Crypto-World

Informační sešit GCUCMP

Ročník 3, číslo 5/2001 **21. květen 2001**

5/2001

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR.
Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>280 e-mail výtisků)

OBSAH : **Str.**

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")

A. Bezpečnost osobních počítačů

Hlavní myšlenky z článku Bruce Schneiera - Safe Personal Computing,

CRYPTO-GRAM 5/2001

(připravil Pavel Vondruška)

Pravidelně dostávám dotaz, co může dělat průměrný internetový uživatel, aby zaručil svoji bezpečnost ? Má odpověď je " NIC". Proti „vládním institucím" nemůžete dělat nic. Jejich převaha je příliš velká. Dokonce ani používání nejsilnějšího šifrování vám nepomůže, policie vám může ve vaší nepřítomnosti nainstalovat program, který umožňuje sledovat vaši práci na klávesnici. Účinně se bránit je obtížné i pro velké organizace.

Následuje několik rad, které vám pomohou zvýšit bezpečnost při připojení na internet. Nejsou dokonalé a také není jednoduché je dodržovat.

1. **Hesla**

Nemůžete si správně zapamatovat všechna hesla, tak se tím netrapte! Vytvořte si dlouhá náhodná hesla a zapište si je. Založte si je do peněženky nebo uložte do programu typu „Password Safe". Hlídejte si je, jako by to byly vaše peníze. Zakažte ve vašem prohlížeči ukládání hesel. Nepřenášejte (e-mailem nebo ve www prohlížeči) hesla nebo PINy v nezašifrované podobě. Počítejte s tím, že všechny PINy mohou být snadno „breaknuty" a podle toho jednejte.

2. **Antivirový software**

Používejte ho. Stahujte a instalujte "updaty" každé 2 týdny, a dále kdykoliv se dočtete o novém viru. Některé antivirové programy samy vyžadují "updatovat ".

3. **Osobní " firewall"** .

Používejte ho. Obvykle není důvod, aby se kdokoliv, odkudkoliv snažil připojit k vašemu počítači.

4. **E-mail**

"Spam" nečtěte a mažte jej. Neotvírejte a okamžitě smažte také zprávy, které mají přílohu a o nichž nevíte, co obsahují. Neotvírejte a okamžitě také mažte obrázky, videa a podobné zásilky zaslané pro „zasmání" a to i od dobrého kamaráda. Vypněte HTML mail.

Nepoužívejte Outlook nebo Outlook Express. Jestliže musíte použít Microsoft Office, zapněte ochranu proti makro virům; v Office 2000 nastavte bezpečnostní stupeň "high" a pokud nemusíte, nevěřte žádnému zdroji. Jestliže používáte Windows, vypněte skrytí přípon souborů pro známé typy aplikací; tím lze zabránit některým útokům typu Trojského koně nebo „maškarádám", kdy se soubor tváří jako jiný typ. Odinstalujte "Windows Scripting Host", pokud jej delší dobu nebudete potřebovat.

5. **Web stránky**

Použití SSL nezajišťuje, že "vendor" je spolehlivý nebo že jím zpravované databáze jsou bezpečné. Přemýšlejte, než začnete obchodovat na webovských stránkách. Neposílejte na webovskou stránku data (typu finanční částky, osobní data) beztoho, aniž byste za ně měli nějakou jasnou protihodnotu. Když nechcete poskytnout osobní informace - tak použijte lži. Jestliže vám webowské stránky dávají možnost neukládat vaše data pro příští použití, využijte toho.

6. Prohlížeč

Omezte používání “cookies“ a appletů na těch pár stránek, kde využíváte nějakou potřebnou službu. Pravidelně čistěte vaše “cookie“ a dočasný temp adresář. (Mám za tím účelem zhotovený dávkový soubor, který se spouští při každém zapnutí počítače.) Jestliže to je možné, nepoužívejte Microsoft Internet Explorer.

7. Aplikace

Na vašem počítači používejte jen omezený počet aplikací. Jestliže aplikaci nepotřebujete, neinstalujte ji. Pokud dlouhou dobu nepotřebujete nějakou aplikaci, odinstalujte si ji. Jestliže ji používáte, pravidelně instalujte příslušné “updaty “.

Obr. 1 Bruce Schneier
[schneier@counterpane.com]

8. Zálohování

Zálohujte pravidelně. Zálohujte na disk, pásku nebo CD-ROM. Ukládejte nejméně jednu zálohovací sadu mimo počítač (nejvhodnějším místem je trezor) a nejméně jednu zálohu mějte na počítači. Pamatujte na zničení starých záloh, CD-R disky také fyzicky zničte.

9. Bezpečnost vašeho přenosného počítače

Pokud jste s vaším přenosným počítačem mimo domov, mějte jej po celou dobu stále u sebe. Myslete na něj tak jako na peněženku. Pravidelně z něj mažte nepotřebná data. To samé platí i pro palmtopy. Lidé mají tendenci v nich mít uložena osobní data, včetně hesel a PINů.

10. Šifrování

Instalujte si pro e-mail a pro šifrování souborů některý šifrovací program (např. PGP). Šifrování všech Vašich e-mailů není reálné, ale některý mail může být natolik citlivý, abyste jej neposílali v otevřené podobě. Podobně to platí pro některé soubory na vašem pevném disku - mohou být příliš citlivé na to, abyste je nechali nezašifrované.

11. Všeobecně

Vypněte počítač, když jej nepoužíváte. Speciálně na to dbejte, pokud máte stálé připojení na internet. Jestliže je to možné, nepoužívejte Microsoft Windows.

Provádět toto vše je samozřejmě velice náročné a já sám ne vždy všechna tato pravidla dodržuji. Ale vím, že řídit se těmito radami je pravděpodobně to nejlepší, co můžete pro bezpečnost svých počítačů udělat.

B. Záhadná páska z Prahy (I.díl)

Mgr. Pavel Vondruška, Mgr. Jan Janečko

Asi každý člověk je rád, když se setká s nějakou záhadou a může dokonce pomoci ji objasnit. Co platí pro „obyčejného člověka“, platí pro kryptologa dvojnásob. Srdce kryptologa přímo zaplesá, pokud může při řešení záhady dokonce luštit. Se svým kolegou jsem se k jedné takové záhadě dostal začátkem minulého měsíce.

Vše začalo 13.4.2001 nečekaným e-mailem.

Vazeny pane Vondrusko,
obracim se na Vas s dotazem, zda byste se chtel pokusit o rozreseni jednoho zajimaveho problemu.Jedna se o dernou pasku nalezenou v podhledu Detskeho domu v Praze, datovanou priblizne do r.1940-50.
Pokud nebudete mit zajem Vy sam, muzete me alespon zkontaktovat s nekterym z Vasich oborovych kolegu?
Podrobnejsi informace zaslu na pozadani.

Dekuji
S pozdravem
M. V.

Trvalo pak něco přes týden, než jsme se setkali s držitelem cenné děrné pásky. Páska vypadala zcela jinak než jsme čekali. Po obou stranách měla vodící stopu a měla 31 stop! Takovouto pásku zatím nikdo z nás (ani našich kolegů) dosud neviděl.

