Crypto-World

Informační sešit GCUCMP

Ročník 6, číslo 10/2004 **15. října 2004**

10/2004

Připravil: Mgr. Pavel Vondruška

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

Obsah :

Informace:

Kolektiv kolem Crypto-Worldu (kompletní seznam viz F.Závěrečné informace) byl rozšířen o Jakuba Vránu, který přislíbil od nynějšího čísla udělat konec hrubkám a překlepům. Děkujeme za pomoc! Doufám, že práce dalšího dobrovolníka tak přispěje k vaší větší pohodě při čtení e-zinu.

A. Soutěž v luštění pokračuje druhým kolem!

Mgr. Pavel Vondruška, pavel.vondruska@crypto-world.info

Přesně před měsícem odstartovala tradiční soutěž v luštění jednoduchých šifrových úloh zveřejněním deseti úkolů prvního kola. Příjemným překvapením byl zájem soutěžících. Během první hodiny se jich zaregistrovalo více jak třicet! Osobně mě nejvíce překvapil výkon soutěžícího, který se zaregistroval pod označením ***misof.*** Kódy pro registraci do soutěže jsem rozesílal ve středu 15.9.2004 v 17:39. Soutěžící ***misof*** vyřešil všechny úlohy tohoto kola ani ne za hodinu a půl od rozeslání kódů (správný výsledek desáté úlohy ověřil již v 18:56)! I když úlohy tohoto kola nejsou příliš těžké a jsou pouze variacemi na známé téma (proto také symbolické označení sady úloh 1-5 jako **skautský tábor** a sady úloh 6-10 jako **úlohy pro připravené**), přesto je takovýto výsledek hodný obdivu. Upřímně blahopřeji!

Druhé kolo soutěže bylo zahájeno v sobotu 9.10.2004 v 19:00 hod. zveřejněním čtyř úloh z nichž dvě jsem označil jako **úlohy pro připravené** a zbylé jsou ze sady, kterou jsem pracovně nazval **úlohy pro luštitele.** Ulehčím vám práci a prozradím, že se jedná o klasickou jednoduchou transpozici a jednoduchou záměnu. Informace o dostupnosti úloh druhého kola byla uvedena v **NEWS** na stránce našeho Crypto-Worldu. Řešitelé prokázali, že NEWS sledují, protože již ve 20:57 soutěžící Lama vyřešil prvou ze zveřejněných úloh a během sobotního večera jej následovalo dalších šest soutěžících. První úloha druhého kola (označena 2/1) je opravdu lehkou úlohou, která má, obdobně jako úvodní úloha z prvého kola (označena 1/1), spíše „náborový“ charakter. V okamžiku psaní tohoto příspěvku (10.10 večer) ji vyřešilo již jedenáct soutěžících.

Zveřejněné úlohy odolaly vyřešení déle než úlohy prvého kola. Všechny zveřejněné úkoly druhého kola vyřešil jako prvý soutěžící registrovaný pod jménem ***vn***. Úlohy dokázal prolomit do neděle 10.10. - 17:28 a dosáhl jako první zatím maximálního možného počtu 25 bodů.

Poslední úloha druhého kola je zveřejněna současně s rozesláním kódů ke stažení tohoto e-zinu a uvedena také v příloze k tomuto úvodnímu článku.

Zbývající úlohy (úkoly označené jako úkoly třetího kola) budou zveřejňovány po jedné a to průběžně během následujícího měsíce. O jejich zveřejnění může, ale nemusí (!) být informace v NEWS. Tyto úlohy budou patřit již do kategorie **úlohy pro luštitele** a měly by odolat analýze vždy po dobu několika hodin.

Informace *pro zvídavé*: chcete-li vědět, v jakém pořadí jste Vy nebo vaši soupeři řešili jednotlivé úlohy, nebo které úlohy řešiteli ještě chybí, můžete to jednoduše zjistit takto:

- vstupte na stránku soutěže http://soutez2004.crypto-world.info/
- zvolte v horním menu sekci ***zebricek***
- vyhledejte uživatele, o kterém chcete získat informaci
- podržte myš na jeho jménu
- cca za jednu vteřinu se v informačním okně objeví pořadí úloh, ve kterém je zvolený uživatel řešil
- snadno si z této informace odvodíte, které úkoly ještě řešitel nerozluštil

Přehled úkolů - II.kolo

Talent dělá, co může – génius, co musí. (O. Wilde)

Skupina úloh - *„pro připravené“ (část 2)*

Steganografie (2/1)
Počet bodů: 2
Nápověda: úloha je uvedena pouze pro úplnost. Řešit ji je nutné přímo na www stránce.

```
TATOU LOHAP ATRIM EZISP ISELE HKE.U KOLEM JEOPE TNALE ZTSLO VOKTE
RYMPR OKAZE TEZEJ STEJI VYRES ILI.T ENTOK RATEN ENISL OVOZA SIFRO
VANO, ALEUT AJENO JEDNO DUCHO USTEG ANOGR AFICK OUMET ODOU. NEVIM
ZDANA POVIM ,ALET ATOUL OHANE BUDEV CRYPT
O-WOR LDU10 /2004 UVEDE NA(PR OC?).
```

Kódová kniha, II.světová válka (2/2)
Počet bodů: 2
Nápověda: HBO, léto 2004

BAH-HAS-TKIH BE-SO-DE-DEZ-AHE BESH-LEGAI-NAH-KIH YAH-DI-ZINI NI-DAH-THAN-ZIE IL-DAY A-WOH NE-AHS-JAH BE-TAS-TNI NE-AHS-JAH AH-LOSZ DAH-NES-TSA A-KHA GLOE-IH BE-SO-DE-DEZ-AHE NE-ZHONI WOL-LA-CHEE DIBEH KLESH GLOE-IH TLO-CHIN GAH BE SEIS TSAH TSE-NILL A-KEH-DI-GLINI BE-LA-SANA YIL-DOI NE-AHS-JAH

Skupina úloh - *„pro luštitele“ (část 1)*

Jednoduchá transpozice (2/3)
Počet bodů: 3
Nápověda: Jednoduchá transpozice, Crypto-World 11/2000, str. 2-6

```
EDUUC NHCRE RNDCO VSYRT ARJIZ EKOKL VDNEJ PHIYI EOAYE EZNEZ EDLEL ZNSZM
BNDRI JEOZU SMSDN AANVE PNARN EISAS YDYSE EOZNC CSEOR AWIOY IEYCS BKUIT
VARIE ONSEE ETEOP BTOVE TAZET RXURH ROEVZ ZORDB POINE YSSTD WMPVE DANSV
OVSEZ PEEIT PBOIT PEYID LEDMM EAOTJ NNJZP YMDYE ASONT TTSVL EUIPI BUAIN
REAEN AIRUI VZTID EVIAE HONUO VWPVH HLSAD OEZOI YVHEU ODARE LUOTU EATOS
DDEPN NTEVY UGERL RCEOC (320)
```

