Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 5/2008 **15. květen 2008**

5/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1235 registrovaných odběratelů)

Obsah: str.

Příloha:

1) Mikulášská kryptobesídka (4.-5.12.2008): CFP_MKB2008_May.pdf

2) Příloha k článku „Príklad útoku na podpisovaný dokument … “ : priklad.bmp

A. Príklad útoku na podpisovaný dokument, ktorého typ nie je chránený samotným podpisom

Peter Rybar, pr@mailbox.sk

Príklad ukazuje útok na podpisovaný dokument, ktorého typ nie je chránený samotným podpisom a taktiež na nedostatočnú ochranu pri použití bezpečného prehliadača v certifikovanej aplikácii, lebo príklad v prílohe k tomuto článku spĺňa oba typy dokumentu a tak je len na prehliadači, aký typ dokumentu sa rozhodne zobraziť.

Na spomenutý útok upozorňovalo slovenské NBÚ už niekoľko rokov a na ochranu proti nemu s novelou vyhlášky NBÚ č. 233/2007 Z. z. pripravilo štandard, ktorý so štandardom o formáte podpisu, po prechodnom období od začiatku roku 2008, zakazuje certifikovať aplikácie pre ZEP, ktoré nemajú zabezpečený typ podpisovaného dokumentu v podpise.

Na nešťastie táto povinnosť bola minulý rok v prechodnom období len odporúčaním, čo sa nestretlo s pochopením zo strany výrobcu aplikácie a ich audítora a keďže audítor im priamo povedal „Nebudete MIME implementovať", táto možnosť teoretického útoku v aplikácii ostala neošetrená. Zatiaľ tento útok nebol zverejnený na formáty, ktoré táto aplikácia podpisuje a tak nebol dôvod na prijatie opatrení, no jednoduchosť útoku na príklade BMP a HTM môže motivovať k nájdeniu možných útokov aj na tieto typy dokumentov, ak sa ponechá pre ne priestor neakceptovaním NBÚ odporúčaní a štandardov zverejnených na stránke: http://www.nbusr.sk/sk/elektronicky-podpis/schvalene-formaty/index.html

Aplikácia ELPI2 http://elpi2.szm.com je odolná voči spomenutému útoku vo formáte „podpísaný e-mail" a rovnako i v prípade, ak sa podpisuje viac ako jeden dokument vo formáte ZEP(ZIP). ELPI2 do verzie 0.8, kvôli zabezpečeniu kompatibility so spomínanou certifikovanou aplikáciou, umožní podpísanie jedného dokumentu vo formáte ZEP(ZIP) bez zabezpečenia typu podpísaného dokumentu s MIME typom dokumentu, pričom podpisovanie e-mailu je proti tomuto útoku chránené vo všetkých verziách ELPI2.

Ukážka útoku je v príklade. V príklade uvedenom v prílohe sa po premenovaní koncovky na BMP alebo HTM zobrazí odlišný text.

Z tohto dôvodu slovenské NBU vydalo štandard, v ktorom od začiatku tohto roku zakázalo podpisovanie dokumentov, ktorých typ nie je chránený podpisom v nových aplikáciách. Podpísanie je možné, len ak typ dokumentu je uvedený v MIME-TYPE. Pri XML podpise v DataObjectFormat a pri CMS musí byť dokument v MIME obálke s MIME TYPE, v ktorom je typ dokumentu, alebo typ dokumentu musí priamo vyplývať z jeho použitia, ako je tomu pri PKCS#7 podpise v PDF.

Možné postupy a obrana proti útoku bola tiež popísaná v článku, ktorý vyšiel v Crypto-World 4/2008 ISSN 1801-2140. Nuž, človek to asi prehliada, dokiaľ sa nepopáli, alebo mu niekto neukáže príklad, ako jednoducho sa môže dostať do omylu.

B. Speciální bloková šifra - Nová hešovací funkce.

Petr Sušil, MFF UK, (susil.petr@gmail.com)

Co je to hašovací funkce?

Libovolná funkce F, jejíž vstup má libovolnou (konečnou) délku a jejíž výstup má pevnou délku.

Funkce F je jednosměrná, pokud

1. je snadno spočitatelná – pro libovolný vstup M je snadné spočíst D takové, že D = F(M); „snadné spočíst“ znamená, že existuje Turingův stroj, který spočítá F(M) v polynomiálním čase.

2. Je těžko invertovatelná – pro zadané D je těžké nalézt M takové, že F(M)=D; „těžké nalézt“ znamená, že každý pravděpodobnostní Turingův stroj pracující v polynomiálním čase spočte M takové, že F(M)=D, pouze se zanedbatelnou pravděpodobností.

Existence jednosměrné funkce je ekvivalentní problému P != NP.

Kryptograficky bezpečná hašovací funkce musí mít navíc i následující vlastnosti:

1. odolnost vůči kolizím (silná odolnost vůči kolizím)

- je těžké nalézt dvě různé zprávy takové, že $H(m_1) = H(m_2)$

  „těžké“ znamená, že neexistuje lepší způsob než útok hrubou silou, který z narozeninového paradoxu vyžaduje $2^{digest\_length/2}$ dotazů.

2. Odolnost hledání druhého vzoru (slabá odolnost vůči kolizím)

- pokud dostaneme zprávu M, je těžké nalézt zprávu N tak, že H(M) = H(N); nalezení zprávy N by mělo být stejně těžké jako nalezení vzoru H(M), kdy triviální vzor M neuvažujeme

3. skoro odolnost vůči kolizím, vzoru a druhého vzoru

- tyto vlastnosti jsou často požadovány, neboť pokud útočník umí získat skoro kolizi (vzor, druhý vzor) jeho útok může být často rozšířen na zisk kolize (vzoru, druhého vzoru)

V tomto článku budeme označovat kryptograficky bezpečnou hašovací funkci pouze hašovací funkcí.

