Crypto-World

Informační sešit GCUCMP

Ročník 7, speciál **4. leden 2005**

Speciální vydání -
přehled článků a prezentací členů redakce Crypto-World za rok 2004

P.Vondruška: http://crypto-world.info/vondruska/index.php
V.Klíma : http://cryptography.hyperlink.cz/
T.Rosa: http://crypto.hyperlink.cz/
J.Pinkava: http://crypto-world.info/pinkava/index.php

Připravil: Mgr. Pavel Vondruška

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

Obsah : **str.**

A. Články pro veřejnost (populárně-naučné)

P.Vondruška: http://crypto-world.info/vondruska/index.php
V.Klíma : http://cryptography.hyperlink.cz/
T.Rosa: http://crypto.hyperlink.cz/
J.Pinkava: http://crypto-world.info/pinkava/index.php

Prolomení MD5 a souvislosti
Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (17) – **prolomení hašovací funkce MD5**, Sdělovací technika, 12/2004, str. 14 - 15, http://cryptography.hyperlink.cz/2004/st_2004_12_14_15.pdf (link bude aktivní po vyjití čísla 02/2005).

Kompromitované podepisovací klíče ElGamal v GnuPG
Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (16) – **lidová tvořivost se nevyplácí**, Sdělovací technika, 11/2004, str. 14 - 15, http://cryptography.hyperlink.cz/2004/st_2004_11_14_15.pdf (link bude aktivní po vyjití čísla 01/2005).
Abstrakt: Hlavní architekt projektu GnuPG (též GPG) se 27.listopadu 2003 ocitl ve zvlášť nepříjemné situaci. Musel vydat zprávu, jejíž text byl jasný, stručný a mrazivý: *Byla nalezena závažná slabina v implementaci ElGamal... Toto je reálná, celosvětová slabina, která umožňuje získat během několik sekund váš privátní klíč... Všechny podepisovací klíče schématu ElGamal používané v systému GPG verze 1.0.2 (leden 2000) až 1.2.3 (srpen 2003) musí být považovány za kompromitované...* Lze si domyslet, že člověku, který podstatnou část svého času věnuje právě tomuto volně dostupnému nástupci PGP, se něco takového určitě nepsalo s lehkou rukou. Článek vysvětluje proč k tomu došlo.

Základy autentizace, upozornění na slabinu služby SMS
Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (15) – **základy autentizace**, Sdělovací technika, 9/2004, str. 14 - 15, http://cryptography.hyperlink.cz/2004/st_2004_09_14_15.pdf .
Abstrakt: Tématem tohoto dílu je využití kryptografických metod k bezpečnému prokazování identity subjektů v informačních systémech. Zabýváme se pojmy identifikace, autentizace, autorizace, Kryptologie striktně rozlišuje dva základní druhy autentizace, a to autentizaci subjektu a autentizaci původu zprávy. Dále se zabýváme základními schémata autentizace, schématem výzva-odpověď a využitím asymetrických a symetrických šifer a hašovacích funkcí k autentizaci. Nakonec se ukazuje díra v zabezpečnení autentizace odesílaných SMS zpráv, která může mít někdy vážné důsledky.

Jak používat WinZip, abychom dostali kvalitní šifru
Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (14) – **lze WinZipem kvalitně šifrovat?,** Sdělovací technika, 8/2004, str. 10 - 11, http://cryptography.hyperlink.cz/2004/st_2004_08_10_11.pdf.
Abstrakt: WinZip kromě komprimace umožňuje doplňkově i šifrovat soubory a archivy. I když používá kvalitní šifru, haš a HMAC, přesto z bezpečnostně-systémového hlediska nejsou poskládány zcela bezpečně. Poukazujeme na chyby a uvádíme postup, jak používat stávající WinZip tak jak je, bez zásahu do programu, ale s několika tipy, které umí překonat jeho

nedostatky. Pokud se uživatel našich několika jednoduchých rad bude držet, získává kvalitní šifrovací nástroj. V opačném případě se může naopak dost divit, jak je to možné, že mu unikají informace, když "je to zašifrováno pomocí AES".