Jednoduchá záměna (2/4)
Počet bodů: 3
Nápověda: Jednoduchá záměna, Crypto-World 10/2000, str. 2-4

```
GDCPB BDXNC EXDGR AQVXF IDVZP CEBPW PTWKL SIQWL QLPVQ WPZPG QVXDB QZDAP
SRAQV XFVMN WMARA QVXFR QZZQD YULDI WVVPV NEKLD SNECS NEVXZ PIQMP XXWPL
PBVNE LEMIP SFLNH PIFSP VXZDL IPXWP LDVPV KPMQD ZQGEB PIDAQ VWNLQ MXPLP
KZQXF WFWNV XZPIX FIDRA QVXFB VNEQI VKQLN SDIPL PIPVD IMIQY VXZPY MPIFG
QVXDB QQCDZ VQWLQ ZEVWQ WPZPX WPLQH ECNES FZNVN SDIQG WPMAX WPLQC NVDAZ
QDZPV KNIKD WIDMW HNCES WNYWN KLQKD CPVPM PIDVX ZDCDN KPWGZ DASPR AQVXF
VWPBI PGIDM XFDZP CNKZI PIDHE CPKNE GPBPC INEVX ZPIXN EIDRA QVXFT (415)
```

Periodické heslo, Vigenere (2/5)
Počet bodů: 3
Nápověda: Substituce složitá - periodické heslo, srovnaná abeceda, Crypto-World 12/2000, str. 4-10

```
TEMYY IPVWT MPYYT OPIDR UXQKE MLEDO OXDAX IWCIZ ZEQHD KFREA QVDIZ NZKZI
ZHHGH RIAGI TPVBA ZAREP PTQJS UZULE RRRYU SOHXO ZOYWA UGPVV BUYZI AGGPE
XVDFQ MMPPZ DEXVP UEVIG ITQVM QQZQL RLHGN INNSB WUGUG TUCLH ASDTM XIFPY
GULBM CIGDZ QRMAR KPNYB JKFZT EIBGZ ZRZKV NMYIY HEXBD KLDVN DUFNM PSKAR
KNVOL AGREN AVTNB KWVIF DKFOZ LLKZZ IAVGH ERXWB QPSQT KIHSC IZDIS GZGHY
ZAQZD NMZDF PUGUM SWNIW KGETI WAOYP VVKOZ AQFUX FIZEW FHONB DEOHW GIZQC
LBBKH RIAMU TNICZ OYIXV DTQZF HLUHA RRAVA REXGA HNMGZ ITAXE VEOHS OGJXI
RRUGV IGNAZ AARVW JHOHX WADEX RHQKJ IQWBM TCQGS BRSGW BALRR AZAUT NSKET
VBXAM URVSG ATZBZ KYVIF BXQSI MXXMV EBLNM DYWMF QRSPV KFAOG WFQMV RSUXE
QWMJZ OLBUO XISAC RUDMA IBKSS XMAYR XAWYF IQNAB GJTBL OXZIW UKZAT BCFUV
EAMVQ VRRXG XIZBA ZAVOL UOXIS ACRUD MFBGX ETBCF UVEWQ FQJQR VGPRI IWATL
MNAAE ERLBX GSLBA VADEE AQKCL MDODA XQCQM ZVRAK ZINRA RAVSF KNDEF VCY
```

Pro úplnost opakuji, že po vyřešení úlohy naleznete v otevřeném textu klíčové slovo, kterým prokážete, že jste úlohu správně vyřešili. Pokud jste zaregistrováni, přihlásíte se jednoduše ke svému účtu a přes www rozhraní jej u příslušné úlohy zadáte. **Toto slovo pište vždy velkými písmeny a bez mezer !**

Všem soutěžícím přeji příjemnou zábavu !

Průběžná statistika soutěže (10.10.2004, 23:59)

Celkem soutěžících:	**82**
Počet soutěžících, kteří vyřešili alespoň 1 úlohu:	67
Počet soutěžících, kteří splnili podmínku k zařazení do slosování o ceny:	26
Nejvyšší počet dosažených bodů:	25
Celkem již publikovaných úloh:	14
Maximální počet bodů, které lze prozatím dosáhnout:	25

V průběžném hodnocení vedou tito soutěžící:

1.	***vn***	**25 bodů**	**/10.10 (17:28)**
2.	***peta007***	25 bodů	/ 10.10 (22:38)
3.	***mutant_mouse***	24 bodů	/ 10.10 (21:33)

Aktuální statistika je k dispozici na stránce soutěže:
http://soutez2004.crypto-world.info/index.php?crypto=statistika

B. Rozjímání nad PKI

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

(Informace: ve zkrácené verzi vyjde tento článek v DSM 5/2004.)

„Lid v celém království je pijácký, obžerství oddaný, pověrčivý a chtivý novot.“ E.S. Piccolomini: České dějiny.

Úvodní citát pochází od Eneáše Silvia Piccolominiho (1405-1464), známého spíše jako papež Pius II. Dobře znal české poměry, jeho knihy byly silně protihusitské, ale dílo, které sepsal, rozšířilo husitské myšlenky do celé Evropy a mělo tak zcela opačný účinek než původně zamýšlel.

Proč se o něm a jeho díle zmiňuji? Přál bych si, aby kritika PKI, které je věnován tento článek, působila obdobně jako jeho kritika husitství – tj. aby v konečném důsledku vedla k zájmu o PKI a k jeho šíření, nikoliv k jeho zatracení.

Jak je známo, PKI je zkratka anglického výrazu *Public Key Infrastructure*, nebo-li chcete-li, česky *infrastruktura veřejného klíče*. Odpověď je ve skutečnosti komplikovanější, neboť v současnosti neexistuje jednoznačná definice. Odborníci na informační technologie se shodují, že to není pouze správa klíčů, jak by se mohlo zdát překladem termínu PKI, ale že to je mnohem více.

Pro potřeby tohoto článku použijeme tento výklad: *„PKI je kombinace znalostí, soubor představ, dohod, konvencí, speciálního hardware a software, aplikací, které výhody PKI využívají, standardů, norem, prováděcích směrnic, legislativy a dotčených osob.“* Podívejme se proto na některé vybrané detaily z tohoto rozsáhlého souboru samostatných a různorodých témat.

V posledních pěti letech je PKI vděčné téma. Nešlo si prostě nevšimnout jeho počátečního bouřlivého nástupu, pak přešlapování a nyní jakéhosi stavu očekávání věcí příštích. Za začátek boomu (alespoň legislativního) lze označit rok 1999, kdy v Evropské unii byla schválena Směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy, v roce 2000 v ČR vstoupil Zákon o elektronickém podpisu č.227/2000 Sb., v roce 2002 byla udělena první akreditace a bylo zahájeno vydávání kvalifikovaných certifikátů.