Jak konstruovat hašovací funkci?

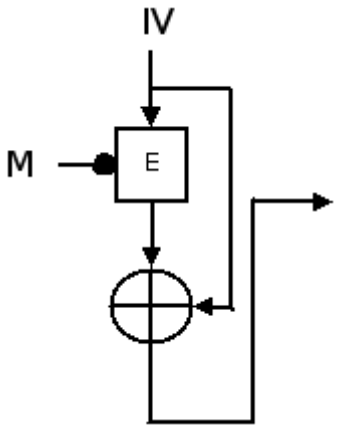
Hašovací funkce je funkce z množiny řetězců libovolné délky do množiny řetězců délky n. Měla by být dostatečně rychlá a měla by mít rozumné paměťové nároky (neměla by si pamatovat celý vstup).

Abychom splnili všechny tyto vlastnosti, jediná možnost je nějaký iterativní výpočet.

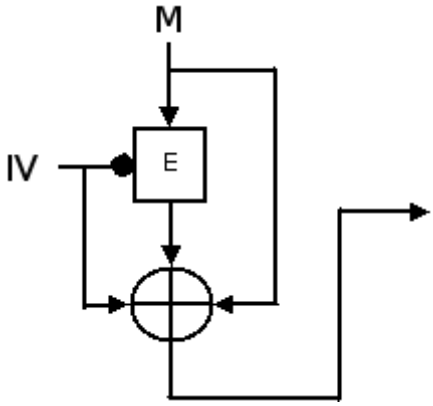
Vytváření kompresní funkce

Kompresní funkce má standardně dva vstupní parametry – blok zprávy a přechodnou haš, a výstup určuje novou (přechodnou) haš.

Kompresní funkce je často vytvořena z existující blokové šifry, protože jsou to velmi dobře studovaná kryptografická primitiva. Čtenář může nalézt seznam možných konstrukcí a jejich důkazů bezpečnosti v [1]. Nejčastěji používané jsou Davies-Meyer a Miyaguchi-Preneel konstrukce.

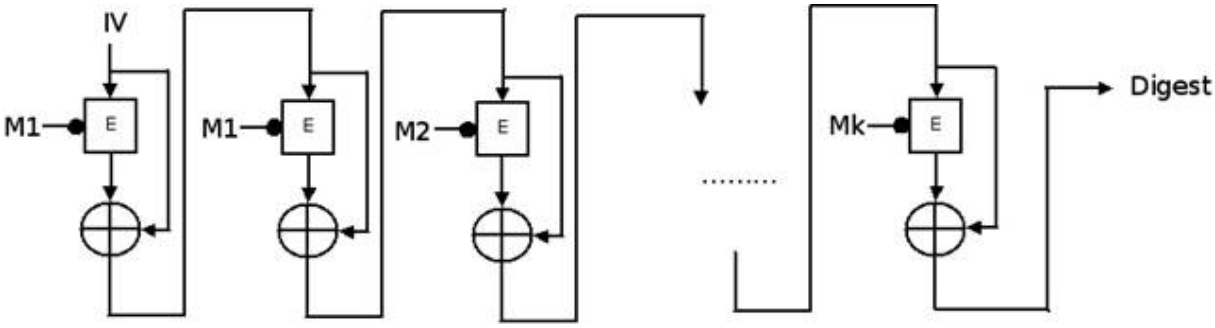


Davies-Meyer

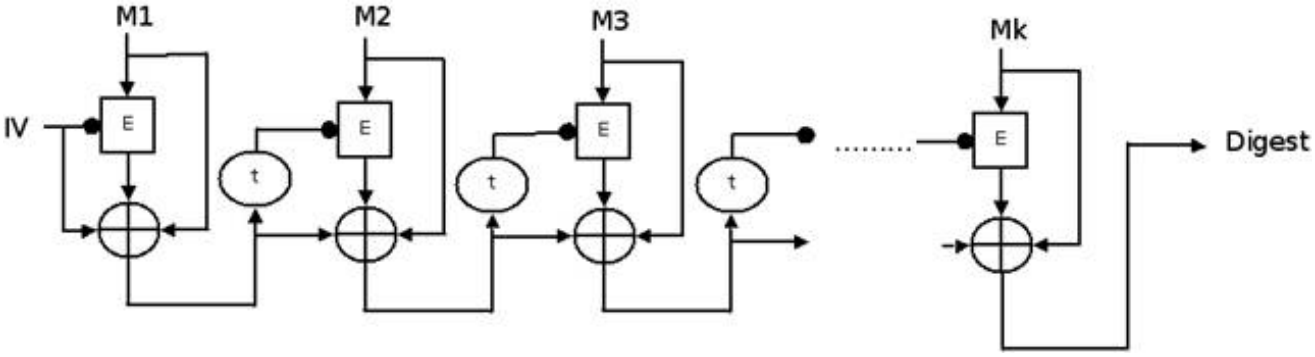


Miyaguchi-Preneel

M znázorňuje blok zprávy. V Davies-Meyer konstrukci je použita jako šifrovací klíč a v Miyaguchi-Preneel je použita jako otevřený text. Hašovací funkce pak vznikne zřetězením kompresní funkce použitím Merkle-Damgard konstrukce.