Délka klíče symetrických a asymetrických šifer
Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (13) – **Volba klíče**, Sdělovací technika, 7/2004, str. 14 - 15, http://cryptography.hyperlink.cz/2004/st_2004_07_14_15.pdf .
Abstrakt: Jaký algoritmus máme použít v aplikaci, kterou navrhujeme? Postačí AES se 128 bitovým klíčem nebo o čtvrtinu pomalejší AES s 256 bitovým klíčem? Jakou hašovací funkci použít k derivaci klíčů? SHA-256 nebo SHA-384 a zkrátit její výstup? O bezpečnosti a vhodných délkách klíčů různých algoritmů se často vedou, tu více tu méně, zasvěcené debaty nejen mezi programátory, bezpečnostními architekty, ale i teoretickými kryptology. Často je také problém shodnout se na tom, jak vlastně chceme bezpečnost měřit. Ukážeme si zde praktický pohled na to, jaké algoritmy nabízí jakou bezpečnost a jaké kombinace algoritmů má a nemá smysl používat.

ElGamal
Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (12) – **Schémata ElGamal**, Sdělovací technika, 6/2004, str. 12, http://cryptography.hyperlink.cz/2004/st_2004_06_12_12.pdf .
Abstrakt: ElGamal představuje rodinu schémat, jejíž základní větve tvoří asymetrické *šifry* a *podpisová schémata*. Předesíláme, že narozdíl od podobně univerzálního systému RSA, kde jak šifrovací, tak i podpisové schéma vycházejí ze stejných základních transformací, v případě ElGamal tak dokonalou provázanost nenajdeme. V podstatě můžeme říci, že šifrovací a podpisové větve zde spojuje toliko společný problém pro jištění bezpečnosti (diskrétní logaritmus) a jméno autora.

Diffieho-Hellmanův protokol dohody na klíči
Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (11) – **Protokol D-H**, Sdělovací technika, 5/2004, str. 16, http://cryptography.hyperlink.cz/2004/st_2004_05_16_16.pdf .
Abstrakt: Asymetrické šifry se v současné době používají prakticky výhradně v rámci takzvaných hybridních šifrovacích schémat. Zde je otevřený text nejprve zašifrován některou ze symetrických metod, kde je ochráněn takzvaným dočasným symetrickým klíčem, který je generován náhodně pro každou novou zprávu. Tento dočasný symetrický klíč je poté sám zašifrován pomocí zvolené asymetrické šifry a v tomto tvaru je přiložen k šifrovému textu zprávy. Důvodem pro takové uspořádání je mimo jiné podstatně vyšší rychlost symetrických metod v porovnání s asymetrickými. Připomeňme také, že asymetrická kryptografie tento trend reflektuje tím, že vytváří speciální druhy schémat právě pro účely bezpečného ustavení dočasného sdíleného symetrického klíče mezi komunikujícími stranami. K nejpoužívanějším schématům takového typu patří i Diffieho-Hellmanův protokol dohody na klíči (zkráceně D-H), kterému se článek věnuje.

Schémata DSA a ECDSA
Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (10) – **DSA, ECDSA**, Sdělovací technika, 4/2004, str. 21, http://cryptography.hyperlink.cz/2004/st_2004_04_21_21.pdf .
Abstrakt: Nejznámějšími schématy pro digitální podpisy jsou v současné době RSA, DSA a ECDSA. Podpisové schéma DSA (Digital Signature Algorithm) definované standardem FIPS

PUB 186-2 a jeho varianta Elliptic Curve DSA (ECDSA), vzniklá přenesením DSA nad algebru bodů rovinné eliptické křivky, hrají právem důležitou úlohu v současné asymetrické kryptografii. Na území USA jsou totiž DSA a ECDSA schváleny standardem FIPS PUB 186-2 pro použití ve vládních institucích, což je určitá výsada, kterou donedávna nemělo ani RSA. Teprve novelizace zmíněného standardu v roce 2000 v tomto smyslu RSA a DSA zrovnoprávnila.

Schéma RSA

Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (9) – **metoda RSA**, Sdělovací technika, 3/2004, str. 17, http://cryptography.hyperlink.cz/2004/st_2004_03_17_17.pdf .

