Rovnice pro pátou iteraci mají tvar:

$$(x^0_1 + \sigma_N + (c_4 \oplus x^0_4) + s^x_5) \oplus (x^{*0}_1 + \sigma_N + (c^*_4 \oplus x^{*0}_4) + s^{*x}_5) \oplus$$

$$\oplus (y^0_1 + \sigma_M + p_4 + s^y_5) \oplus (y^{*0}_1 + \sigma_M + p^*_4 + s^{*y}_5) = \Delta r_5.$$

Pro jednotlivé páry v množině D x M* známe x^0_1, σ_N, c_4, x^0_4, x^{*0}_1, c^*_4, x^{*0}_4, y^0_1, p_4, y^{*0}_1, p^*_4 a Δr_5 a zbývá nám pouze určit σ_M a přenosové dvojbity: s^x_5, s^{*x}_5, s^y_5, s^{*y}_5 na množině D x M*. Odtud snadno určíme hodnoty x^0_5, x^{*0}_5, y^0_5, y^{*0}_5.

Další iterace - v případě obecné iterace ($j \geq 6$) dostáváme:

$$(x^0_{j-4} + \sigma_N + (c_{j-1} \oplus x^0_{j-1}) + s^x_j) \oplus (x^{*0}_{j-4} + \sigma_N + (c^*_{j-1} \oplus x^{*0}_{j-1}) + s^{*x}_j) \oplus$$

$$\oplus (y^0_{j-4} + \sigma_M + p_{j-1} + s^y_j) \oplus (y^{*0}_{j-4} + \sigma_M + p^*_{j-1} + s^{*y}_j) = \Delta r_j.$$

V této rovnici již známe:

$$x^0_{j-4}, \sigma_N, c_{j-1}, x^0_{j-1}, x^{*0}_{j-4}, \sigma_N, c^*_{j-1}, x^{*0}_{j-1}, y^0_{j-4}, p_{j-1}, y^{0*}_{j-4}, \sigma_M, p^*_{j-1}, \Delta r_j.$$

Zbývá vypočíst: s^x_j, s^{*x}_j, s^y_j, s^{*y}_j pro jednotlivé soubory množiny M.

Problém nejednoznačnosti řešení

Nejednoznačnost řešení získaného tímto způsobem: Problém je, že ve skutečnosti nemusíme tímto postupem dospět k jedinému možnému řešení. Vysvětleme to na příkladě rovnice pro třetí iteraci. Pokud pro všechny dvojice (P, C) množiny M* platí: $s^{*x}_3 = s^x_3$, pak sice tuto skutečnost řešením uvažované soustavy rovnic na D x M zjistíme, ale konkrétní hodnotu s^x_3 z ní již neurčíme. V dalších iteracích pak budeme muset uvažovat všechny možné hodnoty s^x_3 a jim odpovídající hodnoty x^0_3.

Snižování nejednoznačnosti řešení v dalších iteracích
Podívejme se na tvar rovnic od 6 iterace dále. V nich se již jako neznámé vyskytují pouze hodnoty přenosových dvojbitů, protože hodnoty σ_N a σ_M v nich považujeme za známé. To znamená, že v těchto rovnicích se výše popsaný mechanismus generování nejednoznačnosti řešení již neuplatní. A, pokud se v nich nevyskytuje jiný mechanismus generování nejednoznačnosti řešení (který jsme přehlédli), pak by řešení rovnic pro další iterace mohlo vést k omezení, případně i k eliminaci, nejednoznačnosti z prvních 5 iterací.

Rekonstrukce hesla Z a neznámých otevřených textů

Rekonstrukce hesla Z:
Výše popsaným způsobem můžeme (zatím nevíme, jak jednoznačně) na nějaké množině D x M párů známých dvojic postupně reprodukovat hodnoty x^0_j, y^0_j (či spíše x^{*0}_j, y^{*0}_j) pro všechna j jdoucí od 0 do 1023. Jejich dosazením do šifrovací rovnice ve tvaru: $z_j = p_j \oplus c_j \oplus x^0_j \oplus y^0_j$ dostaneme heslo Z.

Rekonstrukce neznámého otevřeného textu

Předpokládejme, že jsme v předchozí fázi luštění získali jednoznačné hodnoty parametrů: α_0, α_1, α_2, α_3, σ_N, β_0, β_1, β_2, β_3, σ_M a „hesla“ Z. To znamená, že pro neznámý otevřený text známe hodnoty zpětné vazby s přesností zhruba až na nejméně významné dvoj-bity každého bajtu a s obdobnou přesností známe i bajty otevřeného textu. Otázkou je, jak určit nejméně významné dvojbity bajtů zpětné vazby a otevřeného textu.

Za nejschůdnější považujeme návrat ke standardnímu postupu spočívající v tom, že z množiny jednoznačně určených přenosových dvoj-bitů pro dvojice (P, C) množiny M určíme zbývající bajty klíče šifry hrubou silou. K urychlení výpočtu doporučujeme nejdříve pro nejnižší 3 iterace otestovat, zda v nich se vyskytující přenosové bity na některých hledaných bajtech klíče nezávisejí. Potom lze v těchto iteracích upřesnit hodnoty pouze zbylé části hledaných bitů klíče a výpočet hrubou silou přes tyto iterace by se zkrátil. Získané výsledky by pak posloužili ke zkrácení výpočtů pro další iterace.