Iterace Davies-Meyer konstrukce



Iterace Miyaguchi-Preneel konstrukce

Slabiny v takto vytvořené hašovací funkci

Obecné problémy iterace

Iterace je neodstranitelný bezpečnostní problém. Každá iterovaná hašovací funkce je zranitelná vůči útoku pomocí narozeninového paradoxu. Čtenář může nalézt jednotlivé útoky v [2,3,4,5]. Ukazuje se, že druhý vzor [3] a vzor předem poskytnutého závazku [4] lze nalézt použitím $2^{n/2}$ výpočtů kompresní funkce, přestože očekávaný počet je 2^n; navíc zřetězení dvou nezávislých hašovacích funkcí neposkytuje očekávané zesílení [2]. Takovým útokům navíc nelze předejít [5]. Jediná obrana je tedy výpočetní složitost.

Obecné problémy kompresní funkce

Při útocích na hašovací funkce neexistuje žádný tajný prvek. Pokud chce útočník nalézt kolizi, pak má všechny informace, které potřebuje. Jediná ochrana hašovací funkce je výpočetní složitost. V útocích na MD5 a rodinu SHA se podařilo kontrolovat rozdíly vstupů kompresní funkce (přechodnou haš a blok zprávy) a vzájemně je vyrušit, čímž se snížila výpočetní složitost daného útoku na přijatelnou úroveň. MD5/SHA jsou hašovací funkce implicitně založené na blokové šifře – jde o 4 jednoduché blokové šifry řetězené v CBC módu. Dlouhou dobu se věřilo v bezpečnost těchto funkcí, ale v 2005 čínská profesorka Wangová [6] nalezla kolize v MD5 kontrolováním rozdílů v přechodné haši a bloku zprávy. Klíma [7] a Stevenson [8] později vylepšili tento útok a ukázali, že kolize v MD5 lze nalézt během 1 minuty na běžném notebooku. SHA1 je kryptograficky prolomená, nicméně nároky útoku jsou na hranici současné výpočetní kapacity. Funkce z rodiny SHA2 zatím prolomené nejsou, nicméně trpí stejnými slabinami jako MD5 a SHA1.

Důvody selhání současných hašovacích/kompresních funkcí

Útočník je schopen nalézt kolize v kompresní funkci, přestože je k jejímu vybudování použita silná bloková šifra. Selhání však není v blokové šifře, ale ve způsobu jejího použití. Předchozí obrázky ukazují, že přechodná haš a blok zprávy jsou blokovou šifrou zpracovávány odlišně. To útočníkovi umožňuje nalézt kolize. Tento fakt se nyní pokusíme vysvětlit z pohledu blokových šifer. Útočník volí dvojice šifrových klíčů a zpráv tak, aby našel kolizi, že $E_{k1}(m_1)=E_{k2}(m_2)$. Tento postup není z pohledu blokové šifry útok, avšak jde o velmi silný útok na kompresní funkci. Blokové šifry nejsou navrhované tak, aby takovým útokům odolávaly, neboť takový požadavek je nesmyslný pro šifrovací algoritmus. Bloková šifra je určena pouze k utajení zprávy: osoba chce ochránit obsah zprávy přenášené nedůvěryhodným prostředím. Jednoduše není žádný důvod, proč takový útok uvažovat. Ale tento typ útoku může být využit lineární a diferenciální kryptoanalýzou k nalezení kolizí v každé blokové šifře, která používá klíč a blok zprávy odlišně.

Používání IV a klíče ve stejném významu a možné útoky

Tedy kompresní funkce musí používat IV a blok zprávy stejným způsobem. Tato vlastnost je nazývána homogenita.

Uvažujme dva případy:

1. IV a blok zprávy použijeme jako otevřený text a šifrujeme pomocí pevného klíče. Vzhledem k faktu, že šifra s pevným klíčem je veřejně známá permutace, nám tato konstrukce nezaručuje žádnou bezpečnost.
2. Použití IV a bloku zprávy jako klíč a za otevřený text zvolit pevnou veřejně známou hodnotu. Tato konstrukce by mohla zaručit bezpečnost, nicméně všechny kryptografické vlastnosti musí být ověřeny či dokázány.

Odolnost na hledání vzoru

Kompresní funkce je odolná vůči hledání vzoru, pokud je příslušná bloková šifra odolná proti known-plaintext útoku. (Útočník zná otevřený text, neboť ten je veřejně známý, a výsledný šifrový text. A útočník potřebuje zjistit klíč.)

Odolnost na hledání druhého vzoru

Při tomto útoku se útočník snaží nalézt další klíč takový, že cílový šifrový text se nezmění. Protože prostor klíčů je větší než prostor šifrových textů, existuje více klíčů, které převádějí pevně zvolený otevřený text na šifrový text (nový IV). To znamená, že v kompresní funkci existují kolize z Dirichletova principu. Hledání takové kolize (jejíž otevřený text je pevně daná hodnota a část klíče je známa) je stále útok na hledání klíče a při dostatečné bezpečnosti blokové šifry tato částečná znalost o klíči nelze využít a hledání druhého vzoru je pak stejně obtížné jako hledání vzoru. Nicméně bez znalosti podoby blokové šifry to nelze tvrdit. Hledání druhého vzoru je speciální případ hledání kolizí.

Odolnost na hledání kolizí

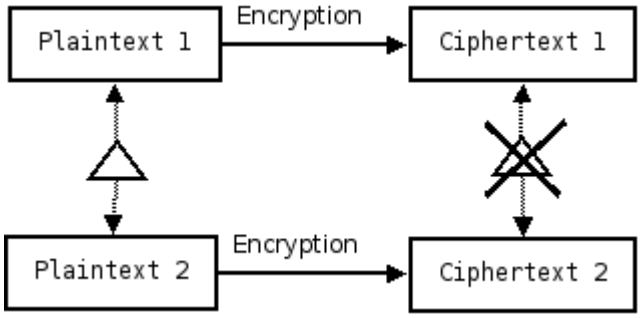
Taková funkce není odolná vůči hledání kolizí. Bloková šifra je použita na šifrování pevně zvoleného otevřeného textu za použití klíče K (vzniklého zřetězením bloku zprávy a IV) a vytvoří nové IV. Ale standardní bloková šifra má slabou expanzi klíče. Lepší expanze klíče by zpomalila šifrování. Nicméně v modelu útočníka na blokové šifry neexistuje žádný útok, který by dokázal využít slabé expanze klíče. Nicméně při použití blokové šifry k vytvoření hašovací funkce je důležitá velmi dobrá expanze klíče. Zpracování klíče je zesílené v blokové šifře nazvané Speciální bloková šifra [9]. Tato bloková šifra (rodina blokových šifer) je odolná vůči útokům jak ze strany otevřeného/šifrového textu tak ze strany klíče.