Abstrakt: Když roku 1978 vyšel článek pánů Rivesta, Shamira a Adlemana o nové asymetrické metodě vhodné pro šifrování a podepisování zpráv, patrně nikoho z autorů nenapadlo, že jejich systém bude o nějakých 26 let později nejrozšířenějším standardem asymetrické kryptografie. Autoři RSA měli štěstí a použili pro jištění bezpečnosti RSA solidní matematický problém, který dodnes nebyl prakticky přemožen a navíc vhodně použili parametr (délku modulu), jehož zvyšováním lze snadno a efektivně zvyšovat bezpečnost RSA. To vše ovšem neznamená, že RSA jako kryptografická metoda by byla bez jakýchkoliv vad na kráse. Naopak, prakticky každý rok se na RSA něco většího či menšího „záplatuje“. Základní definice RSA se totiž zabývá pouze zavedením šifrovacích/odšifrovacích, respektive ověřovacích/podepisovacích transformací, zatímco nejvíce problémů vznikalo ve formátování (kódování) zpráv pro RSA. Další „záplatování“ konkrétních aplikací RSA přinesl objev postranních kanálů, které ukázaly, že RSA je extrémně bezpečnostně citlivá na každý detail konkrétní implementace. RSA se však zatím dokázala ze všech problémů vždy nějak „oklepat“ a žije dál.

Hašovací kód HMAC

Vlastimil Klíma, Tomáš Rosa: Kryptologie pro praxi (8) – **funkce HMAC**, Sdělovací technika, 2/2004, str. 17, http://cryptography.hyperlink.cz/2004/st_2004_02_17_17.pdf .

Abstrakt: Hašovací funkce se používají velmi hojně v celé symetrické i asymetrické kryptografii. V moderních standardech a protokolech (například SSL/TLS) se to jimi a klíčovanými hašovými kódy (Keyed-Hash Message Authentication Code, HMAC) jen hemží. Klíčované hašové autentizační kódy zpráv (HMAC) se vytváří malou modifikací hašovacích funkcí - společně se zprávou M se hašuje i nějaký tajný klíč K. Výsledkem je zabezpečovací kód HMAC(M, K), který případnému útočníkovi znemožňuje pozměnit zprávu a současně i její HMAC, neboť nezná tajný klíč.

Vlastimil Klíma, Milan Zámostný: **Šifrování dat v kapesních počítačích**, Chip Speciál "Počítač v kapse", květen 2004, str. 50 - 53, http://cryptography.hyperlink.cz/2004/PVK_2004_05_50_53.pdf (5 MByte).

Vlastimil Klíma: **Praktické útoky na digitální podpisy používající hašovací funkci MD5**, článek na www.root.cz, 9. 12. 2004 http://www.root.cz/clanek/2535

Abstrakt: Jakékoliv dva různé soubory předáte pomocí určitého postupu dvěma uživatelům, a přitom si oba dva na základě vzájemné kontroly digitálních otisků MD5 budou myslet, že mají tentýž soubor...

Vlastimil Klíma: **Hašovací funkce MD5 a další prolomeny!**, článek na www.root.cz, 25. 08. 2004, http://www.root.cz/clanek/2368
Abstrakt: V srpnu se několik kryptologů postaralo o opravdové překvapení, když předložili kolidující zprávy hned pro čtyři hašovací funkce. Znamená to, že tyto funkce by už dále neměly být používány pro digitální podpisy.

Vondruška, P. : **Šifra z doby d'Artagnana (1. díl)**

Tímto článkem začíná nepravidelný seriál, který vás zavede do různých období a bude vás seznamovat se zajímavými příběhy z dějin kryptologie. V první části se seznámíte s významnou postavou francouzské kryptologie Antoine Rossignolem a s šifrováním z doby, kterou důvěrně znáte z knihy A.Dumase – Tři mušketýři.(publikováno: 20.9.2004)
http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040915_5283431_bezpecnost

Vondruška, P. : **Šifra z doby d'Artagnana (2. díl)**

Druhá část je věnována nomenklátoru. Seznámíte se s touto oblíbenou šifrovací technikou a dozvíte se o výrazném bezpečnostním zlepšení, které Antoine Rossignol zavedl. Dozvíte se, jak vznikla Francouzská akademie věd a jak její vznik souvisí s naším tématem. S Rossignolem se rozloučíme básní, která oslavuje jeho skutky a možnosti kryptoanalýzy.(publikováno: 29.9.2004)
http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040915_5283441_bezpecnost