D. Call for Papers
Mikulášská kryptobesídka

27. – 28. listopad 2014, Praha
http://mkb.tns.cz

Základní informace

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

Workshop se skládá ze (a) dne prezentací příspěvků, diskusí a neformálního setkání ve čtvrtek *27. listopadu* a (b) půldne prezentací příspěvků a diskusí v pátek *28. listopadu 2014*. Pro workshop jsou domluveny zvané příspěvky od:

- Joachim Posegga: Alice in the Cloud: Insights on Security of Air Traffic Control Communication.
- Gregor Leander: Lightweight Cryptography.
- Karthik Bhargavan: Breaking and Fixing the TLS Cryptographic Protocol.
- Karsten Nohl: Bude potvrzeno koncem srpna.
- Peter Gazi: Key-Length Extension for Block Ciphers: Plain and Randomized Cascades.

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

Pokyny pro autory

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

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

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a tak, aby přišly nejpozději do *30. září 2014*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2014 – navrh prispevku“. Příjem návrhů bude potvrzován do dvou pracovních dnů od přijetí.

Návrhy příspěvků budou posouzeny PV a autoři budou informováni o přijetí/odmítnutí do *30. října*. Příspěvek pro sborník workshopu pak musí být dodán do *11. listopadu*.

Důležité termíny

Návrhy příspěvků:	30. září 2014
Oznámení o přijetí/odmítnutí:	30. října 2014
Příspěvky pro sborník:	11. listopadu 2014
Konání MKB 2014:	27. – 28. listopadu 2014

Programový výbor

Michal Hojsík, Honeywell a MFF UK, Praha, CZ
Marek Kumpošt, NetSuite & FI MU, Brno, CZ
Vašek Matyáš, FI MU, Brno, CZ – předseda
Tomáš Rosa, Raiffeisenbank a UK, CZ
Luděk Smolík, Siegen, DE
Martin Stanek, UK, Bratislava, SK
Pavol Zajac, STU, Bratislava, SK

Mediální partneři

E. Pozvánka ke kurzu PKI (+eIDAS) Akademie CZ.NIC

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

Lektory Akademie CZ.NIC jsou jak zaměstnanci sdružení, tak odborníci z praxe.

Problematika infrastruktury veřejných klíčů (PKI) ,

Kurz získal akreditaci Ministerstva vnitra České republiky č. AK/PV-856/2013 podle ustanovení § 31 odst. 5 zákona č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů.

Kurz seznámí účastníky s principy fungování PKI z různých aspektů. Účastník se seznámí se základními principy asymetrických šifer, s definicemi a požadavky zákona o elektronickém podpisu, bude seznámen s technickým a legislativním pohledem na důvěru v certifikáty a ověření podpisu a certifikátu. **Nově je zařazena informace o** nařízení Evropského parlamentu a Rady o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu - **eIDAS**. Součástí budou některé jednoduché praktické dovednosti – zejména práce s certifikáty (generování, export, import, podpis, ověření) a práce s CRL.

Jak se přihlásit

Pro přihlášení do kurzu stačí pouze vyplnit přihlašovací formulář a uhradit kurz. Pokud máte zájem o kurz, který není aktuálně vypsán, napište nám e-mail na akademie@nic.cz a budeme vás informovat o nejbližším termínu konání vybraného kurzu.

Místo konání kurzů

Akademie CZ.NIC

05.06.2014	9:00–17:00	**Brno**
05.06.2014	9:00–17:00	**Brno**
11.12.2014	9:00–17:00	**Praha**

http://www.nic.cz/akademie/contact/

Možnosti slevy

Studenti mají možnost, na základě vložení kopie dokladu o studiu do přihlašovacího formuláře, **získat slevu 90 %** z dané částky kurzu.

F. O čem jsme psali v předchozích 152 číslech…

Kompletní obsah všech **152** vyšlých čísel od září roku 1999 je dostupný na našm webu http://crypto-world.info/index2.php?vyber=obsah

Soubor lze stáhnout z této adresy: http://crypto-world.info/obsah/obsah_roky.pdf

G. Závěrečné informace

1. Sešit

Crypto-World **byl** oficiální informační sešit "***Kryptologické sekce Jednoty českých matematiků a fyziků***" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

3. Redakce stav k 9/2014

E-zin Crypto-World

Redakční práce:	Pavel Vondruška Jozef Krajčovič Jozef Martin Kollar Vlastimil Klíma
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
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/
Jozef Martin Kollar	jmkollar@math.sk ,	
Jozef Krajčovič	kryptosvet@gmail.com ,	http://katkryptolog.blogspot.sk
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška, jr.	pavel@crypto-world.info ,	http://www.pavelvondruska.cz/