Vytvoření speciální blokové šifry

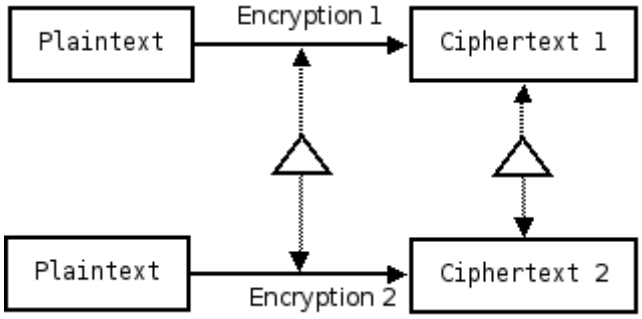
Speciální bloková šifra je bloková šifra se silnou expanzí klíče. Není navržena pro šifrování, ale může k němu být použita.

Jediný problém, který je potřeba vyřešit, je slabá expanze klíče ve standardní blokové šifře, která může být zneužita technikou lineární či diferenciální kryptoanalýzy.

Silná bloková šifra je vždy bezpečná proti lineární a diferenciální kryptoanalýze ze strany otevřeného/šifrového textu. Není žádný důvod ji zabezpečovat proti těmto útokům ze strany klíče, neboť ten je zvolen jednou, pevně a náhodně. Ale takový bezpečnostní požadavek je nutný při vytváření kompresní funkce ze standardní blokové šifry.

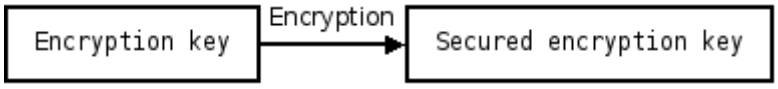


Bloková šifra je odolná vůči diferenciální kryptoanalýze ze strany otevřeného textu.



Bloková šifra není odolná vůči diferenciální kryptoanalýze ze strany klíče.

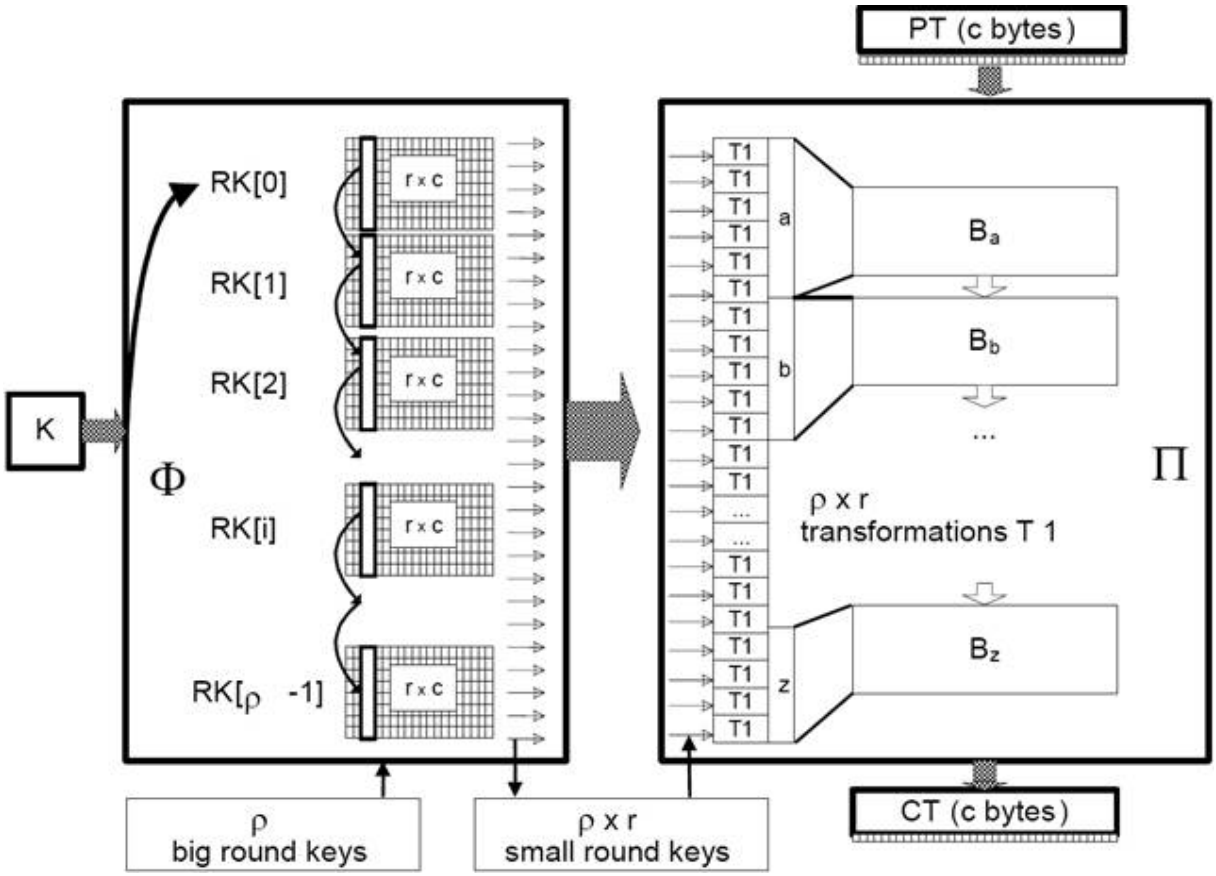
Protože standardní blokové šifry jsou bezpečné vůči útoku ze strany otevřeného textu, může být použita při expanzi klíče ve speciální blokové šifře - k zašifrování klíče pro další rundy a zabezpečení proti diferenciální kryptoanalýze.