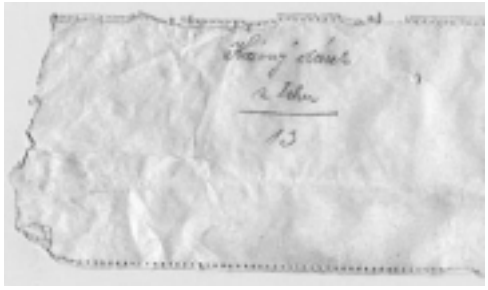
Základní informace:

- šířka pásky: 109 mm
- celková délka informací na pásce je 43,70 m
- k typickému použití originálního papíru:

- barva poněkud zažloutlá, trochu jako u starých knih
- neodpovídá současným typům počítačového papíru, papíru z pokladen, novin, časopisů
- poněkud připomíná starý toaletní papír (nekrepový), je ale docela hladký z obou stran
- svou kvalitou byl spíše určen k jednorázovému (resp. málo četnému) použití

- na začátku tužkou napsáno: Krásný dárek z trhu (podtrženo) 13
- asi po 1 m začínají dírky

- celkový počet přes 13700 znaků
- rozteč mezi dírkami horizontální: 3,175 mm (cca 315 dírek/1 m)
- rozteč mezi dírkami vertikální: 3,16 mm
- někde uprostřed jsou dírky 3 za sebou jdoucích znaků přelepených kouskem lepící pásky staršího typu

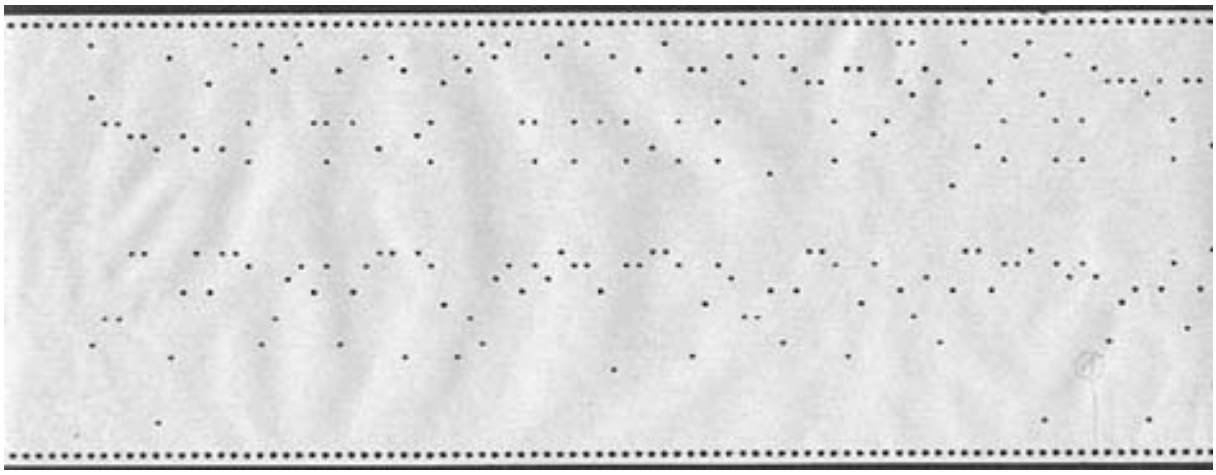


Obr.1 - Začátek záhadné pásky

- Znak s "velkou" dírkou

- velká dírka je vždy ve stejné stopě
- znak s velkou dírkou se vyskytuje buď osamoceně (tj. 1), nebo 3 stejné za sebou (asi 8x)
- celkem je asi 30 takovýchto výskytů (trojice znaků = 1 výskyt)
- dírky v ostatních pozicích jsou v různých stopách
- v rozdělení vzdáleností mezi nimi jsme neobjevili žádné zákonitosti
- trojice dírek často předchází úseky stejných znaků

- dírky jsou kulaté, avšak ne vždy dokonale proražené; jejich průměr nelze přímo změřit
- zda byly raženy po jedné či najednou (v jedné řádce) nelze poznat, nicméně někdy (snad) vypadají synchronně s traktorem, někdy jsou vůči němu mírně posunuty



Obr. 2 - První úsek s informací (tužkou námi dopsána 1 v kroužku)

Nějak se nám nechtělo věřit, že by na pásce byl zašifrovaný text. Šifrové zařízení, které by používalo takovouto pásku, nikdo z nás neznal a že by v domě bydlel „nějaký James Bond“, který by do „toaletního papíru“ zapisoval své tajné poznámky, se nám nezdálo. Pro další pátrání jsme tedy stanovili následující hypotézy:

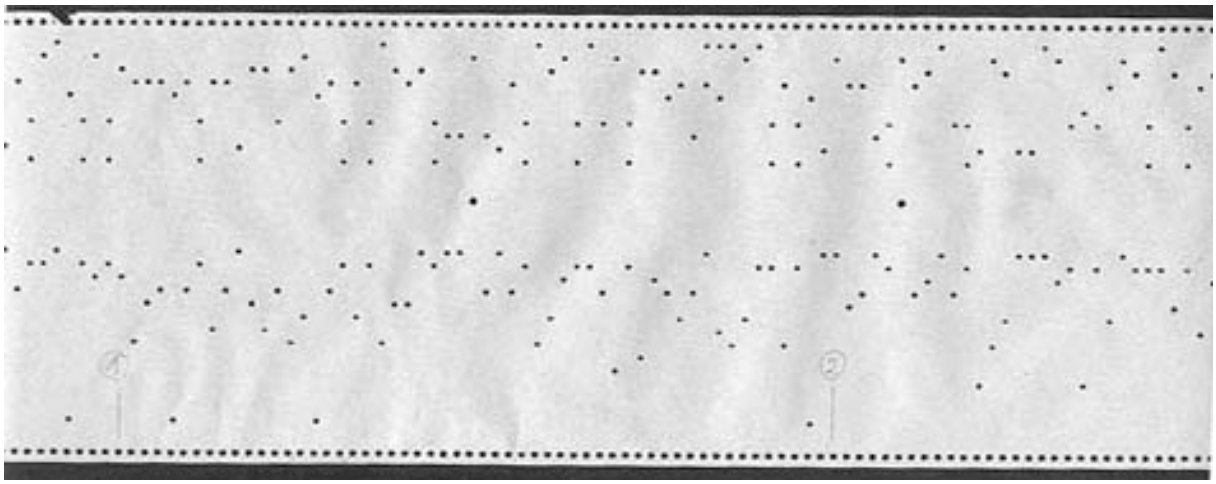
- jedná se o řídicí pásku určenou do hudebního stroje (mechanické piáno, orchestrion)
- jedná se o program do stroje textilního / předlácképo / tkalcovského (" jacguard machine ")
- jedná se o pásku do velké mechanické pokladny
- jedná se o pásku z "šifrovacího" stroje
- jedná se o pásku s kódem do nějakého nám neznámého zařízení
- jedná se o ... ?