Vondruška, P. : **Luštitelé z dob Marie Terezie**

V článku se seznámíte s prací luštitelů *Geheime-Kabinets-Kanzlei* na vídeňském císařském dvoře za vlády Marie Terezie. Toto luštitelské pracoviště patřilo mezi nejlepší obdobná pracoviště v Evropě. Zajímá vás jak zde vypadal typický pracovní den? Chcete se dozvědět, kdo byl Ignaze de Koch? Pokud ano, pak je tento článek určen právě pro vás. (publikováno: 7.10.2004)
http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040929_5284148_bezpecnost

Vondruška, P. : **Dešifrované telegramy dokazují, že se demokraté snažili podplatit republikány při prezidentských volbách**

Když byly při prezidentských volbách sečteny všechny hlasy při všeobecném hlasování, tj. při volbě elektorů, kandidát na prezidenta za demokratickou stranu vedl o 250 000 hlasů před svým republikánským soupeřem. Převaha ve volebním kolegiu tvořeného voliteli závisela na tom, která ze dvou protichůdných úředních zpráv o průběhu všeobecného hlasování na Floridě, Lousianě, Jižní Karolině a Oregonu bude uznána jako platná a správná. (publikováno: 2.11.2004)
http://technet.idnes.cz/sw_internet.asp?r=sw_internet&c=A041101_5285844_sw_internet

Vondruška, P. : **Jak se luští kódové knihy**

V pátém pokračování seriálu věnovaném historii šifrování se dozvíte, jak se dají luštit šifry vytvořené pomocí tzv. kódových knih. Přečtete si o chybách, kterých se šifranti dopouštěli, a které ulehčili luštitelům jejich práci. V závěru se seznámíte s využíváním kódových knih americkým expedičním sborem za první světové války. (publikováno: 15.11.2004)

http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040929_5284158_bezpecnost

Vondruška, P. : **Zimmermannův telegram poslal USA do války**

Šestá část seriálu nás zavádí do období první světové války. Autor shrnuje události, které na základě vyluštění jednoho jediného telegramu ministra zahraničí Arthura Zimmermanna vedly ke vstupu USA do války. Od té chvíle se s konečnou platností změnila rovnováha sil na evropském válčišti ve prospěch Dohody…. (publikováno: 29.12.2004)

http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A041226_135705_bezpecnost_brz

Vondruška, P. : **Praha – Londýn – Ležáky**

Jak probíhalo za druhé světové války spojení odbojářů s centrálou v Londýně a byla tato komunikace bezpečná? Odpověď můžeme najít v depeši, která byla odeslána z Londýna do Prahy přesně rok před nešťastnou událostí v Ležákách.
(publikováno: 24.06.2004)

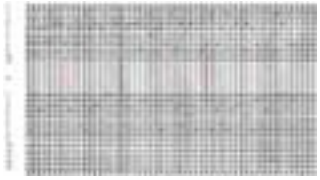
http://technet.idnes.cz/sw_internet.asp?r=sw_internet&c=A040622_5263957_sw_internet

Vondruška, P. : **Záhadná páska z Prahy (1. díl - Nález uschované pásky)**

Koho by nelákaly záhady? Zde máte nyní možnost se s řešením jedné takové seznámit. Ve třech dílech můžete sledovat krok za krokem postup odhalování textu, který je uložen na pásce. Páska byla nalezena při opravě Dětského domu v Praze. Zúčastníte se i hledání zařízení na kterém byly takovéto pásky vytvářeny...
(publikováno: 21.07.2004)

http://technet.idnes.cz/hardware.asp?r=hardware&c=A040720_5265162_hardware

Vondruška, P. : **Záhadná páska z Prahy (2. díl - Rozluštění textu)**



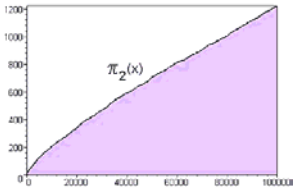
Odhalte s námi tajemství záhadné papírové pásky nalezené v podheldu bývalého Dětského domu v Praze. V předchozí části jsme dospěli k poznání, že děrovaná páska obsahuje šifrovaný text. V dnešním díle se jej pokusíme rozluštit.
(publikováno: 22.07.2004)