Zbývající otázkou je volba šifrového klíče (používaného k zašifrování K). Nejjednodušší je volba pevného klíče. Protože je šifra bezpečná, útočník nemůže řídit diferencemi na vstupu diference na výstupu (tedy v expandované zprávě), které by umožňovaly řízení diferencí na výstupu pomocí diferencí v klíči. Alternativně si lze expanzi klíče představit jako (samoopravný) kód. V tomto případě jde o kód podobný opakovacímu kódu.

Klíma navrhl typ speciální blokové šifry [9], kterou nazval Double net (DN), a podal matematické důkazy, že pro zvětšující se velikosti bloku je daná šifra nerozlišitelná od náhodného orákula. DN je požita jako kompresní funkce a zřetězena pomocí Enveloped Merkle-Damgard konstrukce. Tato nová hašovací funkce je nazvaná Hash Double net (HDN).

Kompresní funkce má jediný vstup vzniklý zřetězením IV a bloku zprávy. Vstup do kompresní funkce vstupuje jako šifrovací klíč a šifrový text je použit jako nové IV.



DN cipher. [7]

Matice je naplněna šifrovým klíčem (levá strana). Matice RK[i] vznikne šifrováním jednotlivých sloupců matice RK[i-1]. Řádky matice RK[j] jsou použity jako rundovní klíče v j-té rundě při šifrování (pravá strana).

Úplný popis DN algoritmu a důkaz bezpečnosti lze nalézt v [9]. DN šifra je použita jako kompresní funkce. Její odolnost vůči hledání vzoru je zajištěna z vlastností blokových šifer – je odolná vůči known plaintext útoku. Jak odolnost na hledání druhého vzoru tak odolnost na hledání kolizí jsou zajištěny dodatečnými vlastnostmi speciálních blokových šifer – silná expanze klíče při šifrování znemožňuje použití diferenciální kryptoanalýzy na straně klíče.

References

[1] Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions

[2] A. Joux, „Multicollisions in Iterated Hash Functions. Applications to Cascaded Constructions“, Advances in Cryptology - Crypto'2004, LNCS 3152, Springer (2004), pp. 306—316.

[3] J. Kelsey, B. Schneier, „ Second Preimages on n-Bit Hash Functions for Much Less than 2n Work,“ Advances in Cryptology - Eurocrypt'2005, LNCS 3494, Springer (2005), pp. 474--490.

[4] T. Kohno, J. Kelsey, „ Herding Hash Functions and the Nostradamus Attack“, First NIST Cryptographic Hash Workshop, Gaithersburg, USA, October 31 -- November 01, 2005. Full version: Advances in Cryptology -- Eurocrypt'2006, LNCS 4004, Springer (2006), pp. 183—200.

[5] J. J. Hoch, A. Shamir, „Breaking the ICE - Finding Multicollisions in Iterated Concatenated and Expanded (ICE) Hash Functions“, Fast Software Encryption -- FSE'2006, LNCS 4047, Springer (2006), pp 179—194.

[6] X. Wang, H. Yu, „ How to Break MD5 and Other Hash Functions“, Advances in Cryptology -- Eurocrypt'2005, LNCS 3494, Springer (2005), pp. 19—35.

[7] V. Klima, „Tunnels in Hash Functions: MD5 Collisions Within a Minute“, Cryptology ePrint Archive

[8] M. Stevens, „Fast Collision Attack on MD5“, Cryptology ePrint Archive

[9] http://crypto-world.info/klima/SNMAC/SNMAC_EN.pdf

C. Z dějin československé kryptografie, část VII., Československé šifrovací stroje z období 1960 – 1970. Šifrovací stroj ŠD – 3 .

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

V letech 1960 až 1963 byl v československé šifrové službě používán první šifrátor s označením ŠD – 1, který pracoval na principu vloženého hesla na pětistopé papírové děrné pásce, používal se pro provoz on-line jako doplněk dálnopisu a byl čistě domácí konstrukce i výroby. Po neúspěchu s výrobou či dovozem moderního komutátorového šifrového stroje s vlastní tvorbou hesla v Československu na konci padesátých let minulého století, který měl pracovní označení ŠD – 2 a byl dost podrobně popsán v předchozích dvou kapitolách, bylo rozhodnuto postupovat už kryptologicky bezpečně prověřenou a osvědčenou cestou a vybavit československou šifrovou službu novým šifrátorem pracujícím s vloženým heslem s označením ŠD – 3. Požadavek na vyšší kapacitu šifrového spojení přicházel zejména od armády, kde bylo v té době rozšiřováno linkové dálnopisné i radiodálnopisné spojení. Československá armáda byla v té době vybavována novými dálnopisnými stroji Dalibor D – 302, které byly ryze domácí provenience a byly vyráběny ve Zbrojovce Brno.