Podle prvních informaci získaných na internetu se zdálo, že by se mohlo např. jednat o „master“ pásku pro mechanické piano Welte-Mignon (Freiburg, Germany) (rozteč 0.12526" - 3.18 mm). Tedy pásku, která mohla sloužit jako vzor pro výrobu pásek dodávaných pro příslušnou verzi mechanického piána. Kontaktovali jsme odborníka v této oblasti pana Robbie Rhodese (USA). Ten velice ochotně začal pomáhat a popis naší pásky rozeslal osmi předním odborníkům do celého světa. Během několika dnů jsme tak dostali řadu informací o páskách pro hudební stroje a to z USA, Itálie a Holandska. Nikdo sice přesně takovouto pásku ani tento typ kódování neznal, ale také nikdo zcela zásadně takovouto možnost nevyloučil.
Velice zajímavé rady poskytl expert na staré hudební nástroje pan Leonardo Perretti.
Pokusil se dokonce i o rekonstrukci "hudebního záznamu". 29. dubna zaslal e-mail, ve kterém píše:

„Začněme touto pracovní hypotézou :
1) páska obsahuje hudbu (já si myslím, že možná ne, ale je to pracovní hypotéza)
2) část pásky s 12 řádky (horní část pásky) je sopránová sekce
3) část pásky s 18 řádky (dolní část pásky) je basová sekce
3) prostřední řádek (ve které bývá větší dírka) je určen pro speciální funkci (pedál?)

4) rozsah pásky je B2/C3
6) zde jsou jen diatonické noty, C3/G4 pro soprán, F0/B2 pro bas (ok, ok, je to málo pravděpodobné, ale musíme na začátku z něčeho vyjít :-))
7) každý sloupek je osminová nota (1/8)

Takto jsem zaslanou část přepsal do svého programu Cakewalk Metro; výsledek ovšem pak připomíná skladbu od Stockhausena (with all of my respect to Stockhausen :-)).“



Obr. 2 - Druhý úsek s informací (1 v kroužku určuje návaznost na předchozí úsek, na tomto obrázku jsou zřetelné "velké" dírky v jedné ze stop)

Získaný výsledek nám pan Perretti zaslal a je součástí dnešní přílohy (soubor mystery.mid). Musím říci, že se mi „skladba“ docela líbí. Poslechl jsem si ji i pozpátku a různě "rychle". Přiznám se, že tam určitou melodii poznávám... Začátek mi dokonce připomněl jeden oblíbený ragtime.

To již jsme ale měli dostatek opsaných znaků z pásky a mohli jsme sami přistoupit k základnímu statistickému rozboru. Opis „znaků“ z pásky je velice pracný - bez přiložení speciálně připravené mřížky na pásku nelze dost dobře určit příslušný řádek a sloupek, ve kterém se dírky nacházejí.

Právě toto byl také důvod, proč jsme si nejdříve ověřovali, že páska není nějakou „klasickou“ páskou do hudebního stroje nebo něco takového. Hodiny trpělivého opisování však přinesly svůj výsledek. Z toho, co jsme získali, bylo jasné, že páska obsahuje nějaký text !

Čtvrtý květen byl pak den, kdy se podařilo proniknout do systému natolik, aby bylo možné začít číst obsah pásky.

Na adrese http://www.mujweb.cz/veda/gcucmp/ je možné stáhnout soubor paska.zip (velikost 1 megabyte), který obsahuje 12 různých naskenovaných úseků pásky. Celá páska obsahuje přibližně 165 takovýchto úseků. Přepis obsahu těchto částí posloužil k rozluštění obsahu pásky.
Pozice jednotlivých naskenovaných úseků na pásce :
Begin ... Part-1 Part-2 .... Part-n .....End-h End-g End-f End-e End-d End-c End-b End-a

C. Ukončení platnosti, zneplatnění (a zrušení) certifikátu (I.díl)

Mgr. Josef Prokeš, ÚOOÚ, josef.prokes@uoou.cz

Náležitosti zneplatnění kvalifikovaných certifikátů nalezneme v několika ustanoveních zákona o elektronickém podpisu. Zdálo by se, že zákonodárce věnoval podmínkám zneplatnění - s přihlédnutím, že zákon vstupuje do smluvních vztahů mezi podepisujícími osobami a poskytovateli - dostatečnou pozornost. Ustanovení o zneplatnění mají normativní charakter a jejich povaha je kogentní, nejedná se o „zbožná přání“ (na rozdíl od formulací § 3 odst. 2 a § 4 zákona, které do právní normy nepatří).

Zopakujme si:

1. Zneplatněné certifikáty není povoleno opětovně zprovoznit a používat.
2. Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, musí neprodleně ukončit platnost certifikátu, pokud o to podepisující osoba požádá, nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů.
3. Poskytovatel certifikačních služeb musí rovněž ukončit platnost kvalifikovaného certifikátu, dozví-li se prokazatelně, že podepisující osoba zemřela nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil, nebo pokud údaje, na základě kterých byl certifikát vydán, přestaly platit.
4. Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, je povinen zajistit provozování bezpečného a veřejně přístupného seznamu kvalifikovaných certifikátů, které byly zneplatněny, a to i dálkovým přístupem.
5. Poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty, je povinen zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je kvalifikovaný certifikát zneplatněn, mohly být přesně určeny a tyto údaje byly dostupné třetím stranám. Seznam certifikátů, které byly zneplatněny, musí obsahovat přesný časový údaj, od kdy byl certifikát zneplatněn.
6. Ukončení platnosti kvalifikovaného certifikátu je rozhodné pro počátek běhu dobu (nejméně 10 let), po kterou je poskytovatel povinen uchovávat veškeré informace a dokumentaci o vydaných kvalifikovaných certifikátech (např. v elektronické podobě).
7. Úřad pro ochranu osobních údajů (dále jen „Úřad“) může současně s rozhodnutím o odnětí akreditace ukončit platnost kvalifikovaných certifikátů vydaných poskytovatelem certifikačních služeb v době platnosti akreditace.
8. Úřad může nařídit poskytovateli certifikačních služeb jako předběžné opatření zneplatnění kvalifikovaného certifikátu podepisující osoby, pokud existuje důvodné podezření, že kvalifikovaný certifikát byl padělán, nebo pokud byl vydán na základě nepravdivých údajů.
9. Nařízení o zneplatnění kvalifikovaného certifikátu může být vydáno také v případě, kdy bylo zjištěno, že podepisující osoba používá prostředek pro vytváření podpisu, který vykazuje bezpečnostní nedostatky, které by umožnily padělání zaručených elektronických podpisů nebo změnu podepisovaných údajů.
10. Ten, kdo spoléhá na elektronický podpis, musí provést veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn. Pokud tak neučiní a podepisující osoba toto prokáže, podepisující osoba je zproštěna odpovědnosti za škodu.

Úmyslně byla zvolena citace ze zákona. Povšimněme si pojmů vztahujících se k zneplatnění, zjistíme, že zákon používá rozdílných pojmů (pomiňme zrušení, které je pouze v názvu ustanovení týkajících se jednání ÚOOÚ). Rozdílných skutečně či zdánlivě? Zjevně není odlišnosti mezi „certifikátem, který byl zneplatněn“ a mezi „certifikátem, kterému byla ukončena platnost“. Jak však chápat „zneplatnění“ a „ukončení platnosti“. Prvé jako proces, druhé jako akt nebo (pro právní teoretiky) jednostranný úkon s veřejnoprávním prvkem?