V letech 2001-2002 byly také postupně schváleny některé další právní předpisy, které umožňují konkrétní využití elektronických podpisů v různých agendách a situacích (komunikace v oblasti veřejné moci, elektronické podatelny, daňová přiznání, žádosti o sociální podporu, vedení zdravotnické dokumentace, podávání některých speciálních hlášení). Pokud jde o budování certifikačních autorit jako jednoho ze základních stavebních kamenů PKI, zavládl proto v období 2000 – 2002 mezi firmami lehký optimismus a byla zahájena výstavba několika rozsáhlých systémů a to jak interních, tak i externích. Náklady na výstavbu jsou relativně vysoké a lze předpokládat, že „business case“ jednotlivých projektů byl těžko naplněn. Proč? Počet prodaných certifikátů není příliš velký a uživatelé, kteří certifikáty vlastní, mají jen málo příležitostí je smysluplně využívat. Obecně se zdůrazňuje, že chybí aplikace, která by rozhýbala trh s prodejem certifikátů. Důvody, proč si uživatelé certifikáty (především kvalifikované certifikáty) pořizují, si dovoluji nazvat fandovstvím. O něco lepší situace je při využívání certifikátů uvnitř společností. Zde se zpravidla vydávají certifikáty na základě schválené bezpečnostní politiky organizace a jsou vhodnou metodou, jak zajistit bezpečnost a důvěrnost přenášených informací, autentizaci a autorizaci k podnikovým aplikacím a systémům.

Stále však panuje určité nepochopení principů zákona o elektronickém podpisu a veřejnost a často i manažeři IT nepříliš dobře interpretují, kdy je nutné používat určité typy certifikátů, kdy je potřeba používat certifikáty od akreditovaného poskytovatele a kdy ne. Přitom jsou situace, kdy dokonce kvalifikované certifikáty používat nelze – ty jsou určeny pouze pro ověřování zaručených elektronických podpisů a nelze je tedy použít pro šifrování nebo autentizaci uživatele.

Podnikatelé nevyužívají dostatečně možnosti, které se zákonem o elektronickém podpisu otevřely. Dívají se na tuto komunikaci stále jako na něco podezřelého a bojí se ji standardně využívat.

Začátkem léta 2004 nabyla účinnosti novela zákona o elektronickém podpisu (č. 440/2004 Sb.) [1]. Novelu hodnotím velmi kladně, protože řeší některé důležité otázky pro praxi. Zavádí pojem *kvalifikované časové razítko*, které umožní prokazovat existenci elektronického dokumentu v čase. Další novinkou je možnost používat *elektronické značky*. Toto ustanovení by mělo umožnit např. vydávání elektronických listin státní správou (např. výpisů, osvědčení aj.), které by byly ekvivalentem papírových dokumentů.

Novela je však především pokus o vytvoření podmínek pro komunikaci *občan–stát* a naplňování vize, kterou předložilo při různých příležitostech MIČR i osobně ministr Vladimír Mlynář. Domnívám se, že to, co v ČR chybí, není legislativa, ale především velká komerční aplikace, která by rozhýbala trh s prodejem a použitím certifikátů.

Bankovní sektor je speciální oblast, kde využití PKI je již relativně dobře zvládnuto. Je to ovšem tím, že pracuje poněkud „proti obecné filosofii PKI“ – tedy využití třetí důvěryhodné strany v komunikaci uživatele (klient) se subjektem spoléhajícím se na podpis (banka). Třetí stranou není nezávislá certifikační autorita, ale zpravidla certifikační autorita banky.

Ještě stále nejsou vyřešeny některé problémy, které ztěžují nasazení resp. využití mimo bankovní a „státní“ sektor. Není dořešena otázka bezpečné úschovy elektronicky podepsaných dokumentů, protože chybí jednotný mezinárodně uznávaný standard, který by tento problém řešil, a tato úschova (méně vhodné je používat slovo archivace) není ani legislativně upravena. Dále je to nedostupnost prostředků pro bezpečné vytváření a ověřování elektronického podpisu, tím se míní prostředky, které splnily požadavky příslušné prováděcí vyhlášky, nikoliv tak označené výrobcem nebo dodavatelem… Obecně je to dále nedostupnost vhodných komponent PKI, stále jsou problémy s kompatibilitou, nedořešeny jsou otázky hodnocení těchto prostředků a v řadě případů je to jejich vysoká cena.

Problém je i v nastavení vztahu důvěry mezi jednotlivými certifikačními autoritami. Jde o zajištění bezpečné a důvěryhodné komunikace uživatelů, kteří mají vydané certifikáty od různých autorit. Řešením by mohlo být vybudování můstkové certifikační autority v ČR (Bridge Certification Authority).

Ve světě se k tomuto řešení již přistupuje, jednou z největších a nejznámějších je můstková autorita v USA – The Federal Bridge Certificate Authority (http://www.bridge-ca.org/), která spojuje řadu významných a rozsáhlých PKI. V Evropě je v komerční sféře známa můstková autorita European Bridge-CA (http://www.bridge-ca.org/). Pro státní správu byl v EU zahájen projekt můstkové certifikační autority IDA (http://europa.eu.int/ISPO/ida/).

Jak to vypadá s nasazením PKI ve světě? Začátkem srpna FBI a CSI publikovaly výsledky průzkumu počítačové kriminality a bezpečnosti 2004 [2]. Interní PKI je podle tohoto průzkumu využíváno jen ve 30 % firem.

Podle právě zveřejněné studie (27.8.) *IT Security Market Report 2004* [3] se zvýšil trh s bezpečnostními produkty a službami v oblasti informačních technologií za rok 2003 o čtvrtinu proti roku 2002. Investice do PKI se však v posledních letech nezvyšují.

I přes řadu popsaných problémů jsem optimista. PKI je z hlediska technologie velice perspektivní, řeší komplexně řadu otázek interní bezpečnosti, jeho potenciál je obrovský. Věřím, že se najde komerční využití, které dokáže zajistit návratnost nutných vysokých investic a které umožní levně využít všechny možnosti tohoto fenoménu posledních let.

Mezi základní stavební kameny PKI patří Certifikační autority (dále jen CA)

Podívejme se dále proto, jak stručně charakterizuji ty nejznámější a jakou bych v případě známkování udělil známku.

První certifikační autorita, a.s. (http://www.ica.cz/)
Vlastník: Česká spořitelna, a.s., Československá obchodní banka, a.s., Eurotel, s.r.o., PVT, a.s., Státní tiskárna cenin s.p.
Komentář: Bezesporu nejznámější a nejvýznamnější certifikační autorita v ČR. Je zatím stále jedinou akreditovanou CA v ČR. Vydává kvalifikované i komerční certifikáty. Zavedla službu vydávání časových razítek. Podílí se na vydávání kvalifikovaných certifikátů na Slovensku. Vydala a spravuje zdaleka největší počet certifikátů v ČR. Disponuje velkou řadou kvalifikovaných odborníků.
Známka: 1 (*Cizí vady máme pře očima, vlastní za zády. Seneca*)

Certifikační autorita TrustPort (http://www.trustport.cz)
Vlastník: AEC, s.r.o
Komentář: V roce 2000 společně s I.CA nejvýznamnější CA. Vysoce hodnotím jejich software pro koncového uživatele, zavedení asymetrické kryptografie založené na eliptických křivkách, kvalitní certifikační politiku (jednu z prvních u nás, která vycházela z doporučení RFC 2527). CA sehrála důležitou úlohu v prosazování myšlenek využití elektronického podpisu (konference Security, Roadshow atd.). Zavedla službu vydávání časových razítek. Postavení, které měla v roce 2000, však postupně ztrácí.
Známka: 2-3 (*Zbytečná skromnost chudému škodí. Homér*)

