Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 4, číslo 5/2002 **17. květen 2002**

5/2002

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/

(342 e-mail výtisků)

Obsah : **Str.**

Příloha: SBKS 2002 – výzva pro autory cfp.pdf

A. Ověření certifikátu poskytovatele
Mgr. Pavel Vondruška, GCUCMP

Úřad pro ochranu osobních údajů (dále Úřad) ověřil ve smyslu § 10 odst. 7 zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) kvalifikovaný certifikát akreditovaného poskytovatele certifikačních služeb První certifikační autority, a.s. Výsledek zveřejnil na své webové stránce www.uoou.cz a ve Věstníku Úřadu č.17.

Poř. čís.	Ověření kvalifikovaného certifikátu poskytovatele			Věstník ÚOOÚ č.
	Subjekt:		Adresa:	
1.	**První certifikační autorita, a.s., identifikační č. 26 43 93 95**		**Podvinný mlýn 2178/6, PSČ 190 00 Praha 9**	**17**
V ý s l e d k y o v ě ř e n í :				
A.	Jméno:	**qica_root_cert_20020321.pem**	Délka: **2265**	Poslední změna: **22. 3. 2002** v **11:14** hod.
	Formát certifikátu:		**O t i s k :**	
	PEM	SHA-1	**4BFB ED36 68FC 2B0A B729 8EC0 53B5 3649 6E15 0AAE**	
		MD5	**297C 49A7 B63C B15A F3B7 0F45 2D3B 5132**	
B.	Jméno:	**qica_root_cert_20020321.der**	Délka: **1630**	Poslední změna: **21. 3. 2002** v **21:02** hod.
	Formát certifikátu:		**O t i s k :**	
	DER	SHA-1	**6E32 893F 22A5 E1CD 9CD6 32E4 10E2 76FF 14B7 66BE**	
		MD5	**C3F3 5AB5 24C7 9276 634B 4DB4 E86A FE57**	
C.	Jméno:	**qica_root_cert_20020321.txt**	Délka: **6256**	Poslední změna: **22. 3. 2002** v **11:18** hod.
	Formát certifikátu:		**O t i s k :**	
	TXT	SHA-1	**AC46 FB40 E929 F12D 758A 0B8E 0192 516B 1B65 6C8A**	
		MD5	**5EAC 0082 F5F5 9E3D EAB4 0FE6 27BE 5ED2**	

O co vlastně jde?

V podmínkách udělení akreditace pro poskytování certifikačních služeb (§ 10 zákona č. 227/2000 Sb.) v odstavci 7 je uložena následující povinnost :
„Součástí rozhodnutí Úřadu o akreditaci je ověření kvalifikovaného certifikátu poskytovatele certifikačních služeb Úřadem“.

V praxi to znamená, že akreditovaný poskytovatel certifikačních služeb předloží Úřadu všechny své kvalifikované certifikáty, které chce používat, a to ve všech formátech, které nabízí (zpravidla DER, TXT a PEM, případně EDI). Jedná se o kvalifikované certifikáty poskytovatele, které je nutné instalovat do uživatelských aplikací a které slouží k ověření podpisů kvalifikovaných certifikátů a CRL (seznamu kvalifikovaných certifikátů, které byly zneplatněny). Těmto certifikátům musí uživatel důvěřovat a měl by je získat nějakým

důvěryhodným způsobem. Poskytovatel (zjednodušeně řečeno) nesmí používat pro výše uvedené účely jiné, než tyto ověřené kvalifikované certifikáty.