Otázka zneplatnění může být pro elektronické podepisování klíčová. Funkce elektronického podpisu je odlišná od funkce běžného podpisu, nesporně širší než u obyčejného podpisu, podobně naroste i právní význam elektronického podepisování. Zákony poměrně často stanoví určité požadavky na formu úkonů a náležitosti prostředků, jimiž se provádí dokládání čehokoliv (osvědčení, prokázání, dokazování). Svými vlastnostmi a funkcemi mohou některé druhy elektronický podpisů dodat dokumentům širší (nebo jinou) hodnotu důvěry nebo napomohou identifikaci (příp. autentizaci) těch, kteří činí právní úkony, účastníků právních vztahů (v dikci zákonů – „určení osoby“). Přinejmenším a v konečném případě se vždy uplatní v procesu dokazování, a to nejen ve prospěch toho, kdo dokument podpisem opatřil (např. trestněprávní žaloba pro trestný čin pomluvy spáchaný prostřednictvím podepsané webové stránky).

Je-li elektronického dokumentu podepsán určitým druhem podpisu, je nezbytné se přesvědčit, zda-li je dokument opatřen podpisem „platným“, s nímž musí být spojen certifikát nikoliv neplatný. Lze si představit nedorozumění a „nedopatření“, které mohou nastat v důsledku jednání nedbalých úředníků veřejné správy, pokud si tito dostatečně neověří platnost certifikátu. Avšak v případě soukromých subjektů je možno předpokládat náročné spory o platnost certifikátů.

Uprostřed sporu se ale ocitne také poskytovatel. Co mu říká zákon? Především mu ukládá značné povinnosti a s nimi spojuje odpovědnost. Proto by bylo vhodné, aby zákonodárce upravil konkrétní povinnosti takovým způsobem, aby jejich výklad nezavdával důvod k nejasnostem. Takovéto případné nejasnosti by poskytovatele postavily do jádra sporu. Možný sporný příklad nám zákon bohužel nabízí, uveďme si jej v souvislosti se seznamem kvalifikovaných certifikátů, které byly zneplatněny. Na rozdíl od seznamu vydaných kvalifikovaných certifikátů není stanovena povinnost údaje obsažené v seznamu kvalifikovaných certifikátů, které byly zneplatněny, okamžitě aktualizovat.

Zákon předpokládá následující události:

- podání žádosti o zneplatnění,
- ukončení platnosti,
- zařazení informace o ukončení platnosti do seznamu kvalifikovaných certifikátů, které byly zneplatněny,
- zveřejnění seznamu kvalifikovaných certifikátů, které byly zneplatněny.

Jednání poskytovatele od podání žádosti do uvedení v seznamu ponechává zákon na úpravě poskytovateli, samozřejmě s dodržením zákonných povinností, např. po podání žádosti do ukončení platnosti certifikátu přikazuje zákon konat neprodleně. Nezbytné je dodržet smluvní ujednání mezi poskytovatelem a podepisující osobou (smlouva musí být písemná, jinak je neplatná).

V části druhé:

1. Jakou dobu lze rozumět pod pojmem „neprodleně“, význam pojmu v případě právního sporu.
2. V jaké lhůtě zařadit údaje o zneplatněném certifikátu do seznamu, v jaké lhůtě zveřejnit seznam?
3. Důsledky absence některých požadavků na seznam zneplatněných certifikátů v zákoně.
4. Nedostatky zákona s ohledem na možnou odpovědnost subjektů (poskytovatel, podepisující osoba, osoba spoléhající na podpis).
5. Od kterého okamžiku v případech procesu zneplatnění nastává odpovědnost poskytovatele, příp. osoby spoléhající na certifikát, resp. přechází odpovědnost od podepisující osoby, která požádala o zneplatnění?
6. Co musí učinit poskytovatel, pokud osoba splní zákonnou povinnost a neprodleně vyrozumí poskytovatele o hrozícím nebezpečí?

D. Identrus - celosvětový systém PKI
Ing. Josef Ulehla, UEP, a.s.

Využití internetu čím dál více směřuje ke globálnímu elektronickému podnikání a globálnímu elektronickému obchodování. Obchodníci obsluhují své zákazníky v online obchodech; internet stále více nahrazuje dopisy a faxy. Naneštěstí existují různé obchodní systémy i různé metody jejich zabezpečení, přičemž kvalita zabezpečení je obtížně kontrolovatelná.

Současné kreditní karty jsou vhodné například pro internetový nákup knih, ale nepomohou výrobcům nacházet nové zahraniční trhy a online uzavírat mnohamilionové obchody.

I. Historie Identrus

Aby mohly být obchody označované B2B a někdy až BB2BB (Big business to Big Business) bezpečně a efektivně uzavírány, položily globální finanční instituce - ABN AMRO Bank, Bank of America, Barclays, Chase Manhattan, Citigroup, Deutsche Bank a HypoVereinsbank - **počátkem roku 1997** základy Identrus.

V březnu 1999 byla zformována společnost Identrus.

V září roku 2000 bylo spuštěno celosvětově první systémové řešení Identrus v Deutsche Bank ve spolupráci IBM, SECUDE, Arthur Andersen a TrustCenter, technologicky založené na obchodu e-BX™ a kryptografii SECUDE TransFair.

Počátkem roku 2001 přichází do života Identrus PKI.

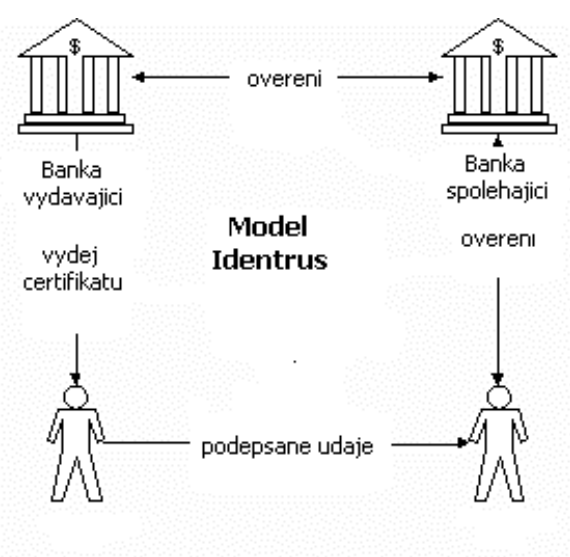
Dnes jsou členy Identrus tyto finanční instituce: Abbey National PLC, ABN AMRO, AIB Group, Australia and New Zealand Banking Group Ltd. (ANZ), Banco Bilbao Vizcaya Argentaria, S.A., Banco Sabadell, Banco Santander Central Hispano, Banesto, Bank of America, Bank of Ireland, Bank of Scotland, The Bank of Tokyo-Mitsubishi Ltd., Barclays PLC, BNP Paribas, Canadian Imperial Bank of Commerce (CIBC), Chase Manhattan Bank, Citigroup, The Co-operative Bank , Commerzbank, Crédit Agricole France, Crédit Lyonnais, Deutsche Bank, Dresdner Bank, HSBC Group, HypoVereinsbank, Industrial Bank of Japan, Limited (IBJ), ING Group, Lloyds TSB, National Australia Bank Limited, Nordea, The PNC Financial Services Group, Inc., Royal Bank of Canada, Royal Bank of Scotland Group, Sanwa Bank, Scotiabank, SEB Bank, Société Générale, Sumitomo Mitsui Banking Corporation, Wells Fargo Wholesale Internet Services, Westdeutsche Landesbank Girozentrale, Westpac Banking Corp.