První prototyp dálnopisného stroje „Dalibor"

Šifrovací stroj ŠD – 3 byl vyvinut na Zvláštní správě Ministerstva vnitra ČSR v letech 1958 až 1960 a byl následně vyráběn v 1. spojovací základně Ministerstva národní obrany v Hradci Králové. Celkem bylo v několika sériích vyrobeno 815 kusů tohoto zařízení. V československé šifrové službě začal být šifrátor ŠD – 3 používán od roku 1962 a v armádě našel uplatnění až do začátku osmdesátých let minulého století. V roce 1980 se v armádě ještě používal a v roce 1985 byl u armády veden jako záložní spojovací prostředek. Po vyřazení těchto šifrovacích strojů u ministerstva vnitra, koncem sedmdesátých let, odebírala armáda tyto šifrátory na náhradní díly, neboť je měla zařazeny v mobilizačních zásobách.

Dálnopisný stroj D-302 „Dalibor"
vyráběný ve Zbrojovce Brno

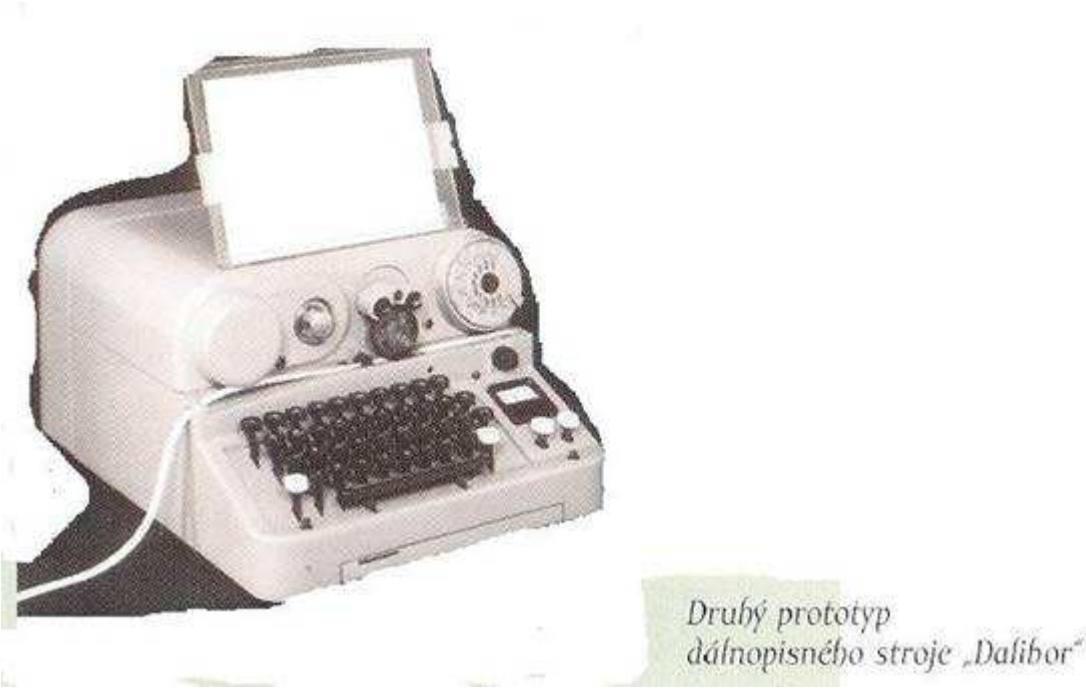
Používaná terminologie pro označení šifrovacího stroje ŠD – 3 není úplně precizní. Jednak se tento název používal pro sestavu dálnopisu Dalibor D – 302 spolu s reléovým šifrovacím doplňkem. Celá tato sestava bývala také kromě názvu ŠD – 3 označována jako dálnopis či šifrovací dálnopis Dalibor typ 305. Méně často se používalo označení ŠD – 3 jen pro výše zmíněný reléový šifrovací doplněk, který realizoval šifrování sčítáním otevřeného textu s heslem na pětistopé papírové děrné pásce a dešifraci odečítáním hesla na děrné pásce od šifrového textu. Dálnopisná šifrovací sestava Dalibor typ 305 umožňovala přímé (on-line) i předběžné (off-line) šifrování, obojí však pouze v modulu 32. Souprava Dalibor typ 305 byla elektromechanické konstrukce o rozměrech asi 450mm x 400mm x 350mm a byla vybavena odstředivým regulátorem otáček motoru a stroboskopickou kontrolou. Souprava byla obvykle zelené (někdy též šedé) barvy a byla vybavena uzamykatelným krytem, který bylo možno zapečetit. Stejně jako šifrovací stroj ŠD – 1 byl i šifrátor ŠD – 3 v prvních sériích vybaven

řezačkou použité heslové děrné pásky. Protože tento způsob likvidace heslové děrné pásky přestal být považován za bezpečný a začal být naopak považován za nadbytečný, byla u novějších strojů již tato řezačka z konstrukce vypuštěna. Vstupem šifrovacího stroje ŠD – 3 byla buď klávesnice shodná s klávesnicí dálnopisu Dalibor D – 302 nebo snímač pětistopé děrné pásky. Výstupní text se tiskl v řádcích na pás papíru (přepínač plynulého tisku nebo tisku do skupin byl umístěn vpředu nad klávesnicí) nebo byl při režimu off-line děrován perforátorem na pětistopou děrnou pásku v modulu 32 v sestavě s tzv. automatizačním doplňkem, který bude popsán dále. Na zadní straně stroje se nacházel napájecí síťový kabel opatřený zástrčkou pro napájení 220V AC a dále linkový kabel s kolíkovou zástrčkou, který se v režimu on-line připojoval do externí linkové zásuvky a v režimu off-line jej bylo nutno zasunout do dálnopisné zásuvky umístěné rovněž na zadní straně stroje. Do soupravy šifrovacího stroje ŠD – 3 patřilo rovněž plastové pouzdro se dvěma tubami mazacího oleje, čistícím štětcem, šroubovákem, ladičkou pro kontrolu otáček motoru, dvěma náhradními uhlíky motoru a dvěma náhradními relé do šifrovacího bloku.