http://technet.idnes.cz/hardware.asp?r=hardware&c=A040721_5265232_hardware

Vondruška, P. : **Záhadná páska z Prahy (3. díl - Zařízení)**

K čemu záhadná páska, nalezená ve výklenku Dětského domu, sloužila a na jakém zařízení byla vytvořena? Končí napínavé luštění, kterého jste se mohli zprostředkovaně zúčastnit.
(publikováno: 23.07.2004)
http://technet.idnes.cz/hardware.asp?r=hardware&c=A040722_5265284_hardware

Vondruška, P. : **Červen - měsíc prvočísel**



Svět prvočísel (a s jistou nadsázkou celý náš svět) se od května do června 2004 výrazně změnil. Bylo oznámeno nalezení nového největšího známého prvočísla, pak následovalo překvapující oznámení o vyřešení otázky počtu prvočíselných dvojčat, byla vyřešena Riemannova hypotéza.
(publikováno: 30.06.2004)
http://technet.idnes.cz/sw_internet.asp?r=sw_internet&c=A040622_5263958_sw_internet

Vondruška, P. : **Hackeři, Crackeři, Rhybáři a Lamy? (1. díl)**

Článek se zabývá pojmenováním skupin, které souvisí s počítačovou kulturou současné generace a s kriminálními činy, které se v kybersvětě rozšířily. První část se zabývá výkladem pojmu hacker a otázkou hackerské etiky a kultury. (publikováno: 19.08.2004)
http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040812_5271893_bezpecnost

Vondruška, P. : **Hackeři, Crackeři, Rhybáři a Lamy? (2. díl)**

Druhá část pokračuje popisem skupin, které v kybersvětě provozují nejrůznější druhy kriminální činnosti: cracker, warez, phracker, rhybář. Článek je ukončen výkladem oblíbeného oslovení současné e-generace – lama. (publikováno: 20.08.2004)
http://technet.idnes.cz/bezpecnost.asp?r=bezpecnost&c=A040812_5271894_bezpecnost

Pavel Vondruška, ml. : **Hashovací funkce v PHP**, server PCSvet, rubrika: Programování - PHP, 26.1.2004. Cílem článku je seznámit čtenáře se základy hashovacích funkcí a ukázat, jak je lze využít pomocí knihovny mhash v jednoduchých aplikacích.
http://www.pcsvet.cz/art/article.php?id=4590

Pinkava, J.: **recenze knihy** "*Wenbo Mao: Modern Cryptography, Theory & Practice*" ,DSM 5/2004, http://crypto-world.info/pinkava/clanky/mao.pdf

Pinkava, J**.: recenze knihy** "*Neil Ferguson, Bruce Schneier: Practical Cryptography*", DSM (v tisku), http://crypto-world.info/pinkava/clanky/sneier.pdf

P.Vondruška,D.Bosáková, A.Kučerová, J.Peca : **Elektronický podpis - přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o el. podpisu a výklad základních pojmů**, ANAG 2001, http://www.crypto-world.info/kniha/
Poznámka: V červnu 2004 bylo po dohodě s nakladatelstvím ANAG povoleno volné šíření knihy.

Další články (dostupné zatím pouze v písemné podobě)

Vondruška,P.: **Rozjímání nad PKI**, Data Security Management, DSM 5/2004, Praha
Management Summary **:** Autor článku se zamýšlí nad současným vnímáním PKI ve společnosti, nad některými vybranými problémy, které jeho nasazení doprovázejí. Píše, že všeobecně očekávaný boom se nekonal a snaží se poukázat na některé možné příčiny tohoto stavu. V závěru poukazuje na některá aktuální fakta popisující nasazení PKI ve světě. Vyjadřuje přesvědčení, že se najde komerční využití, které dokáže zajistit PKI návratnost investic.