Partnery pro řešení Identrus jsou:

- SECUDE Gmb, IBM, Sun, JCP, Razorfisch (i-Cube), Litronic, Entegrity..
- Baltimore, Verisign, TC Trustcenter, Valicert, CerCo, Kyberpass, Computer Associates..
- ID2, Gemplus, Oberthur, ActicCard,Reinbow, nCipher, ConcordEracom…

Infrastruktura Identrus je otevřená, připojují se stále další finanční instituce a další partneři upravují svá technologická řešení standardům Identrus.

V Identrus procesu elektronického obchodu přebírají finanční instituce tradiční roli budování důvěry mezi různými obchodními partnery (čtyřrohý model). Aplikace, které jsou používány



v globální infrastruktuře veřejných klíčů sítě Identrus, pak mohou zajišťovat bezpečnostní funkce, jako jsou identita a autenticita partnerů, integrita údajů, důvěrnost a neodmítnutelnost odpovědnosti obchodních transakcí.

Cílem Identrus je vytvoření celosvětové sítě důvěrných finančních institucí s úplnou důvěrou a možností řízení rizik.

Identrus zajišťuje důvěru, ochranu proti podvodům a platební vyrovnání v on-line obchodech realizací Identrus servisních služeb, kterými jsou:

Identita
Kontrola identity je založena na OCSP (RFC 2560).
Kontrola statusu je prováděna na základě Identrus Certifikátů.
Každá finanční instituce provozuje OCSP komunikátor.
Identrus root CA podepisuje certifikáty OCSP komunikátorů finančních institucí.

Záruky
Identrus nedává záruky absolutní bezpečnosti, ale garantuje akceptovatelná rizika.
Poskytuje různé úrovně řízení rizik:
- status certifikátu se nekontroluje,
- status certifikátu se kontroluje náhodně,
- status certifikátu se kontroluje v čase transakce (= základní úroveň jistot),
- status certifikátu se kontroluje v čase transakce a navíc banka podepisujícího zákazníka dává obchodníkovi záruky.

Platba
Platba se provádí na základě digitálně podepsaných potvrzení. Je možné používat modely:
- platba je iniciována přes banku obchodníka,
- platba je iniciována zákazníkem přes jeho banku.

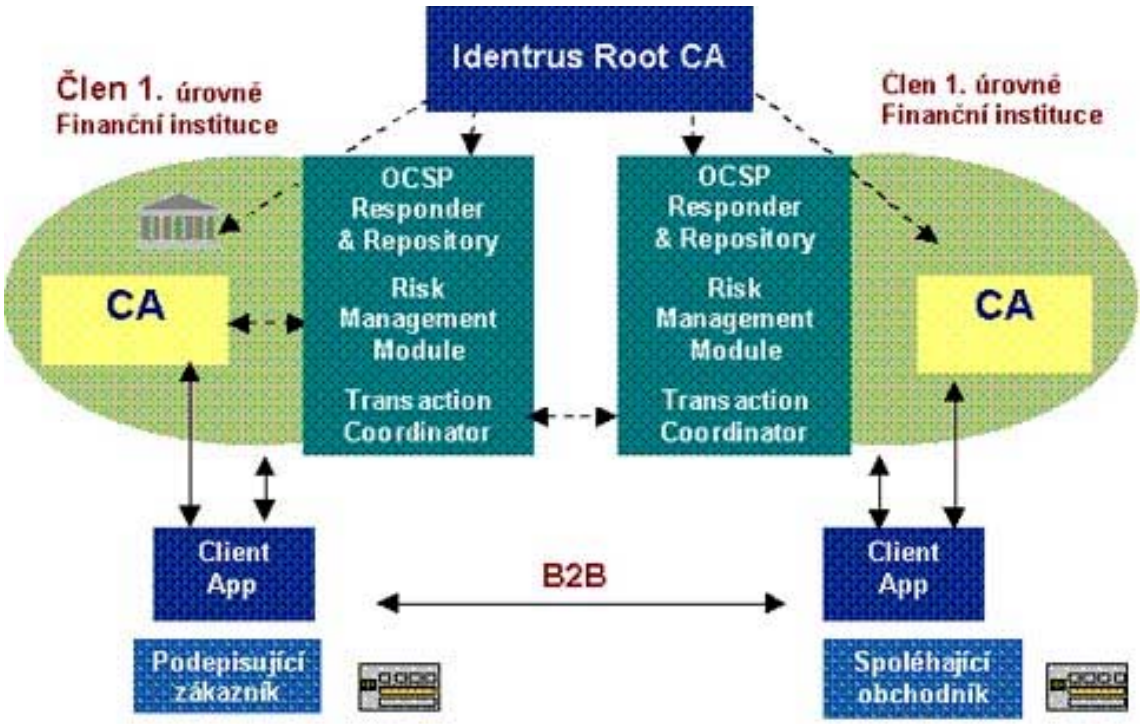
II. SECUDE Identrus řešení

Společnost SECUDE měla od počátku důležitou roli v budování systému Identrus. Na základě svých zkušeností s poradenstvím pro různé finanční společnosti dodala firma SECUDE své know-how při procesu řešení specifik Identrus.

SECUDE podporuje pomocí svých softwarových produktů obě strany, které se účastní PKI systému Identrus: podepisujícího zákazníka (zákazníka, který generuje svůj elektronický podpis) a spoléhajícího zákazníka (obchodníka, který musí na tento podpis spoléhat). Všechny standardní produkty SECUDE jsou postaveny tak, že splňují podmínky systému Identrus. Obzvlášť produkt SECUDE TransFair umožňuje snadné použití Identrus systému pro existující obchody a tržní řešení. Výsledkem této inteligentní architektury jsou minimální náklady na začlenění.

Přehled řešení SECUDE pro Identrus:

- Knihovna SDK pro aktivaci libovolné webové aplikace pro systém Identrus (TransFair Server).
  - Platformy: Windows NT 4.0, Windows 2000, AIX, HP-UX, Linux, Solaris, SunOS.
- Plugin prohlížeče a Java klient podle specifikací Identrus se zobrazením komponentu pro čitelný text (TransFairClient).
- Nástroj pro Identrus čipovou kartu a konfigurace pro smartcard terminál.
- Začlenění do Microsoft Outlook 97, 98, 2000.
- Začlenění do Lotus Notes 4.5, 4.6, 5.0.
- Začlenění do Microsoft Office.
- Začlenění do Microsoft Explorer.
- Podpora OCSP.
- Podpora Transaction Coordinator.
- Webové aplikace již spuštěné:
  - Intershop 4,
  - eBx of IBM.