Certifikační autorita Globe Internet, s.r.o. (http://www.ca.cz, http://www.certifikacniautorita.cz)
Vlastník: Active ISP ASA
Komentář: CA se řadí mezi ostřílené hráče na našem trhu. Podle mne však stále přešlapuje a přemýšlí a přemýšlí… Líbí se mi jejich čtyřdílný seriál o zavedení elektronického podpisu a využití elektronické fakturace. Nelíbí se mi jejich současná certifikační politika (nikoliv obsahem, ale protože není napsána podle standardu RFC). Nový vlastník pravděpodobně prioritu v této aktivitě nevidí.
Známka: 3 (*S rozumem najdeš i ztratíš. Skotské přísloví.*)

Certifikační autorita CA Czechia (http://www.caczechia.cz/)
Vlastník: Zoner software, s.r.o.
Komentář: CA, která se snaží jít s dobou (v dobrém slova smyslu). Osobně velice oceňuji jejich volně šiřitelný program pro stahování seznamu zneplatněných certifikátů - CRLManager. Líbí se mi jejich webová stránka, je přehledná a užitečná.
Známka: 3 (*Kdo by měl rád to nestoudné a drzé mládí? Cicero*)

Interní certifikační autorita ČESKÝ TELECOM a.s. (http://www.intca.ct.cz/)
Vlastník: ČESKÝ TELECOM, a.s.
Komentář: CA je postavena podle velice přísných bezpečnostních norem. Vydává osobní certifikáty pro zaměstnance a externí spolupracovníky a certifikáty pro SSL komunikaci. Certifikáty jsou ověřitelné i mimo společnost. Před realizací je projekt budování Můstkové certifikační autority v ČR.
Známka: 2-3 (*Každý sám nejlíp ví, kde ho střevíc tlačí. Plutarchos*)

PostSignum (http://www.postsignum.cz, http://www.ceskaposta.cz/sluzby/)
Vlastník: Česká pošta, s.p.
Komentář: Spící medvěd, který by po probuzení mohl sehrát důležitou úlohu v rozvoji PKI v ČR. Umím si představit, že právě zde by mohla vzniknout komerčně zajímavá aplikace, která by mohla rozhýbat zájem o certifikáty.
Známka: 3-4 (*Ani růst vousů neuspěcháš. Indické přísloví*)

eIdentity, a.s. (http://www.eId.cz/, http://www.ie.cz/)
Komentář: Nejmladší ze zde uvedených poskytovatelů certifikačních služeb. Konkrétní řešení bylo převzato od CA KPNQwest. Společnost má ambici vydávat kvalifikované certifikáty. Vzhledem k vývoji legislativy a přísným normám se však domnívám, že k dosažení akreditace čeká tuto autoritu ještě složitá a trnitá cesta. Mnou přidělenou známku ovlivňuje i to, že nevím, kdo odborně „táhne“ tuto autoritu k vytyčenému cíli.
Známka: neklasifikována (*Začátky všech věcí jsou malé. Aurelius*)

Literatura

[1] Úplné znění zákona č. 227/2000 Sb., o elektronickém podpisu (včetně novel č. 226/2002, Sb., č. 517/2002 Sb. a č. 440/2004 Sb.), http://www.micr.cz/files/1540/UZ-227_2000.pdf

[2] CSI/FBI Computer Crime and Security Survey, CSI 2004, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[3] Research and Markets: IT Security Market Report 2004 Aug. 27, 2004, http://www.tmcnet.com/usubmit/2004/Aug/1068560.htm

[4] Vondruška, P.: Vztah důvěry mezi můstkovými certifikačními autoritami, Data Security Management, DSM 6/2003, Praha.

[5] Vondruška, P.: Rozjímání nad PKI, Data Security Management, DSM 5/2004, Praha.

C. Kryptografie a normy
Platnost elektronického podpisu a hledisko času

Jaroslav Pinkava, PVT a.s.

1. Úvod

Tento článek vychází ze zamyšlení nad zdánlivě jednoduchou otázkou. Jak je to vlastně s platností elektronického podpisu? Elektronický podpis je považován za platný, jestliže lze jeho platnost ověřit. To je vcelku pochopitelné a jednoduché tvrzení. Logické je hledat pro toto tvrzení i oporu v zákoně. Český zákon o EP 227/2000 sb. (ve znění pozdějších novel) říká v paragrafu 3.(skromně): "Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu." Ale ani směrnice EU se nijak precizací momentu ověření příliš nezabývá. Nepochybně v tom má i prsty deklarovaná technologická nezávislost. Dost těžko se proto mohla zabývat konkrétními cestami pro ověřování elektronického podpisu. Samozřejmě praxe elektronického podpisu již cesty, kterými ověřování platnosti elektronického podpisu probíhá, vybudovány má. Je však otázkou, nakolik tyto cesty jsou již hotovým řešením a nakolik zde existují problémy dosud neřešené.

2. Ověřitelnost elektronického podpisu

Nejprve však zůstaňme v situacích, kterými se zabývá dnešní praxe elektronického podpisu. Jak postupuji při jeho ověření, tedy ověření platnosti konkrétního elektronického podpisu? Obracím se k platnosti digitálního certifikátu veřejného klíče, který přináleží příslušnému použitému soukromému podpisovému klíči. Tj. zjišťuji (v momentu ověřování) zda období platnosti certifikátu (na něm vyznačené) pokrývá okamžik, ve kterém právě jsem. Fakticky se jedná o to, zda platnost certifikátu již nevypršela, ale teoreticky může být platnost (třeba jen dočasně) pozastavena. Informace obsažené v certifikátu však nejsou k tomuto ověření dostatečné. Mohlo totiž dojít k jeho odvolání (z řady různých důvodů). Musím tedy získat i tyto potřebné informace (CRL, OCSP). Například praxí používanou v řadě případů je, že při převzetí elektronicky podepsaného dokumentu se čeká na následně vydané (z časového hlediska) CRL a teprve pokud zde ověřím, že certifikát nebyl odvolán, konstatuji, že z tohoto hlediska nic nebrání tomu, aby daný elektronický podpis ověřen byl. Ještě je tu však jeden moment, který by se opomíjet neměl. Jako ověřovatel bych měl být i ujištěn, že platí i podpis na certifikátu (příslušné certifikační autority), popřípadě v složitějších situacích ověřit celou tzv. certifikační cestu (např. podpisy nadřízených certifikačních autorit až ke kořenové certifikační autoritě). Provedu-li toto vše, pak jsem skutečně platnost elektronického podpisu ověřil.