Vondruška,P.: **Entrust není jen vzdálený přístup nebo zabezpečená pošta**, Zpravodaj 10/2004, Praha

Rosa,T.: **Nepopiratelnost digitálních podpisů**, Data Security Management, DSM 5/2004,
Článek se zabývá problematikou digitálního podpisu jakožto základního stavebního prvku služeb nepopiratelnosti podle norem ISO/IEC 13888 a ISO/IEC 10181-4. Cílem je představit vybrané kryptologické aspekty, které úzce souvisí s konstrukcí služeb nepopiratelnosti vyšší úrovně (nepopiratelnost odeslání či doručení zprávy atp.), a vyzdvihnout aktuální problémy.

B. Přednášková činnost

P.Vondruška: http://crypto-world.info/vondruska/index.php
V.Klíma : http://cryptography.hyperlink.cz/
T.Rosa: http://crypto.hyperlink.cz/

Přednášky na MFF UK
(Úvod do klasických a moderních metod šifrování ALG082)
http://adela.karlin.mff.cuni.cz/~tuma/nciphers.html

Vlastimil Klíma: **Základy moderní kryptologie - Symetrická kryptografie I**. (nové myšlenky kryptografie, bezpečnostní cíle, kryptoanalýza, typy kryptografických systémů, kryptologie), MFF UK, prosloveno v rámci přednášek oboru "Matematické metody informační bezpečnosti", 5.3.2004
http://adela.karlin.mff.cuni.cz/~tuma/nciphers/Symetricka_kryptografie_I.pdf

Vlastimil Klíma: **Základy moderní kryptologie - Symetrická kryptografie II**. (symetrická kryptografie, proudové a blokové šifry, DES, EAS), MFF UK, prosloveno v rámci přednášek oboru "Matematické metody informační bezpečnosti", 12.3.2004
http://adela.karlin.mff.cuni.cz/~tuma/nciphers/Symetricka_kryptografie_II.pdf

Vlastimil Klíma: **Základy moderní kryptologie - Symetrická kryptografie III.** (operační mody blokových šifer a hašovací funkce), MFF UK, prosloveno v rámci přednášek oboru "Matematické metody informační bezpečnosti", 19.3.2004
http://adela.karlin.mff.cuni.cz/~tuma/nciphers/Symetricka_kryptografie_III.pdf

Tomáš Rosa: **Asymetrická kryptografie I**, MFF UK, prosloveno v rámci přednášek oboru "Matematické metody informační bezpečnosti", 2.4.2004
http://adela.karlin.mff.cuni.cz/~tuma/nciphers/mff-ls04-asym1.ppt

Tomáš Rosa: **Asymetrická kryptografie II**, MFF UK, prosloveno v rámci přednášek oboru "Matematické metody informační bezpečnosti", 9.4.2004
http://adela.karlin.mff.cuni.cz/~tuma/nciphers/mff-ls04-asym2.ppt

Tomáš Rosa: **Kvantová kryptografie**, MFF UK, prosloveno v rámci přednášek oboru "Matematické metody informační bezpečnosti", 21.5.2004
http://adela.karlin.mff.cuni.cz/~tuma/nciphers/qc_uvod_v2.ppt

Pavel Vondruška.: **Elektronický podpis**, MFF UK, prosloveno v rámci přednášek oboru "Matematické metody informační bezpečnosti", 16.4.2004
http://adela.karlin.mff.cuni.cz/~tuma/nciphers/elektronicky_podpis.pdf

Pavel Vondruška: **Standardy a normy**, MFF UK, prosloveno v rámci přednášek oboru "Matematické metody informační bezpečnosti", 23.4.2004
http://adela.karlin.mff.cuni.cz/~tuma/nciphers/standardy_normy-1.pdf

Seminář - Bezpečnost Informačních Systémů v praxi
MFF UK Praha (Malostranské náměstí)
http://bis.modry.cz/

Klíma, V.: **Hashovací funkce MD5 a čínský útok**, MFF UK, prosloveno v rámci semináře „Bezpečnost informačních systémů v praxi“, 22.11.2004
Během velmi přednášky byly představeny základní myšlenky dnešních běžně používaných hashovacích funkcí, jejich slabá místa, ale i nedávno prezentovaný "čínský útok" a důsledky z něj plynoucí http://bis.modry.cz/index.php?page_name=historie&article_id=5
prezentace v powerpointu
(http://cryptography.hyperlink.cz/2004/Hasovaci_funkce_a_cinsky_utok_MFFUK_2004.ppt) (a v pdf http://cryptography.hyperlink.cz/2004/Hasovaci_funkce_a_cinsky_utok_MFFUK_2004.pdf), text bez Kelsey-Schneierova doplňku, viz (http://cryptography.hyperlink.cz/2004/cinsky_utok_a_hashe.pdf).