III. Použité zdroje

[1] materiály SECUDE GmbH
[2] http://www.secude.com
[3] http://www.identrus.com

E. Kryptografie a normy
Díl 7. Normy IETF – S/MIME, část 2.

Jaroslav Pinkava, AEC spol. s r.o. & Norman Data Defense Systems, CZ

l. Úvod

Pokračování seriálu „Kryptografické normy“ v Crypto-Worldu navazuje na článek v předešlém čísle a bude tedy věnováno problematice bezpečnosti mailových zpráv - formátu **S/MIME**. První část byla věnována historii vzniku norem pro bezpečný mail a byla vysvětlena obsahová stránka formátu S/MIME. Vzhledem k tomu, že pracovních dokumentů skupiny IETF-S/MIME je poměrně dost, bude obsahový přehled dokumentů rozdělen – v této druhé část se budeme věnovat RFC dokumentům, následující třetí část (v příštím čísle) bude obsahovat přehled existujících draftů.

2. Dokumenty IETF S/MIME - Request For Comments (RFC)

2.1. S/MIME Version 2 Message Specification (RFC 2311)

Jak již bylo řečeno v první části článku, verze 2 specifikace S/MIME vyžaduje použití algoritmu RSA pro výměnu klíčů a vyžaduje použití slabé kryptografie. Tedy tato verze slouží pro využití v rámci řešení, která jsou (nebo byla) určena pro vývoz do zemí, kde je nutné aplikovat omezení vzhledem k použití tzv. silné kryptografie.

Cílem dokumentu je popis protokolu, který přidává k datům typu MIME vlastní kryptografický podpis a další služba spojené se šifrováním. Je zde definováno jak vytvořit tělo MIME zprávy, kryptograficky rozšířené dle PKCS #7. Také je zde definován postup vytváření žádostí o certifikát (dle PKCS #10) a vytváření MIME typů pro přenos těchto žádostí.

Materiál je formulován jako soustava požadavků a doporučení. Přitom požadavky jsou kladené především s ohledem na přicházející zprávy, zatímco doporučení se týkají převážně odchozích zpráv. Přitom je třeba vzít do úvahy, že S/MIME lze používat v libovolném přenosovém systému, který je schopen přenášet data typu MIME.

S/MIME zprávy jsou kombinací MIME těl a objektů PKCS. Přitom je použito více MIME typů i více PKCS objektů. S/MIME popisuje jeden formát pro data „pouze zabalená“ (enveloped only), několik formátů pro data pouze podepsaná a několik formátů pro podepsaná a zabalená data.

2.2. S/MIME Version 2 Certificate Handling (RFC 2312)

Toto je druhý z dokumentů, který se týká S/MIME verze 2. Přímo v úvodu obsahuje následující upozornění: „Informace obsažená v dokumentu má historický charakter a dokument není IETF normou.“

Pro zjištění zda použité klíče, které se vztahují k zaslané zprávě jsou platné, potřebuje příslušný S/MIME agent ověřit (certifikovat) platnost těchto klíčů. Popis cest, jak naplnit tento požadavek (s využitím digitálních certifikátů) je obsahem daného dokumentu.

Specifikace v dokumentu obsažená je kompatibilní s PKCS #7 (používá typy dat definované v PKCS #7 - Cryptographic Message Syntax) a opírá se dále rovněž o PKCS #1 (RSA Encryption) a PKCS #10 (Certification Request Syntax). Široce jsou používány především dva následující mechanismy pro přístup k certifikátům:

a) adresáře dle normy X.500 (Distinguished Name);
b) DNS (Domain Name System).

Samozřejmě příslušný „poštovní" agent musí rovněž poskytovat mechanismus ukládání a zabezpečení obdržených certifikátů tak, aby k nim mohl být později poskytnut přístup (lokální databáze certifikátů). Mechanismus pro import a export certifikátů by měl být takový, aby mu stačilo opírat se pouze o zprávy PKCS #7.

Je požadováno, aby příslušný S/MIME agent byl schopný vygenerovat žádost o certifikát na základě znalosti veřejného klíče uživatele a příslušných potřebných informací (jméno uživatele,…). V řadě případů je dvojice klíčů (veřejný a soukromý) generována souběžně. Ovšem je nutné připustit i situace, kdy dvojice klíčů je generována externím procesem (např. na připojeném HW zařízení). Neměly by být vytvářeny certifikáty pro tutéž dvojici klíčů vázané na různá jednoznačná jména (Distinguished Name). Na druhou stranu může k jednomu jednoznačnému jménu existovat více certifikátů na různé dvojice klíčů.

K žádostem o certifikát: Přijímající S/MIME agent musí podporovat identifikaci klíče RSA. Musí být podporováno použití SHA-1 a MD5 s RSA šifrováním a mělo by být podporováno použití MD2 s RSA šifrováním při ověřování podpisů na žádostech o certifikát (certifikační autoritou). Naopak žádosti o certifikát nesmí být podepsány s použitím MD2 s RSA podpisovým algoritmem. Žádosti o certifikát musí obsahovat platnou e-mailovou adresu.

Certifikační autority by měli používat při podpisování certifikátů SHA-1 a RSA podpisovým algoritmem.

2.3. Cryptographic Message Syntax (RFC 2630)

CMS (Cryptographic Message Syntax) syntaxe je syntaxe používaná (vzhledem k libovolným zprávám) pro vytváření digitálních podpisů, otisků zpráv (message digest), autentizaci zpráv či pro jejich šifrování. Je to vlastně popis určitého způsobu zabalování (encapsulation) vzhledem k ochraně dat. Je takto umožněna i vícenásobná obálka dat a využívání atributů různých typů (např. časový údaj vzhledem k podpisu). Hodnoty CMS jsou generovány pomocí ASN.1 při použití BER kódování a obvykle jsou reprezentovány jako oktetové řetězce.

Dokument definuje jeden obsahový typ vázaný bezprostředně na ochranu dat – ContentInfo a šest dalších obsahových typů: data, signed-data, enveloped-data, digested-data, encrypted-data, and authenticated-data.

Implementace CMS musí (mají) zahrnovat následující algoritmy:
Hashovací funkce: SHA-1 (MD-5);
Podpisové algoritmy: DSA (RSA);
Dohoda na klíči: Diffie-Hellman dle X9.42 - Ephemeral-Static;

Přenos klíčů: RSA;
Autentizace zpráv: HMAC s SHA-1 - dle RFC 2104;
Šifrovací algoritmus: 3-DES (RC-2).

2.4. Diffie-Hellman Key Agreement Method (RFC 2631)

Podkladem pro vznik tohoto materiálu byl draft normy ANSI X9.42, přitom byla zvolena jedna speciální varianta DH algoritmu z této normy. Diffie-Hellmanova dohoda na klíči je algoritmus, který používají dvě strany, které se chtějí dohodnout na sdíleném tajemství. Součástí materiálu je i postup jak na základě tohoto sdíleného tajemství vytvářet libovolné množství klíčů (pro symetrickou šifru).

Protože algoritmus může mít i širší využití (mimo rámec S/MIME), je zde uveden jeho popis (s využitím značení z originálu dokumentu).