Ale - je tu skutečně určité faktické ale. Mohu toto ověřování znova provádět i do budoucna? Může třeba za dvacet třicet let mé postupy zopakovat? A třeba za sto let? Pokud se obrátíme k papírovým dokumentům resp. podepsaným papírovým dokumentům, vidíme, že zde vhodnou analogii nacházíme těžko. Podpis na papírové smlouvě (pokud je důležitá, tak podpis bude i třeba ověřen notářem) lze ověřit i třeba za těch dvacet let. Historicky se dají ověřovat třeba i podpisy na smlouvách, které jsou staré několik století atd. Jak to však bude s

elektronicky podepsaným dokumentem? Digitální certifikát byl autorovi podpisu vydán například na období jednoho roku. Po ukončení platnosti tohoto digitálního certifikátu neexistuje způsob, jak bych příslušný podpis mohl ověřit - nemám proti čemu. Příslušný certifikát již není platný a to ještě je třeba zvážit i situace, kdy majitel certifikátu může požádat o jeho zneplatnění i před ukončením doby platnosti certifikátu. Důvody specifikovat nemusí, běžně je toto umožňováno pro zajištění bezpečnosti elektronického podpisu v situacích, kdy došlo či mohlo dojít ke kompromitaci soukromého podpisového klíče majitele certifikátu (třeba krádeží či ztrátou notebooku, který příslušný soukromý klíč obsahoval).

Dostáváme se tedy k jádru věci. Pokud chceme uschovávat elektronicky podepsané dokumenty (tedy archivovat) a mít možnost tento podpis ověřovat i v budoucnu, pak začínají vznikat určité problémy. Těch problémů může být celá řada.

Uveďme nejprve jednoduchou situaci, která se vlastně ještě ani archivace nedotýká. Přesto je zde otázka času klíčová. Obchodní partner mě zašle objednávku na zboží jím elektronicky podepsanou. A protože si usmyslil, že mě dostane do problémů, příští den nechá odvolat svůj digitální certifikát. Já ještě ten samý den, co byla objednávka odeslána, ověřím elektronický podpis, žádné problémy neshledám a pracně nakoupím vše, co je pro vyřízení objednávky třeba. Za dva dny mám vše připraveno a odesílám zboží partnerovi. Ale tady vznikne zádrhel. Partner prohlásí, že soukromý klíč mu byl odcizen a že proto i odvolal svůj digitální certifikát. Podpis musel vzniknout až po odvolání certifikátu. Záležitost dostanou do rukou právníci. Ale teď se ukáže, že vůbec nemusím mít dostatek důkazů k tomu, abych obhájil svoji pravdu. Klíčem rozhodnutí soudu musí být otázka časového momentu, ve kterém byla podepsaná objednávka odeslána. Já budu tvrdit samozřejmě, že odešla před odvoláním certifikátu. Ale jak to prokázat. Pokud budu argumentovat časem na hodinách počítače, opačná strana namítne, že tento čas se dá snadno zmanipulovat a bude mít pravdu. Já pokud nenajdu - náhodou - nějaká další svědectví, která by moje tvrzení dostatečně potvrdila, mám prostě smůlu a soudní při zákonitě prohraji. Zachránilo by mě, kdybych prokazatelným způsobem mohl říci, že příslušný dokument musel být podepsán v době platnosti odpovídajícího digitálního certifikátu. Důvěryhodné časové razítko - ano, to je to, co jsem potřeboval. Pokud bych byl dostatečně opatrný a (například) partnerovu objednávku bych takovým časovým razítkem opatřil, mám vystaráno a partner nemá šanci uspět se svým podrazem.

Pojem časového razítka se neobjevil ve Směrnici EU o elektronickém podpisu, neobsahoval ho původně ani zákon č.2227/2000 sb. Teprve letošní novela zákona již s tímto pojmem počítá a zavádí pojem kvalifikovaného časového razítka, čímž se rozumí datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem. Je připravována také novela Směrnice EU a ze zachycených diskuzí vyplývá, že pojem časového razítka bude organicky včleněn.

Výše byl uveden případ, kde již samo zavedení a správné použití časového razítka vede k vyřešení příslušného (bezpečnostního) problému. Ale samotné časové razítko není všelék. Co se situacemi, kdy budu potřebovat ověřit platnost elektronického podpisu na dokumentu například pět let starém. Ověřit potřebuji platnost el. podpisu v momentě, kdy byl vytvořen, tedy před těmi pěti léty, ale jak to provést? A dejme tomu, jsem instituce, která ke své činnosti vždy potřebovala archivovat určité dokumenty a mít možnost zpětně jejich platnost ověřovat (například jsem katastrální úřad). A rozhodl jsem se přejít na elektronickou

podobu dokumentů a jejich archivaci. Lze to vůbec? Co k tomu potřebuji je zřejmé - možnost ověřit například i ve vzdálené budoucnosti, že příslušný elektronický podpis byl platný v momentu vytváření tohoto podpisu. Pracovně můžeme takovýto podpis nazvat archivním elektronickým podpisem a načrtnout následující model.

„Historicky" se z hlediska chápání el.podpisu ve vztahu k elektronickým dokumentům dají vydělit 3 etapy (odpovídají tomu také verze českého zákona o EP):

1) elektronický podpis jako fenomén sám o sobě vázaný na platnost certifikátu, podpis nelze ověřit mimo období platnosti certifikátu;
2) elektronický podpis s časovou značkou, podpis lze ověřit v období „platnosti" časové značky (což ale také není věčně); vazba je zde také ale na ověřitelnost certifikátu té CA, která podepsala svým soukromým klíčem certifikát vydaný uživateli.
3) archivní elektronický podpis, platnost časové značky lze (doufejme neomezeně) prodlužovat (například novým „přepodepsáním").

Naše legislativa nejprve odpovídala etapě 1, nyní je v etapě 2 a zatím nepochytila etapu 3. Směrnice EU (protože nová verze stále neexistuje) je ještě stále v etapě 1.

Ale jak tento pojem archivního elektronického podpisu dešifrovat?

Na stránkách Crypto-Worldu ([1], [2]) bylo již otázkám archivace elektronických dokumentů věnováno nemálo pozornosti a to zejména z existujících bezpečnostních pohledů. Existují přístupy, které zejména v poslední době danou problematiku intenzivně rozpracovávají. Zmíněny byly připravované dokumenty skupiny *ltans* směrované konkrétně na problematiku digitálních archivů. Dále existují dva dokumenty pracovní skupiny ETSI (viz níže), které rozpracovávají formáty elektronických podpisů takovým způsobem, aby byly pro archivaci využitelné.

Je třeba však zmínit, že ve světě již celá řada digitálních archivů funguje a existují rozpracované přístupy, které se otázkami digitální archivace zabývají. Uděláme proto malou odbočku tímto směrem.

3. OAIS

Dokument ([3]) Reference Model for an Open Archival Information System (OAIS), jenž byl vydán jako BLUE BOOK CCSDS 650.0-B-1, January 2002 a v roce 2003 jako norma ISO 14721:2003, je dokumentem normativního typu, který si vzal za cíl definovat obecný model informačního systému sloužícího k archivaci elektronických dat obecně (ne nutně elektronicky podepsaných).

Historicky nezbytnost zabývat se intenzivně danou problematikou vznikla v NASA - jako potřeba archivovat digitální údaje z kosmického výzkumu, a to fakticky již od roku 1966. Byla postupně použita celá řada různých technologií. V roce 1982 vznikl Consultative Committee for Space Data Systems jako mezinárodní skupina aktivit spojených s výzkumem vesmíru, vyvinul řadu normativních postupů, od roku 1990 spolupracuje s ISO, která mu následně doporučila připravit normu. Postupně vzniklo několik verzí dokumentu (tzv. white

book, red book, poslední z roku 2002 označen jako blue book). Poslední verze je ta, co je k dispozici na webu, byla schválena řídícím výborem CCSDS a je k dispozici na adrese http://www.ccsds.org/ - do pěti roků po jejím vydání má proběhnout revize.