Vondruška,P.: **PKI ... aneb jak to funguje a jak by to fungovat mělo…**, MFF UK, prosloveno v rámci semináře „Bezpečnost informačních systémů v praxi“, 13.12.2004
http://crypto-world.info/vondruska/prezentace/mff_13_12_04.ppt

C. Vybrané prezentace (konference, semináře)

P.Vondruška: http://crypto-world.info/vondruska/index.php
V.Klíma : http://cryptography.hyperlink.cz/
T.Rosa: http://crypto.hyperlink.cz/
J.Pinkava: http://crypto-world.info/pinkava/index.php

Vlastimil Klíma: **Útoky na šifru HBB**, Mikulášská kryptobesídka (http://www.tns.cz/kryptobesidka/), 6. - 7. prosinec 2004, Hotel STEP, Praha.

Vlastimil Klíma: **Nedůvěřujte kryptologům**, IT & Security Conference (http://www.dcd.cz/09_sec.htm), DCD Publishing, Hotel Diplomat, Praha, 10. - 11. 11. 2004
Nové kryptologicko-bezpečnostní paradigma: prolomení některé kryptografické techniky by mělo být chápáno jako zákonitý důsledek vývoje v této oblasti

Rosa, T.: **(Ne)popiratelnost digitálních podpisů**, Universita Palackého, 7. října, Olomouc, 2004, http://crypto.hyperlink.cz/files/rosa_upol04.pdf

Rosa, T.: **Nepopiratelnost digitálních podpisů**, ve sborníku 2. pedagogicko-vědecké konference Právní regulace společnosti informačních sítí, Západomoravská vysoká škola, Třebíč, 27. září 2004
Příspěvek se věnuje problematice digitálního podpisu jakožto základnímu stavebnímu prvku služeb nepopiratelnosti podle norem ISO/IEC 13888 a ISO/IEC 10181-4. Zatímco otázkám konstrukce robustních důkazů o nepopiratelnosti vybraných událostí je v uvedených normách věnována relativně velká pozornost, tak otázce nepopiratelnosti samotného dílčího aktu provedení operace podpisu v použitém podpisovém schématu už tak silná pozornost věnována není. Ještě menší pozornost pak bývá věnována tomu, jestli charakteristiky, které se pod pojmem nepopiratelnost studují v oblasti kryptologie, jsou právě tím souborem vlastností digitálních podpisů, který je bezpečnostními architekty implicitně předpokládán ve standardech uvedeného typu. Naším cílem je představit zde vybrané kryptologické aspekty digitálních podpisů, u kterých je reálný předpoklad úzké souvislosti s konstrukcí služeb nepopiratelnosti vyšší úrovně (nepopiratelnost odeslání či doručení zprávy, atp.).
přednáška: http://crypto.hyperlink.cz/files/rosa_ZMVS04.pdf
prezentce : http://crypto.hyperlink.cz/files/rosa_zmvs04_predn.pdf

Rosa, T.: **Bezpečnostní politika – dokument mnoha tváří a účelů**, IT Security 2004, pořádáno Institute for International Research, Wien (http://www.iir.at/)
Cílem je uvést všem notoricky známou problematiku bezpečnostní politiky alternativním způsobem a představit v něm politiku jako formální nástroj s matematicky uchopitelnými a zpracovatelnými vlastnostmi. Výsledek má bezpečnostní manažery a ostatní čtenáře motivovat k samostatnému zamyšlení nad tím, jak také lze přistupovat k bezpečnostní politice.
Příspěvek byl se stejným cílem prezentován i na semináři IT Governance: **Pokročilé přístupy k řízení a správě informatiky**, pořádaném asociací ISACA (http://www.isaca.cz/).
prezentace: http://crypto.hyperlink.cz/files/rosa_bpol_1.1.zip