Jak bylo řečeno, je nejprve počítáno sdílené tajemství, tj. určité tajné číslo ZZ, které bude známo pouze vlastním účastníkům DH algoritmu, tj. přijímající a vysílací straně. Postup je následovný, sdíleným tajemstvím je číslo:

ZZ = g ^ (xb * xa) mod p

Přitom jednotlivé strany toto číslo získají následovně (každá odlišnou cestou):

ZZ = (yb ^ xa) mod p = (ya ^ xb) mod p

kde ^ je symbol označující operaci umocnění a

ya je veřejný klíč strany A; ya = g ^ xa mod p
yb je veřejný klíč strany B; yb = g ^ xb mod p
xa je soukromý klíč strany A
xb je soukromý klíč strany B
p je velké prvočíslo
q je velké prvočíslo
g = h^{(p-1)/q} mod p, kde
h je přirozené číslo, 1 < h < p-1 a platí h{(p-1)/q} mod p > 1
(g je řádu q mod p)
j – pro něj platí p=qj + 1

Generování samotných klíčů probíhá dle vzorce

KM = H (ZZ || OtherInfo),

kde H je hashovací funkce (SHA-1), ZZ je sdílené tajemství (číslo stejné délky jako prvočíslo p, případná chybějící místa jsou doplněna nulami, tj. je-li p dlouhé např. 1024 bitů, je ZZ dlouhé 128 bajtů). Při vytváření klíče je generován jeden nebo více bloků KM (dle potřebné délky klíče).

Prvočísla p a q použitelná pro algoritmus DH dle X9.42 musí splňovat rovnici p=jq + 1 (kde je přirozené číslo větší než 2). Algoritmus pro vytváření takovéto dvojice prvočísel je rovněž součástí materiálu. Stejně tak je dán algoritmus pro generování parametru g.

Soukromý klíč x leží mezi čísly 2 a q-2, a měl by být náhodně generován (délka q je minimálně 160 bitů).

Popisovaná verze DH algoritmu je použitelná v rámci dvou modelů . V prvním z nich (Ephemeral-Static Mode) má přijímající strana pevnou dvojici klíčů (s digitálním certifikátem pro příslušný veřejný klíč), avšak vysílající strana generuje pro každou zprávu novou dvojici klíčů (soukromý a veřejný). Tedy sdílené tajemství ZZ je odlišné pro každou zprávu. V druhém modelu (Static-Static Mode) mají obě strany pevné a certifikované dvojice klíčů. Potom tedy ZZ je totéž pro všechny zprávy a je nutné vytvářet klíče pro symetrické šifrování ještě pomocí další informace známé oběma stranám (není však nutné, aby byla utajována).

2.5. S/MIME Version 3 Certificate Handling (RFC 2632)

Dokument plní stejné funkce pro S/MIME verze 3 jako plní dokument RFC 2312 pro S/MIME verze 2. Hlavní rozdíl spočívá ve využívání PKIX certifikátů (k RFC a draftům skupiny PKIX v rámci IETF se dostaneme v některém z budoucích pokračování seriálu). Odsud vyplývají i odlišné podmínky pro použití jednotlivých algoritmů. Např. rozpoznání použití (přijímajícím agentem) podpisového algoritmu DSA je již obligatorní; velikost RSA klíče je v mezích 512-2048 bitů.

2.6. S/MIME Version 3 Message Specification (RFC 2633)

Opět - tento dokument je analogem RFC.2311 (pro S/MIME verze 2), tj. smysl a filosofie obou dokumentů jsou tytéž, odlišnosti jsou pouze v některých detailech v návaznosti na použité algoritmy. Důležitou odlišností je využití vlastní S/MIME syntaxe definované dle CMS v RFC.2630 (oproti PKCS #7 ve verzi 2 S/MIME). To také umožňuje větší variabilitu při volbě algoritmů. Nezbytnou je možnost generovat parametry pro algoritmus DSA.

2.7. Enhanced Security Services for S/MIME (RFC 2634)

Dokument popisuje další čtyři služby, které S/MIME může (jako opci, tj. volitelně nikoliv povinně) vykonávat. Těmito službami jsou:

- podepsané přijetí zprávy;
- bezpečnostní návěští (spojeno s přístupovými právy ve vztahu k obsahu původního otevřeného textu);
- bezpečné mailové adresáře;
- podepisování certifikátů.

První tři služby jsou analogické službám v protokolu MSP (Message Security Protocol), podepisování certifikátů je důležité tam, kde jsou certifikáty zasílány spolu s podepsanou zprávou.

Tyto služby jsou formulovány jako určitá rozšíření formátu S/MIME verze 3.

2.8. Methods for Avoiding the 'Small-Subgroup' Attacks on the Diffie-Hellman Key Agreement Method for S/MIME (RFC 2785)

Pokud je Diffie-Hellmanův algoritmus pro dohodu na klíči používán v implementacích S/MIME verze 3, je nezbytnou ochrana před tzv. útokem „malé podgrupy“. Ochrana není zadarmo, stojí uživatele určitý čas navíc pro zpracování.

Pokud veřejný klíč protější strany má (při zachované velikosti) malý řád, pak tato strana je schopna získat (v určitých situacích) informace o našem soukromém klíči. Např. pokud získá informace o tom, že daná dešifrace byla či nebyla úspěšná, pokud je dostupný šifrový text zašifrovaný dohodnutým klíčem, atd.

Konkrétně útok může probíhat následovně. Předpokládejme, že stran A má platný veřejný klíč ya a strana B má platný veřejný klíč yb. Přitom řád klíče yb je mnohem menší než q a je roven číslu r. Potom platí yb^r=1 mod p. Strana A nyní vygeneruje sdílené tajemství ZZ jako yb^xa mod p, přitom ZZ má nyní pouze r možných hodnot (namísto q-3). Pokud nyní strana A zašifruje s pomocí ZZ otevřený text a pošle ho straně B, stačí straně B provést totální zkoušky možných hodnot r (namísto q-3 možných hodnot). Až nalezne správnou hodnotu r, získala strana B informaci o čísle xa mod r. Potom stačí získat několik takovýchto hodnot (pro různá r) a činskou větou o reziduích získáme hodnotu soukromého klíče xa (kompletní informaci). Existují i další obdobné útoky.

Jednou z možných ochran je např. následující způsob. Certifikační autorita provádí ověření veřejných klíčů pomocí tohoto jednoduchého algoritmu:

1) ověří zda y leží mezi čísly 2 a p-1. Pokud tomu tak není, je klíč neplatný.
2) Spočte y^q mod p. Jestliže výsledek je roven 1, je klíč platný, v opačném případě nikoliv.

Tento postup lze použít pouze pro pevnou dvojici klíčů (static) nikoliv pro dvojici klíčů s krátkou dobou platnosti (ephemeral).

Certifikační autorita může v rámci rozšíření certifikátů (nebo odkazem na CPS) ujistit zákazníky, že daný klíč prošel příslušným ověřením.

Pokud prvočíslo p bylo generováno tak, že pro něho platí vzorec p-1=2*q*k, kde k je velké prvočíslo nebo součin velkých prvočísel (to znamená větších než q), pak útočník není schopný nalézt efektivně prvky malých řádů, které by mohl využít pro výše popsaný útok. Stále ale existuje jeden známý prvek řádu 2 (číslo p-1) a metoda není využitelná v situacích, kde je kritickou i ztráta jednoho bitu soukromého klíče.