V roce 2003 byl dokument vydán jako ISO 14721:2003:

- Specifikuje referenční model pro otevřený systém archivace dat (open archival information system - OAIS). Cílem normy ISO 14721:2003 je ustavit systém pro archivaci dat a to jak v digitalizované, tak i ve fyzické podobě, spolu s organizačním schématem, které se skládá z lidí, kteří akceptují odpovědnost za uložená data a zpřístupňují je cílové komunitě.

- Tento referenční model se týká kompletně všech funkcí, které souvisí s archivním uchováváním dat včetně jejich příjmu, archivního uložení, správy dat, přístupu a distribuce. Také se týká migrace digitálních dat na nová media a formáty, datových modelů, které jsou používány pro reprezentaci dat, role softwaru při uchovávání dat a výměny digitálních dat mezi archivy. Identifikuje jak externí tak i interní rozhraní k funkcím archivu a identifikuje služby vyšších úrovní na těchto rozhraních. Poskytuje některé ilustrativní příklady a některá doporučení typu "best practice". Definuje minimální množinu záruk za archiv (aby mohl být nazýván OAIS) a také definuje maximalistický archiv, který dává širokou škálu podmínek a koncepcí.

- Model OAIS popsaný v ISO 14721:2003 lze aplikovat na libovolný archiv. Konkrétně ho lze aplikovat na organizace, které odpovídají za to, že data jsou dlouhodobě dostupná. To se týká také organizací, které mají jinou odpovědnost, jako např. zpracování a distribuce dle potřeb nějakých programů.

Daný model je pouze abstraktním informačním modelem práce s digitálními objekty (a asociovanými metadaty) a jeho cílem není konkrétní implementace. Open Archival Information System je tedy referenční model archivu, který sestává z organizace lidí a systémů, která akceptovala odpovědnost za uchovávání dat a jejich zpřístupnění Cílové Komunitě. OAIS Reference Model ilustruje funkce a informační toky, které jsou využitelné pro digitální archiv, jenž je konstruován tak, aby bylo možné provozovat bezpečnou dlouhodobou úschovu digitálních objektů.

Dnes již existuje celá řada funkčních digitálních archivů vytvořených na základě filozofického přístupu OAIS, který je v popsán v citované ISO normě.

4. Elektronické podpisy a archivace

Konkrétní řešení, které by umožňovalo archivovat elektronicky podepsané dokumenty, musí vzít do úvahy jak archivační pohled (a to jak z hlediska použitelných norem, tak i z hlediska příslušné legislativy), tak specifika elektronických dokumentů, mezi která patří i použití elektronických podpisů a důvěryhodná archivace takto podepsaných elektronických dokumentů.

Vyřešení otázky, s jakými pracovat formáty elektronických podpisů, je tedy jednou z nezbytných podmínek pro úspěšné fungování archivu, který obsahuje elektronicky podepsané

dokumenty. V dalších číslech Crypto-Worldu bude proto pozornost věnována následujícím dvěma normativním dokumentům ETSI ([4], [5]), které se touto problematikou zabývají.

Dokument ETSI TS 101 733 (poslední verze je z prosince 2003 a nese označení V.1.5.1):

Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats má za sebou již relativně dlouhou historii. Během ní prošel řadou úprav a verzí. V prvních verzích obsahoval kapitoly, které se týkaly aspektů pro politiky elektronických podpisů, ty byly pak přeneseny do samostatného dokumentu ETSI TR 102 272. V dokumentu je definována celá řada formátů elektronických podpisů a to tak, aby byly podchyceny potřeby možných praktických situací.

Dokument ETSI TS 101 903 (verze V.1.02.02 se objevila v dubnu roku 2004) je orientován na problematiku XML elektronických podpisů, které dlouhodobě zůstávají v platnosti (materiál se opírá o předchozí citovaný dokument ETSI TS 101 733).

5. Literatura

[1] J. Pinkava: Digitální certifikáty č.11. Archivace elektronických dokumentů, Crypto-World 4/2003

[2] J. Pinkava: Archivace elektronických dokumentů, Crypto-World 11/2003, 1/2004, 2/2004.

[3] Norma ISO 14721:2003, Space data and information transfer systems - Open archival information system - Reference model

[4] ETSI TS 101 733, V.1.5.1, Electronic Signatures and Infrastructures (ESI); Electronic Signature Format

[5] ETSI TS 101 903, V.1.02.02, XML Advanced Electronic Signatures (XAdES)líbený článek – podpisy s dlouhodobou platností

D. Anotace - Hashovací funkce v roce 2004 (příloha k e-zinu Crypto-World 10/2004) Jaroslav Pinkava, PVT a.s.

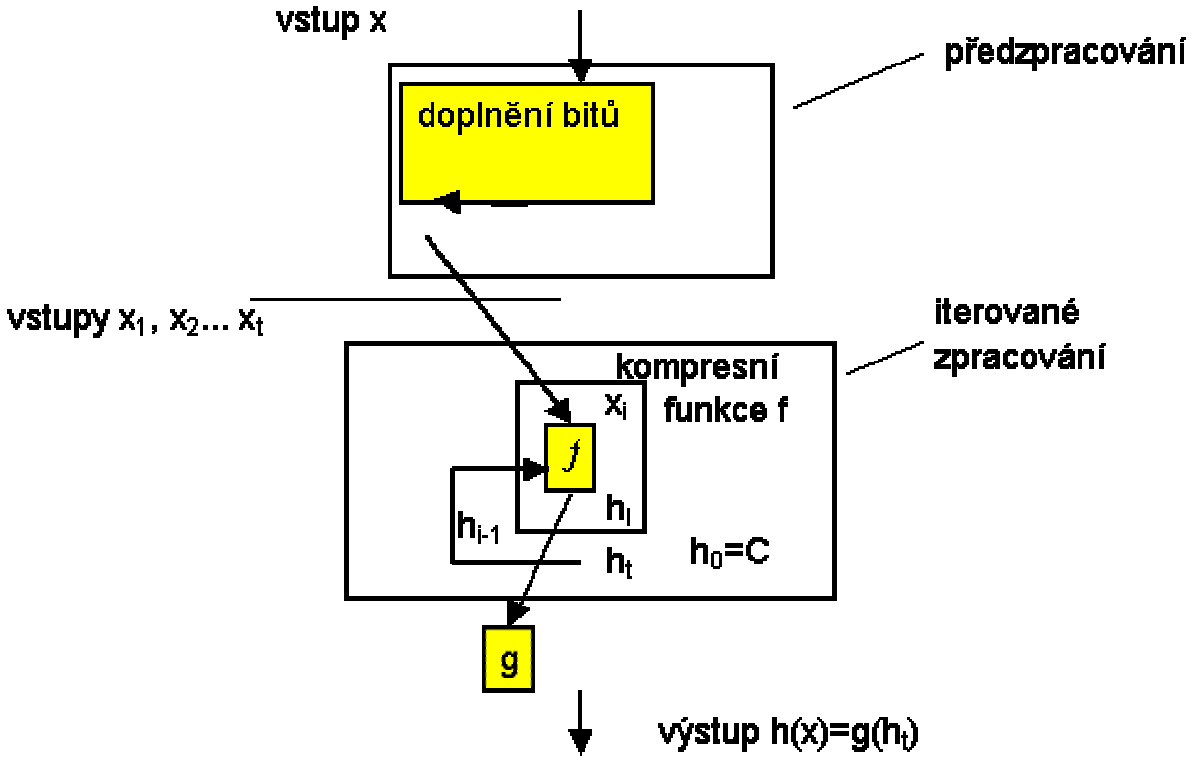
Příloha k dnešnímu číslu Crypto-Worldu je rozšířená a revidovaná verze článku ***Hashovací funkce v roce 2004***, která byla otištěna v Crypto-Worldu 9/2004. Článek je také samostatně dostupný na www stránce autora:

http://crypto-world.info/pinkava/clanky/hash_2004.pdf

Článek obsahuje popis základních vlastností hashovacích funkcí, popisuje některé momenty vývoje dané oblasti kryptografie. Dále je zde obsažen stručný přehled existujících útoků. Na základě těchto popisů následuje přehled posledních výsledků, přednesených na konferenci CRYPTO 2004 (Biham, Joux, čínští kryptologové).

Opravena je zde pasáž, která byla uvedena v odstavci 6 původního článku a která obsahovala chybu, kterou podrobně komentuje kolega Klíma v následujícím článku tohoto e-zinu.

Současně využívám této možnosti a omlouvám se čtenářům za nepřesnost, chyba je plně na mé straně a vznikla jako důsledek časového stresu.



E. Komentář k nepřesnostem v článku J.Pinkava: Hashovací funkce v roce 2004 (Crypto-World 9/2004)

Vlastimil Klíma, v.klima@volny.cz

1. Úvod

Článek "Hashovací funkce v roce 2004" v Crypto-Worldu č.9/2004 od Jaroslava Pinkavy se zabývá hašovacími funkcemi. Článek obsahuje širší kontext o hašovacích funkcích, aby se pokusil vysvětlit podstatu čínského útoku na hašovací funkce. Zatímco kontext je v zásadě v pořádku, ***vysvětlení čínského útoku obsahuje chyby, které jsou systematického rázu***. To se samozřejmě může stát, a proto jsem se rozhodl uvést věci na správnou míru, neboť Crypto-World bývá zdrojem informací pro různé bezpečnostní pracovníky, vývojáře a studenty, kteří by měli mít k dispozici správnou interpretaci dosažených výsledků.

2. Pojmy kolize a kompresní funkce

V úvodu si doplníme některá fakta, která budeme potřebovat, a určíme si kontext útoků na hašovací funkce.

Hašovací funkce, které budeme popisovat, jsou všechny iterativního typu. Jsou definovány pomocí kompresní funkce f a inicializační hodnoty H_0. Při hašování zprávy m je tato určitým způsobem doplněna a poté rozdělena na bloky m_i (i = 1,..., n) pevné délky. U námi popisovaných funkcí (MD4, MD5, SHA-0, SHA-1, SHA-256) je to 512 bitů. Poté kompresní funkce f v i-tém kroku (i = 1,..., n) zpracuje vždy daný kontext H_{i-1} a blok zprávy m_i na nový kontext H_i. Vidíme, že název kompresní funkce je vhodný, neboť funkce f zpracovává širší vstup (H_{i-1}, m_i) na mnohem kratší H_i, tedy m_i se sice funkčně promítne do H_i, ale současně dochází ke ztrátě informace (šířka kontextu H_0, H_1,...H_i,... zůstává stále stejná). Po zhašování posledního bloku m_n dostáváme kontext H_n, z něhož bereme buď celou délku nebo část jako výslednou haš. U funkce MD5 je šířka kontextu 128 bitů a výslednou haš tvoří celý kontext H_n.

Pro další výklad si povšimněme, že když hašujeme druhý blok m_2, je to jako bychom začínali hašování od začátku, ale s inicializační hodnotou H_1 nikoli H_0. Čili výsledek hašování zprávy m_1, m_2, ... s inicializační konstantou H_0 je stejný jako výsledek hašování zprávy m_2,... s inicializační konstantou H_1, atd.

Kolize hašovací funkce h spočívá v nalezení různých zpráv M1 a M2 tak, že h(M1) = h(M2). Kolize kompresní funkce f spočívá v nalezení inicializační hodnoty H a dvou různých bloků B1 a B2 tak, že $f(H, B1) = f(H, B2)$. Rozdíl je tedy v tom, zda si můžeme libovolně volit inicializační vektor H_0. Jak je vidět, nalezení kolize kompresní funkce je obecně „snazší“ úloha, nicméně nebývá tak „daleko“ od kolize haše.

3. Čínský útok a jeho interpretace

Současný stav hašovacích funkcí nejvíce ovlivnily útoky a práce prezentované v období konání nejprestižnější kryptografické konference Crypto 2004 v srpnu t.r. v Kalifornii. Jednak to byly příspěvky řádné, jednak mimořádné, velmi krátké neformální příspěvky, které se prezentují na tzv. Rump Session ve velmi rychlém sledu (pár minut na příspěvek). Čínský

tým zde dostal, vzhledem k mimořádnému výsledku, 15 minut. Jak by ne, když to, co předvedli, mělo mimořádnou hodnotu pro kryptografickou komunitu [4]. O obrovském zájmu o jejich příspěvek svědčí i to, že vůbec poprvé za dobu konání konferencí Crypto byla Rump Session přenášena v přímém přenosu na Internetu (informovali jsme o tom v News na domovské stránce Crypto-Worldu, příspěvek 440)

Právě tento zásadní výsledek byl však v článku [3] zásadně špatně interpretován, a to v klíčové myšlence **kolizí MD5**. Chybná interpretace je přitom opakována celkem na čtyřech místech příspěvku. Pokusím se tedy o správné vysvětlení. Čínští výzkumníci přišli s metodou, jak nalézt kolize dvou různých 1024bitových zpráv, a dělají to tak, že nejprve naleznou dvě **různé** 512bitové půlzprávy (bloky) M1, M2, což jim trvá cca hodinu, a potom k nim naleznou dvě **různé** 512bitové půlzprávy N1, N2 (což trvá už jen sekundy) tak, že složené zprávy (M1, N1) a (M2, N2) mají stejnou haš. Dokonce uvádí předpis, jak se první poloviny M1 a M2 těchto komponovaných zpráv mají **lišit** a jak se druhé poloviny N1 a N2 mají **lišit**. Právě jedním z překvapení útoku bylo, že konstanty, o které se první a druhé poloviny liší, jsou k sobě inverzní (M2 = M1 + C, N2 = N1 - C). Hlavní myšlenkou útoku tedy bylo najít takovou zvláštní konstantu C a pak během první hodiny útoku nalézt zprávu M1 tak, aby **M1** a **M2** = M1 + C při hašování vedly na **určitý odlišný** kontext (mezivýsledek hašování H_1, viz iterativní proces výše) takový, že **tato odlišnost je srovnána při hašování následných bloků N1 a N2** = N1 - C. První odlišné bloky zprávy tedy vytvoří sice různé kontexty, ale druhé bloky to srovnají na celkový stejný výsledek. Pokud nyní hašování buď ukončíme nebo budeme v obou případech pokračovat už jen stejnými bloky zprávy, obdržíme v obou případech stejný hašový kód, tedy kolizi. Tato vlastnost **neplatí** pro všechny bloky M1, takže je nutné je zvláštním způsobem konstruovat.