Připomeňme si některé další povinnosti poskytovatele, které se vztahují k těmto ověřeným certifikátům. Tyto povinnosti jsou stanoveny především ve vyhlášce č. 366/2001 Sb. v § 3 : **„Bezpečnost postupu při vydávání kvalifikovaných certifikátů a provozování seznamu kvalifikovaných certifikátů, které byly zneplatněny“**

„(1) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podepisuje zaručeným elektronickým podpisem kvalifikované certifikáty a seznamy kvalifikovaných certifikátů, které byly zneplatněny. Tento zaručený elektronický podpis musí být založený na kvalifikovaném certifikátu poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty.“

„(4) V případě, že jsou data pro vytváření elektronického podpisu používána pro podepisování vydávaných kvalifikovaných certifikátů a pro podepisování seznamu kvalifikovaných certifikátů, které byly zneplatněny, nelze je použít pro jiné účely.

(5) Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty zajistí dostupnost svého kvalifikovaného certifikátu nejméně dvěma na sobě nezávislými způsoby.

(6) Seznam kvalifikovaných certifikátů, které byly zneplatněny, je provozován tak, aby jeho dostupnost byla zajištěna nejméně dvěma na sobě nezávislými způsoby, které umožňují dálkový přístup a jsou nepřetržitě dostupné.“

Zveřejněné otisky ověřených kvalifikovaných certifikátů akreditovaného poskytovatele slouží k tomu, aby před instalací kvalifikovaného certifikátu akreditovaného poskytovatele certifikačních služeb byla možnost porovnáním otisků zjistit, zda:

- kvalifikovaný certifikát byl skutečně ověřen Úřadem,
- zda kvalifikovaný certifikát byl vydán příslušným akreditovaným poskytovatelem certifikačních služeb,
- zda se jedná o kvalifikovaný certifikát, který „certifikuje“ data pro ověřování elektronického podpisu, kterým odpovídají data pro vytváření elektronického podpisu, kterými akreditovaný poskytovatel „podepisuje“ vydávané kvalifikované certifikáty a seznamy kvalifikovaných certifikátů, které byly zneplatněny.

Tuto kontrolu lze provádět (a je vhodné ji provádět) i následně. Jejím smyslem je ověření, že někdo cizí/neoprávněný nenahradil instalovaný certifikát akreditovaného poskytovatele jiným certifikátem, který vydal „útočník“. Takovýto certifikát může formálně obsahovat všechna data shodná s daty akreditovaného poskytovatele, samozřejmě s výjimkou podpisu poskytovatele.

Pokud nezjistíme, že někdo takovouto záměnu provedl, pak certifikáty, které vydal „útočník“, jsou ověřeny jako platné a domníváme se, že je vydal akreditovaný poskytovatel certifikačních služeb.

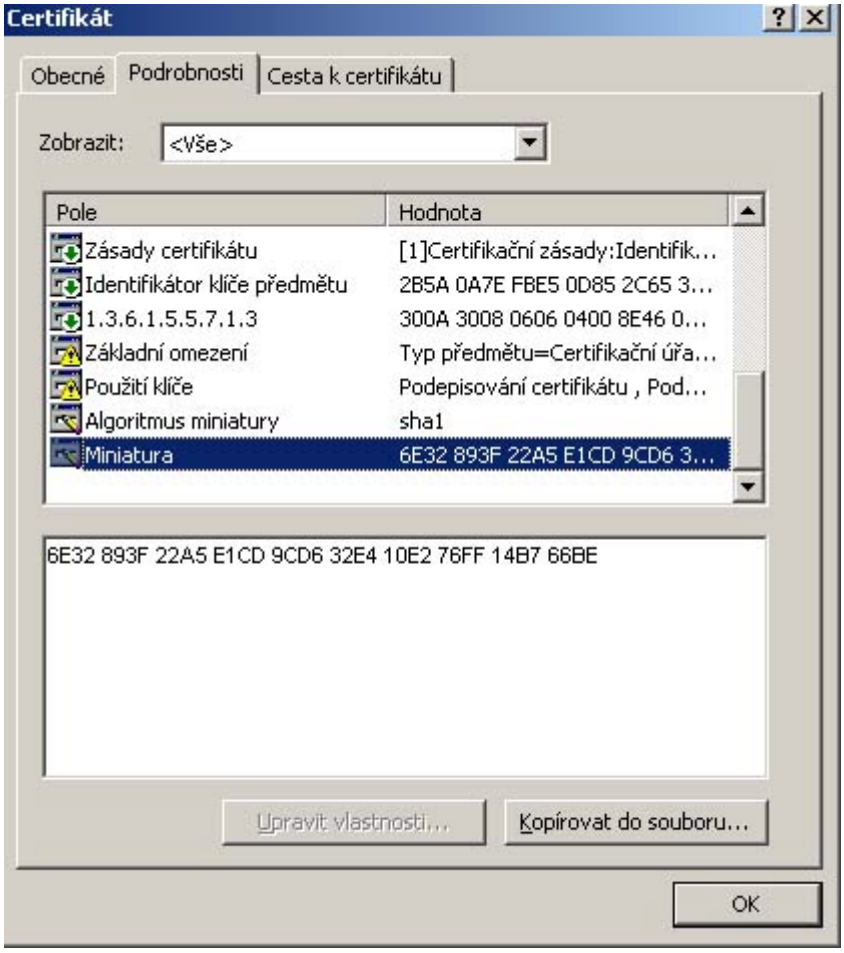
Otisky zveřejněné Úřadem byly počítány z obsahu celého souboru – certifikátu v příslušném formátu, a to podle následujících standardů:

SHA-1 (National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-1, April 17, 1995)

a

MD5 (Request for Comments: 1321, The MD5 Message-Digest Algorithm, R. Rivest, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992).

V případě kvalifikovaného certifikátu poskytovatele (v nejběžněji používaném formátu DER) se můžete velice jednoduše přesvědčit, zda máte stažený/nainstalovaný certifikát ověřený Úřadem. Stačí v některém z viewerů (např. v produktech MS Outlook, MS Internet Explorer) otevřít certifikát, o němž chceme rozhodnout, zda je či není ověřen Úřadem. Zobrazí se nám následující (nebo jemu velice podobný – podle verze produktu) výsledek :



V položce „miniatura“ pak najdeme otisk certifikátu. Použitá hashovací funkce je uvedena v položce „algoritmus miniatury“ (zpravidla SHA-1). Nyní stačí porovnat tento otisk s otiskem uvedeným ve Věstníku Úřadu, resp. s otiskem, který je zveřejněn na webovské stránce Úřadu, nebo jej máte z jiného zdroje – např. z tohoto čísla Crypto-Worldu. Věstník Úřadu lze považovat za důvěryhodný zdroj, další zdroje mají pochopitelně spíše informativní povahu.

Pro otisk kvalifikovaného certifikátu První certifikační autority a.s. ve formátu DER je uvedena v těchto zdrojích hodnota: 6E32 893F 22A5 E1CD 9CD6 32E4 10E2 76FF 14B7 66BE.

Porovnáním zjistíme, že tato hodnota je shodná s údajem v miniatuře – jedná se tedy o kvalifikovaný certifikát poskytovatele, který byl ověřen Úřadem. Na takovýto certifikát se můžete spolehnout a nic nebrání jeho instalaci.

Pro porovnání certifikátů v ostatních formátech potřebujete k výpočtu otisků použít některou z dostupných aplikací. Takto vypočtený výsledek opět jednoduše porovnáte s hodnotou otištěnou ve Věstníku. Úřad připravuje zveřejnění vhodné aplikace pro výpočet otisků certifikátů pomocí hashovacích funkcí SHA-1 a MD5 na své webovské stránce (http://www.uoou.cz).