K šifrovacímu stroji ŠD – 3 se ještě vyráběl automatizační doplněk typ 327, který nebylo možno samostatně použít a pracoval výhradně s ŠD – 3. Byla to vlastně ještě dále rozšířená sestava Dalibor typ 305, která pomocí doplňku typ 327 mimo jiné umožňovala při off-line šifrování výstup šifrového textu přes děrovač na pětistopou papírovou děrnou pásku v modulu 32. Sestav s těmito automatizačními doplňky typ 327 bylo ve dvou sériích vyrobeno celkem 220 kusů a ještě v letech 1980 – 1982 byly údajně používány. Jednalo se vlastně o vylepšení šifrovacího stroje ŠD – 3 s cílem mechanizovat práce spojené s přípravou a přenosem šifrových zpráv. Rychlost činnosti této sestavy byla 400 znaků za minutu.

Koncepce šifrovacího stroje ŠD – 3 byla ve své době velmi moderní. Šifrovací blok byl pouze modulem ke standardně vyráběnému dálnopisnému stroji a tvořily spolu kompaktní celek. Hlavním problémem bezpečného používání tohoto šifrátoru tak bylo perfektní klíčové hospodářství a to včetně ničení použitých heslových materiálů, kterých bylo při silném provozu velmi mnoho (objem hesla byl stejný jako objem předávaných textů). Stejnou cestou šli všichni světoví výrobci dálnopisných šifrátorů, ale na rozdíl od Československa oni velmi brzy vyvinuli i relativně bezpečné dálnopisné šifrovací moduly s vlastní tvorbou hesla, které pak používala například většina západoevropských zemí i v dálnopisném diplomatickém

spojení od sedmdesátých let do poloviny devadesátých let 20. století. Pravdou zůstává, že při velmi tvrdém ataku tyto systémy často neodolaly. Stejný osud ovšem potkával mnohdy i systémy „jednodobé pásky“ (one time pad) typu šifrátoru ŠD – 3, kde kromě spíše ojedinělého porušení důsledně jednorázového použití hesla docházelo ke kompromitaci přímo heslového hospodářství. V Československu se v té době v odpovídajících aplikacích, zejména v armádě, používaly dlouhodobě výhradně šifrovací stroje s vlastní tvorbou hesla dodávané ze SSSR.



Druhý prototyp dálnopisného stroje „Dalibor“

Již od roku 1957 byl na Zvláštní správě ministerstva vnitra vyvíjen generátor absolutně náhodné a stejně pravděpodobné posloupnosti hesla pod označením HPS – 2. Pro generování takovéto libovolně dlouhé dvouhodnotové posloupnosti mělo být využito rozpadu některého vhodného radioaktivního prvku. Podle poznámek jednoho z účastníků jednání na toto téma neměli v SSSR s touto metodou v roce 1957 zkušenosti a nepoužívali ji. Problémů byla řada, zejména nebylo k dispozici vhodné velkokapacitní paměťové zařízení a dále nebyla výpočetní kapacita na testování dlouhých posloupností. Přestože byla snížena původně požadovaná univerzálnost vyvíjeného zařízení, byl tento generátor vyroben a heslové materiály na něm byly produkovány.

Vývojovou skupinu šifrovacího stroje ŠD – 3, která sídlila v Praze Ruzyni, vedl od roku 1958 na Zvláštní správě ministerstva vnitra Ing. Lubomír Odvárko, který přišel z Aritmy Praha. Ve skupině pracovali rovněž dipl. tech. Zdeněk Křesina a Karel Fuka. Ing. Odvárko zemřel asi v roce 1960, když na pracovišti dostal infarkt a druhý den ráno v nemocnici vstal z postele, šel se oholit a následný druhý infarkt již nepřežil. Vývojem ŠD – 3 byl pak pověřen Zdeněk Křesina.

Šéfkonstruktérem dálnopisu Dalibor D – 302 ve Zbrojovce Brno byl legendární Ing. Weber, který byl německého původu a před 2. světovou válkou byl údajně šéfkonstruktérem německého šifrátoru ANNA. Tento šifrátor byl podobné konstrukce jako Enigma, tedy diskový komutátorový, ovšem s 12 disky a byl používán ve Wehrmachtu za 2. světové války údajně zejména Rommelovou armádou v severní Africe. Bratr tohoto zbrojováckého inženýra Webera pracoval prý podle svědků jako šéfkonstruktér u západoněmecké firmy Standard Elektrik Lorenz (SEL), která byla jedním ze tří nejvýznamnějších německých výrobců šifrovacích strojů ve druhé polovině 20. století. Podle vzpomínek jednoho s pamětníků probíhala spolupráce s Ing. Weberem i při konstrukci šifrátoru ŠD – 3 (!).

Ilustrační obrázky dálnopisného stroje Dalibor D – 302, který byl vyvinut a vyráběn v tehdejším národním podniku Zbrojovka Brno, byly převzaty z publikace Michal Burian, Jiří Rýc - Historie spojovacího vojska (Ministerstvo obrany ČR – Agentura vojenských informací a služeb, 2007).

D. Mikulášská kryptobesídka , Call for Papers

4. – 5. prosinec 2008, Praha , http://www.buslab.cz/mkb

BUSLab

TRUSTED NETWORK SOLUTIONS

Základní informace

Mikulášská kryptobesídka se koná letos již poosmé. 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 *4. prosince 2008* a (b) půldne prezentací příspěvků a diskusí v pátek *5. prosince 2008*.