Avšak aby byla vidět síla útoku, autoři ukázali, že po první (hodinu trvající) fázi, kdy naleznou (M1, M2), jsou k ní schopni nalézt **více dvojic** (N1 a N2), (N1´, N2´), ... vedoucích ke kolizi, tj. *h*(M1, N1) = *h*(M2, N2), *h*(M1, N1´) = *h*(M2, N2´). Tedy prokazují, že původní různé kontexty dovedou dovést ke stejné haši několika cestami.

V [3] se píše, že ... " *Jako příklad jsou uvedeny dvě zprávy v délce 1024 bitů,* ***přitom se shodují v prvních 512 bitech*** *a mají tentýž hash. ... h(x) = h(y), přitom x = (**M1**, N1) y = (**M1**, N2) ...*" a dále, že "*Na základě výsledku čínských matematiků je možné zkonstruovat dvě zprávy, které se v první části zcela shodují, v druhé části se liší a mají přitom týž haš*".

Tato interpretace, která snad vznikla nepozorným čtením původního příspěvku, je v rozporu s hlavní myšlenkou útoku o nalezení diferenční konstanty C, v níž se **první** poloviny zpráv liší.

Dále se v [3] tvrdí "*...V příkladu jsou uvedeny zprávy se shodnou první částí, ale nejedná se o nějakou smysluplnou část, tj. asi skutečně je výsledkem nějakých výpočetních postupů. Pokud by tomu tak nebylo a bylo by z hlediska použité metody možné např. přímo volit obsah části zprávy, praktický dopad by mohl být více nepříjemný.*"

To je další věc, kterou je potřeba poopravit. "Pokud by tomu tak nebylo… " lze nahradit "Skutečně tomu tak je…", neboť v čínském útoku lze libovolně volit začátky obou kolidujících zpráv. Číňané jsou totiž schopni svůj útok provést s libovolnou inicializační hodnotou, jak ukázali i prohlásili. Mohou si tedy **zvolit libovolnou smysluplnou zprávu** T a poté k ní konstruovat jak jsou zvyklí (M1, N1) a (M2, N2) tak, že *h*(T, M1, N1) = *h*(T, M2, N2). Proč? Když hašují zprávu (T, ...) dojdou po zhašování T (uvažujeme pro jednoduchost T zarovnanou na bloky) k určitému kontextu H_n. Ten prohlásí za novou inicializační konstantu H_0' (je jim jedno, jakou má hodnotu) a začnou svůj útok od ní. Zkonstruují (M1,

N1) a (M2, N2) tak, že *pro tuto inicializační konstantu* vedou ke kolizi, jinými slovy **dosáhli toho, že *h*(T, M1, N1) = *h*(T, M2, N2) pro libovolnou zprávu T** zarovnanou na bloky.

V [3] se dále uvádí, že "*...pak by bylo možné toho využít tak, že útočník získá dokument podepsaný druhou stranou, změní část dokumentu, podpis zůstává týž.*",

To je další zásadní omyl, neboť **útočník není tak mocný a musí obě kolidující zprávy vytvářet sám**. Čínský útok neumí k danému dokumentu nalézt jiný, se stejnou haší! Umí "pouze" najít dva různé dokumenty se stejnou haší. Správná formulace hypotetického útoku tak zní „*…že útočník **nechá svůj pečlivě připravený dokument podepsat** druhou stranou, změní část dokumentu, podpis zůstává týž.*“ V karikatuře si můžeme představit například jak zaměstnanec dává šéfovi podepsat žádost o dovolenou, se kterou mu „náhodou“ koliduje příkaz na zvýšení platu…

Mnoho z těchto věcí bylo vyjasněno v diskusi k článku na serveru root "Hašovací funkce MD5 a další prolomeny!", http://www.root.cz/clanek/2368. Jeho text a další linky a informace naleznete na stránce věnované tématu kolizí hašovacích funkcí http://cryptography.hyperlink.cz/2004/kolize_hash.htm (která je průběžně aktualizována).

4. Závěr

Závěrem pár slov k samotnému článku. Ve složitých vědních disciplínách, kam kryptologie bezesporu patří, se čas od času stane, že nějaký příspěvek jaksi „ujede“. Podle toho, jak daleko od pravdy odchylka míří, chopí se obvykle někdo jiný pera a papíru (či dnes spíše klávesnice) a napíše reakci, ve které se snaží uvést věci na pravou míru. Zvláště pokud se jedná o omyl toho typu, jakého jsme zde svědky. Akademická obec je na taková pravidla samozřejmě zvyklá a nikdo se z toho důvodu nad tím nepozastavuje. Vzhledem k tomu, že odběratelé Crypto-Worldu však nemusí mít s touto (snad trochu zvláštní) kulturou své zkušenosti, rozhodl jsem se připojit tento krátký vysvětlující komentář. Chci jím dát najevo, že nic z toho, co zde bylo uvedeno, není mířeno proti osobě autora [3], ale je pouze snahou opravit zde uvedená nepřesná tvrzení.

5. Literatura

[1] Vlastimil Klíma: "Hašovací funkce MD5 a další prolomeny!", http://www.root.cz/clanek/2368

[2] Průběžně aktualizovaná stránka k hašovacím funkcím v archivu autora na http://cryptography.hyperlink.cz/2004/kolize_hash.htm

[3] Jaroslav Pinkava: "Hashovací funkce v roce 2004",Crypto-World č.9/2004, str. 15-18, http://www.crypto-world.info/

[4] Xiaoyun Wang, Dengguo Feng , Xuejia Lai, Hongbo Yu: Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, http://eprint.iacr.org/2004/199.pdf

F. O čem jsme psali v říjnu (1999 – 2003)

Crypto-World 10/1999 (http://crypto-world.info/index2.php?vyber=casop1)

Crypto-World 10/2000 (http://crypto-world.info/index2.php?vyber=casop2)

Příloha : ZoEP.htm

Dnešní užitečnou přílohou je plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000.

Crypto-World 10/2001 (http://crypto-world.info/index2.php?vyber=casop3)

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)

(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

Crypto-World 10/2002 (http://crypto-world.info/index2.php?vyber=casop4)

Crypto-World 10/2003 (http://crypto-world.info/index2.php?vyber=casop5)

G. Závěrečné informace

1. Sešit

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

Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:

http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze **jméno a příjmení, titul**, pracoviště (není podmínkou) a **e-mail adresu** určenou k zasílání kódů ke stažení sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info . Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce :	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf

NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška

Webmaster Pavel Vondruška,jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@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/