B. Radioaktivní rozpad a kryptografické klíče (pokračování)

Dr. Luděk Smolík, seculab s.r.o., lsmolik@web.de
Dieter Schmidt, Universität Siegen, NSR

Tématem prvního článku (Cryptoworld 6/2001) byl popis fyzikální podstaty zařízení typu „True Random Number Generator“ (TRNG), který na rozdíl od „Deterministic Random Number Generator“ (DRNG) obsahuje fyzikální zdroj náhodných informací. U DRNG je zdrojem informací matematický algoritmus , který sice splňuje některé požadavky na statistickou kvalitu generovaných čísel, ale nelze být konstruován tak, aby splnil požadavek nepředvídatelnosti generovaných čísel. Jednoduše řečeno, je jedno jak rafinovaný algoritmus se v generátoru skrývá, množina generovatelných čísel zůstane vždy konečná, což na druhou stranu znamená, že lze (alespoň teoreticky) z posloupnosti generovaných čísel předpovědět následující.

V druhé části bychom Vás rádi seznámili s problematikou testů náhodnosti náhodných čísel a s tím spojenou stále se opakující otázkou po důvěryhodnosti takovýchto čísel.
Nebudu nosit dříví do lesa a pro stručné uvedení testovacích algoritmů se odkážu na obšírný článek pana doktora Tesaře v Cryptoworld 2/2002 .

Proč je ale potřebné zabývat se vůbec touto otázkou ? Nejtypičtější využití náhodných čísel při výpočetní simulaci je dnes každému studentu dobře známé. Zde se spokojíme většinou s pouze statisticky náhodnými čísli a uplatnění najdou různé dobře prozkoumané druhy DRNG. Laicky řečeno tato čísla musí plnit číselný interval hlavně rovnoměrně. Informace, která je skrytá v posloupnosti čísel, musí být minimální, aby se právě neprozradila vůči nastaveným limitům testovacích kritérií a nebo aby nezpůsobila systematické efekty ve výpočtech.

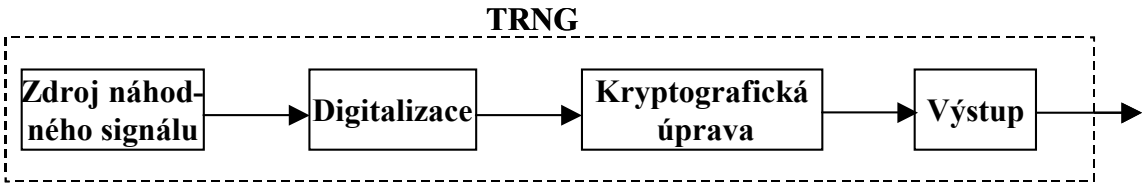
Pro kryptokrafické účely s nejvyššími požadavky na kvalitu a důvěryhodnost ale tyto generátory typu DRNG zdaleka nestačí. K požadavkům se zde přidruží již jmenovaná nepředvídatelnost generovaných čísel, což je vlastnost právě doslova ortogonální k tomu, co je podstatou deterministických algoritmů.
Proto je potřeba kryptografickou způsobilost zařízení pro tvoření náhodných čísel dokázat.
Ne, skutečnost je ještě komplikovanější. Nestačí jenom dokázat, že zařízení vytvořilo náhodná čísla v minulosti, ale je nutný formální důkaz toho, že je bude tvořit alespoň teoreticky nekonečně dlouho dále. Jakákoliv odchylka od této důslednosti může být použita pro budoucí, nám dnes ještě neznámý útok. Nezasvěcenému čtenáři se možná zdají podobné požadavky až přemrštěné a diskuze akademická ale nepříjemné případy minulosti nás poučily (kupříkladu PGP, Netscape, GSM a další). A konečně, klíče pro elektronický podpis mají přetrvat více než jenom pár týdnů nebo měsíců.

V důkazu se právě nachází hluboký rozdíl mezi deterministickým a fyzikálním generátorem.