Pro workshop jsou domluveny zvané příspěvky:

- **Eli Biham** (Technion, Haifa, Israel): *On the (In)security of the Ciphers and Protocols of GSM*.

In this talk we describe the ciphers and protocols used for the GSM cellular phone network, and discuss the (in)security of the system. We describe several techniques to attack the ciphers A5/2 and A5/1, and how they can be applied as a ciphertext-only attack. We also show that active attacks on the protocols can recover keys of ciphers that are not used during that transmission. As a result, it is possible to listen in to GSM phone conversations, steal calls during the conversation, and even issue new calls on behalf of (and paid by) an attacked phone.

This talk summarizes several papers on this issue. This is a joint work with Elad Barkan and Nathan Keller.

- **Richard Clayton** (University of Cambridge, UK): *Can cryptography secure the Internet?*

Every system that runs over the Internet, from email through web browsing, from banking to eCommerce, from checking bus timetables to booking a hotel, ultimately depends on the security of the Domain Name System (DNS) and upon the security of BGP, the protocol used by routers to keep track of the best way of routing packets. Unfortunately, both the DNS and BGP are horribly insecure, and can be easily subverted. Most of the serious failures thus far have been accidental and easy to deal with, but eventually criminals will work out how to subvert the system without being immediately detected. Then we'll all be sorry! This talk examines the extent to which cryptography can make the Internet's infrastructure secure, and some of the reasons why cryptographicsolutions are yet to be deployed.

- **Jozef Gruska** & **Jan Bouda** (MU, Brno): *New directions in quantum cryptography*

The field of quantum information processing, communication and cryptography develops rapidly both to breadth and depth. About 400 papers are produced per month, from deep foundational and theoretical results to a variety of interesting experimental results. The goal of this talk is to highlight the development in cryptographic areas of quantum information processing, namely encryption, authentication, identification and digital signatures.

- **Martin Hlaváč** & **Tomáš Rosa** (UK, Praha & e-banka): *Towards Disclosing the RSA Private Key of an e-Passport*

The recent deployment of the electronic passports equipped with RFID chips might leave one asking on how far is that platform secure. We briefly review (and also demonstrate partially) several generic and unavoidable weaknesses of the RFID chips, such as an ID cloning, the relay attack, and electromagnetic side channels. Secondly, we focus on a specific cryptographic operation of the e-passport. It is shown that due to an existing side channel an insecure implementation of one single cryptographic primitive such as the modular multiplication can cause the entire (otherwise secure) scheme to collapse. To provide an attack on the real e-passport, two elementary steps need to be done. First, the side channel signal has to be mapped on the assumed chip operations. Secondly, we have to develop a mathematical tool allowing us to exploit such a signal. Our contribution deals mainly with the second part, the first one leaving open with several positive indices. We show that given the amount of so-called final substitutions in Montgomery multiplication algorithm (used for RSA signing operation) one can launch a known cipher text attack on the RSA instance. This is an improvement of the existing chosen ciphertext attack [1]. As the original attack required a chosen ciphertext condition, it was useless for the e-passport signature scheme. Therefore, we regard our improvement as being essential step towards breaking the e-passport active authentication scheme.

[1] Tomoeda et al., An SPA-Based Extension of Schindler's Timing Attack against RSA Using CRT, 2005

- **Zdeněk Říha** (MU, Brno): *On security and crypto issues of e-passports*

The follow up talk (of the talk on MKB 2007) will focus on security issues of electronic passports. In particular possibilities of identifying the passports issuing country will be discusses. A few optional features and not unified error response codes allow for relativelly easy identification of a manufacturer of the chip and possibly also of a particular model of the chip. In practice that means that whenever we can communicate with the ePassport we can guess the issuing country even if we do not perform the Basic Access Control authentication.

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

Mediální parneři

Pokyny pro autory

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

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

Příspěvky připravené podle výše uvedených pokynů zasílejte ve formátu RTF, nebo PDF a to tak, aby na uvedenou adresu přišly nejpozději do *30. září 2008*. Pro podávání příspěvků prosím použijte adresu matyas ZAVINAC fi.muni.cz a do předmětu zprávy uveďte „MKB 2008 – 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 *21. října*. Příspěvek pro sborník workshopu pak musí být dodán, společně s krátkým životopisem (50-100 slov), do *18. listopadu*.

Důležité termíny

Návrhy příspěvků:	30. září 2008
Oznámení o přijetí/odmítnutí:	21. října 2008
Příspěvky pro sborník:	18. listopadu 2008
Konání MKB 2008:	4. – 5. prosince 2008

Programový výbor

Dan Cvrček, VUT v Brně & MU, Brno
Vlastimil Klíma, nezávislý kryptolog
Vašek Matyáš, MU, Brno – předseda
Zdeněk Říha, MU, Brno & JRC Ispra, Itálie
Martin Stanek, UK, Bratislava
Luděk Smolík, MU, Brno
Pavel Vondruška, Telefónica O2 & UK Praha

E. O čem jsme psali v květnu 2000 – 2007

Crypto-World 5/2000

+ příloha : J.Hrubý , soubor QNG.PS

Crypto-World 5/2001

Příloha : priloha.zip : součástí jsou soubory obsah.rtf (obsah všech dosud vyšlých e-zinů Crypto-World) a mystery.mid (viz. článek "Záhadná páska z Prahy")

Crypto-World 5/2002

Příloha: SBKS 2002 - výzva pro autory cfp.pdf

Crypto-World 5/2003

Crypto-World 5/2004

Crypto-World 5/2005

Crypto-World 5/2006

Crypto-World 5/2007

F. Závěrečné informace

1. Sešit

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

2. Registrace / zrušení registrace

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

3. Redakce

E-zin Crypto-World

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