Mikulášská kryptobesídka 2004 (MKB)
6.12.- 7.12.2004, Mezinárodní workshop (http://www.tns.cz/kryptobesidka)
Hotel STEP, Praha
Panelová diskuse: Archivace dokumentů - bezpečnost a kryptografie
Účastníci: Pinkava, Smolík, Zajac - moderátor Vondruška
http://crypto-world.info/vondruska/prezentace/mkb_07_12_04.ppt

PKI 2004 - realizácia elektronických podpisů v praxi
11.11.2004, Hotel Holiday INN,Bratislava
link na konferenci:
http://www.tempest.sk/index/podstranka.php?id=25&idm=0&&idf=&modul=9&param1=0&topbut=6&param2=37&lang=sk
Vondruška,P. : **Můstková certifikační autorita** (Bridge Certification Authority)
prezentace : http://crypto-world.info/vondruska/prezentace/pki_11_11_04.ppt

Elektronický podpis - kľúč k moderným elektronickým službám
19.4.- 20.4.2004, Mezinárodní konference
Hotel Plejsy, Krompachy, Slovesnko
přednáška :
Vondruška,P., Sekera,T. : **Zkušenosti s budováním komerční certifikační autority na bázi Entrust a navázání vztahu důvěry s ostatními subjekty PKI**
přednáška :
Vondruška,P.: **Navázání vztahu důvěry mezi certifikačními autoritami**
http://www.e-unicom.sk/konferencia/

Pinkava, J. : **Elektronický podpis**, předneseno na PEF MZLU Brno 12.10.2004.
Prezentace: http://crypto-world.info/pinkava/prezentace/epodpis.ppt

D. Soutěž 2004

http://soutez2004.crypto-world.info/index.php

V roce 2004 poběhla pro čtenáře e-zinu Cypto-World již tradiční soutěž v luštění jednoduchých šifrových úloh

Úlohy, komunikace s řešiteli : **P.Vondruška**
Tvorba stránky soutěže: **P.Vondruška, jr.**

Napsali o soutěži 2004
(13.9.2004), root.cz - Crypto-World: český web věnovaný kryptologii++,
(http://www.root.cz/clanek/2396)
(15.9.2004), Crypto-World 9/2004 - Soutěž v luštění 2004 začala !
http://crypto-world.info/casop6/crypto09_04.pdf
(16.9.2004), Technet.idnes.cz - Luštěte šifry a setkejte se s kryptology, nebo whisky
(http://technet.idnes.cz/zprava.html?zprava=29824)
(16.9.2004), Pooh.cz - Luštění šifer http://www.pooh.cz/a.asp?a=2010665
(16.9.2004), Československý DX Klub - Tradiční podzimní soutěž v luštění jednoduchých šifrových úloh začala... http://www.dx.cz/
(11.10.2004), Pooh.cz - Luštění šifer, dějství druhé
http://www.pooh.cz/cybercave/a.asp?a=2010841
(15.10.2004), Crypto-World 10/2004 - Soutěž v luštění pokračuje druhým kolem !
http://crypto-world.info/casop6/crypto10_04.pdf
(14.11.2004), Crypto-World 11/2004 - Soutěž 2004 - úlohy závěrečného kola!
http://crypto-world.info/casop6/crypto11_04.pdf
(16.11.2004), Pooh.cz - Soutěž v luštění šifer již zná svého vítěze!
http://www.pooh.cz/cybercave/a.asp?a=2011127
(19.12.2004), **Crypto-World 12/2004 – celé číslo věnované soutěži, řešení úloh**, postřehy řešitelů
http://crypto-world.info/casop6/crypto12_04.pdf

E. Crypto-World – 2004

http://crypto-world.info/index2.php

Crypto-World 1/2004

Crypto-World 2/2004

Crypto-World 3/2004

Crypto-World 4/2004

Crypto-World 5/2004

Crypto-World 6/2004

Crypto-World 78/2004

Crypto-World 9/2004

Crypto-World 10/2004

Crypto-World 11/2004

Příloha : Crypto-World 11/2004 – speciál (24 stran)
(V.Klíma : Nedůvěřujte kryptologům, ke stažení na adrese :
http://crypto-world.info/index2.php?vyber=casop6)

Crypto-World 12/2004

Redakce 2004

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.

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@pvt.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/