V dokumentech P1363 je specifikována následující metoda chránící proti útoku malé podgrupy. Místo výpočtu ZZ dle vzorce ZZ=yb^xa mod p, spočítá strana A

ZZ=(yb^j)^c mod p,

kde c=j^(-1)*xa mod q. (obdobně strana B). Výsledek musí být různý od čísla 1.

Pokud Diffie-Hellmanova výměna klíčů probíhá pro dva páry klíčů s krátkou dobou platnosti (ephemeral) je zvážení možnosti útoku malé podgrupy zcela nezbytné a je třeba zvolit některý z ochranných postupů. Na druhou stranu jedná se o dvojici klíčů s krátkou dobou platnosti (možná dokonce určenou pouze pro aktuální spojení) a příslušný klíč jako útočník může získat pouze druhá strana v rámci tohoto spojení. Tato strana má však k dispozici stejně patřičný otevřený text a jinak své znalosti využít nemůže.

2.9. Use of the KEA and SKIPJACK Algorithms in CMS (RFC 2876)
Use of the CAST-128 Encryption Algorithm in CMS (RFC 2984)
Use of the IDEA Encryption Algorithm in CMS (RFC 3058)

V nadpisu zmíněná RFC se zabývají použitím specifických kryptografických algoritmů v CMS.

3. Použité zkratky

V následujícím je stručně popsán význam zkratek, se kterými se čtenář může setkat v tomto článku.

ANSI	American National Standards Institute
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One - ISO/IEC norma pro kódování
BER Encoding	Basic Encoding Rules
CAST	symetrický kryptografický algoritmus, autoři Carlisle Adams a Stafford Tavares (Entrust Technologies)
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List (seznam odvolaných certifikátů)
DER Encoding	Distinguished Encoding Rules
DES	symetrický kryptografický algoritmus, bývalá US norma(NIST)
3-DES	symetrický kryptografický algoritmus, současná US norma
DH	Diffie-Hellman (schéma pro výměnu klíčů)
DNS	Domain Name System
DSA	Digital Signature Algorithm (US norma pro dig. podpis)
ESS	Enhanced Security Services
IDEA	symetrický kryptografický algoritmus
IETF	The Internet Engineering Task Force
KEA	Key Exchange Algorithm
MD2	hashovací funkce vzniklá v dílnách firmy RSA
MD5	hashovací funkce vzniklá v dílnách firmy RSA
MIME	Multipurpose Internet Mail Extensions
MSP	Message Security Protocol
NIST	National Institute of Standards and Technology (U.S.A.)
PKCS	Public Key Cryptographic Standard
PKIX	Public Key Infrastructure Exchange, pracovní skupina IETF
RC2	symetrický kryptografický algoritmus, autor Ronald Rivest
RFC	request for comment
RSA	Rivest-Shamir-Adleman – algoritmus asym. kryptografie, první významný kryptosystém s veřejným klíčem
S/MIME	Secure/Multipurpose Internet Mail Extensions
Skipjack	symetrický kryptografický algoritmus
X.509	ITU-T digital certificate.

4. Literatura

[1] S/MIME Mail Security (smime)
http://www.ietf.org/html.charters/smime-charter.html
[2] J.Pinkava. Kryptografické normy díl.6. Normy IETF – S/MIME, část 1., CryptoWorld 4/2001

F. Letem šifrovým světem - přehled vybraných akcí

1. Implementace elektronického podpisu ve veřejné správě , 24. - 25.května , organizátoři ÚVIS + SPIS, Tuchlovice u Kladna, výjezdní zasedání zainteresovaných pracovníků veřejné správy a zvaných odborníků , http://www.spis.cz , http://www.uvis.cz

2. Information Security Summit, 30. - 31.května, Míčovna Pražského hradu - Praha, http://www.dsm.tate.cz

3. SECURITY 2001, 7.června 2001 Praha, pořadatel AEC, informace na http://www.aec.cz (**CD s** prezentacemi jednotlivých účastníků konference bude mimo jiné obsahovat i všechna dosud publikovaná čísla e-zinu **Crypto-World 9/1999 – 4/2001** !)

4. Eighth Annual Workshop on Selected Areas in Cryptography (SAC2001), 16. - 17. srpna, Fields Institute, Toronto, Ontario , Kanada http://lasecwww.epfl.ch/sac2001/

5. 2nd NESSIE Workshop, 12. - 13. září 2001, Royal Holloway, University of London, http://www.isg.fhul.ac.uk/nessie

6. WISA 2001, The 2nd International Workshop on Information Security Applications, 13.-14. září, Seoul, Korea, http://elec.sch.ac.kr/wisa2001

7. Information Security Conference ´01, 1. - 3. října, Malaga, Španělsko, http://www.isconference.org

8. Cryptography - Fundamentals and Applications, výukový seminář, 15.-18. října 2001, Engelberg, Switzerland, vedoucí semináře Ueli Maurer, seminars@dplanet.ch
   témata jednotlivých lekcí : Information Security, Cryptography - Basic Concepts and Terminology, Discrete Mathematics and Terminology, Discrete Mathematics Primer, Theoretical Foundations, Block Ciphers - Design and Cryptanalysis, Stream Ciphers - Design and Cryptanalysis, Hash Functions - Design and Cryptanalysis, Public-Key, Cryptography and Digital Signatures, Probably-Secure Systems, Key Management, Public Key Infrastructures (PKI), Cryptographic Protocols, Digital Payment Systems

9. The 5th Workshop on Elliptic Curve Cryptography (ECC 2001), 17. -19.října , University of Waterloo, Kanada, http://www.waterlooinn.com

10. DATAKON 2001, konference, 20.-23.října 2001, Hotel SANTON, Brno http://www.datakon.cz

11. O čem jsme psali před rokem ?
    Crypto -World 5/2000
    http://www.mujweb.cz/veda/gcucmp/casop2/Crypto5_00.html
    A. Statistický rozbor prvého známého megaprvočísla (P.Tesař, P.Vondruška)
    B. Mersennova prvočísla (P.Vondruška)
    C. Quantum Random Number Generator (J. Hruby)
    D. Sdružení pro bezpečnost informačních technologií a informačních systémů (BITIS)
    E. Code Talkers (II.díl) , (P.Vondruška)
    F. Letem šifrovým světem

G. Závěrečné informace

1.Sešit

Crypto-World je oficiální informační sešit primárně určený pro členy "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní 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 (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://www.mujweb.cz/veda/gcucmp

Pokud se zajímáte pouze o sešit Crypto-World, můžete použít lépe dostupnou adresu:

http://cryptoworld.certifikuj.cz

2. Registrace / zrušení registrace

Zájemci o zasílání tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@uoou.cz (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://www.mujweb.cz/veda/gcucmp/ . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@uoou.cz (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán.

3. Spojení

běžná komunikace, zasílání příspěvků, informace
pavel.vondruska@uoou.cz alias **vondruskap@uoou.cz**

pavel.vondruska@post.cz