U deterministického generátoru je formální, matematický důkaz vcelku snadný. Jedno kdy a kde na světě a jedno v jaké aplikaci se tyto generátory právě spustí, budou fungovat lépe nebo hůře ale vždy s jim *implementovanou* výkonností.
U fyzikálního generátoru je formální důkaz prakticky neproveditelný. Samozřejmě nebude nikdo z nás zpochybňovat platnost známých fyzikálních zákonů, ale nepřehledné množství a provázanost všech možných systematických efektů, které mohou ovlivnit funkci, znesnadňují formulaci seriózního formálního důkazu. Kromě toho je důkaz nekonečného chaosu (maximální entropie), který by museli generované čísla vykazovat již sám o sobě z praktického časového hlediska neproveditelný.

Jak tedy řešit toto vzniklé dilema ? Dnes praktikované východisko je vcelku pragmatické, monitoruje se „on-line“ výstup generátoru a kontroluje se statistická kvalita generovaných čísel. Ucelený a propracovaný katalog testů a návod pro klasifikaci zařízení pro

nasazení v certifikačních autoritách najdeme kupříkladu v [1] a [2]. Propaguje se zde ovšem strategie dvojnásobné bezpečnosti. Pojem TRNG je rozšířen o proces tak zvané kryptografické úpravy, při které se vstupující bitová posloupnost po digitalizaci náhodného signálu podrobuje další matematické operaci, která by neměla podstatně snižovat entropii vstupující informace. Je ovšem obtížné toto tvrzení „on-line“ kontrolovat, neboť materiál pro výrobu klíčů by neměl být pro analýzu hromaděn na nějakém paměťovém médium (s výjimkou výpočetní paměti samotné). Míra entropie nemůže být teoreticky zvýšena, jelikož se při kryptografické úpravě jedná o matematickou to znamená opět o deterministickou operaci



Obrázek 1: Schéma fyzikálního generátoru podle [1] a [2]

Vrátíme se nyní k testu našeho generátoru [3]. Data byla analyzována po digitalizaci signálu, to znamená testován byl přímo fyzikální generátor. Změny vznikající následující kryptografickou úpravou nebyly cílem našeho studia.

Bitové posloupnosti byly podrobeny testům Golomb I,II,III, a poker testům pro 2 a 4 bity.
Golomb I test měří poměr frekvence výskytu bitových stavů „0“ a „1“.
Golomb II test měří výskyt tak zvaných sériích stejných bitů. Analyzovali jsme série délky 1 až 12 bitů.
Golomb III testuje autokorelaci bitové posloupnosti. Autokorelační funkce byly tvořeny pro všechna posunutí mezi 1 a 16 bity.
Poker testy měří relativní pravděpodobnost výskytu bitových vzorků.
Pro 2-bit poker se analyzuje výskyt vzorků: 01, 10, 00 a 11, očekává se relativní pravděpodobnost 1/4 pro každý vzor.
Analogicky je pravděpodobnost pro každý vzor 4-bitového pokeru 1/16.

Analyzováno bylo 16000 datových řad každá délky 4 kByte. Pro každou řadu byla vypočítána hodnota χ^2 patřičného testu.
Pro ilustraci zde uvádíme vzorec pro výpočet χ^2-hodnoty 4-bit pokeru:

$$\chi^2 = \sum_{i=1}^{m=16} \frac{\left(n_i - n/64\right)^2}{n/64}$$

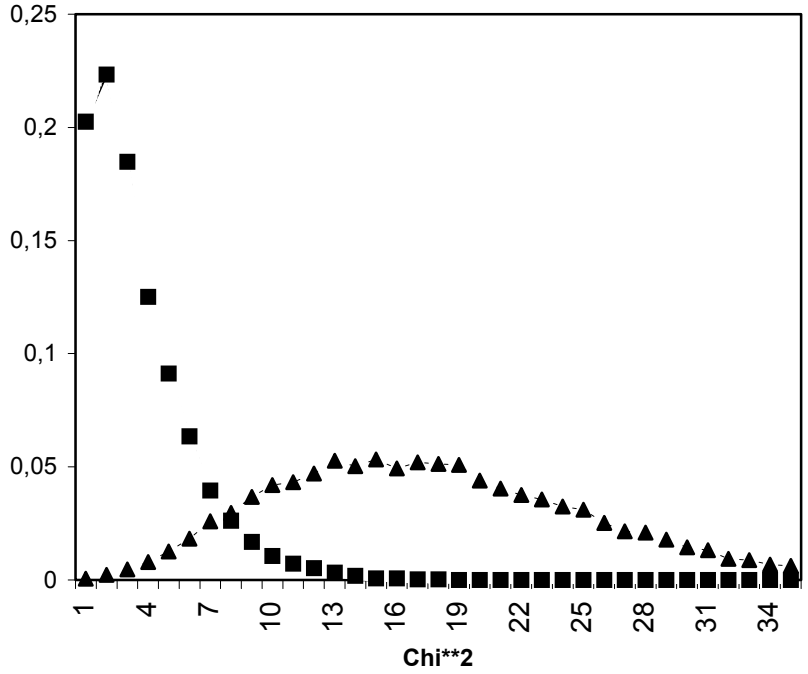
Přičemž je n délka datové řady v našem případě 4096 bitů dlouhá, n_i znamená počet i-té varianty 4-bitového pokeru ve zkoumané řadě a index i běží přes všech 16 možných variant.
Výsledkem každého výše uvedeného testu byl tedy histogram, do kterého vstoupilo vždy 16000 χ-kvadrátů. Tato experimentální rozložení byla přiblížena teoretickou křivkou a byla opět spočítána χ^2 hodnota tohoto přiblížení. V následující tabulce jsou uvedeny výsledky testů ve formě konečné χ^2 hodnoty. Všechny testy potvrzují hypotézu nahodilosti generovaných čísel.

Testovací kritérium	χ^2	**1% kvantila**	**0,1% kvantila**
I Golomb	74,2	76,2	89,1
II Golomb	34,1	52,7	60,9
III Golomb	44,4	60,4	69,2
2 poker	52,5	57,8	67,4
4 poker	51,8	60,4	69,2

Tabulka 1: Výsledky testů

V rámci diplomové práce [4] jsme nezávisle studovali jeden komerční TRNG, který používá též radioaktivní rozpad jako zdroje náhody a podrobili ho stejným testům se stejně velkou statistikou. Tento generátor je prakticky předchůdcem zde popsaného zařízení, byl evaluován a certifikován v roce 1999 jednou německou laboratoří a v rámci akreditace jedné z největších německých certifikačních autorit: Tento TRNG byl připuštěn do provozu a pracuje jako součást generátoru kryptografických klíčů podle kategorie „E4/síla mechanizmu vysoká“ dodnes.

Obrázek 2 demonstruje výsledky měření. Jako příklad jsme zvolili již představený 2 poker test. Na ordinátě jsou naneseny χ^2 hodnoty a na abszise relativní počet měřeného výskytu. Pro snadnější srovnání jsou křivky normalizovány na plochu 1. Šedá křivka je výsledek teoretické předpovědi pro χ^2 rozdělení pro očekávanou hodnotu 3 stupňů volnosti, a dobře přibližuje měření (černé čtverce) s našim zařízením [3]. Očekávaná hodnota je 3, protože součet pravděpodobností pro výskyt kombinací 00, 11, 01, a 10 je roven 1, a proto jsou jenom 3 sčítanci lineárně nezávislí. Výsledky měření s komerčním TRNG jsou zobrazeny též na obrázku 2 jako černé trojúhelníky. Zde vidíme, že kvalita náhodnosti generovaných čísel je podstatně nižší než v našem případě. Prakticky ve všech testech jsme našli podobné výsledky a tento fakt zde opodstatňuje obavy a potřebu kryptografické úpravy ([1], [2]), která je předepsaná pro nasazení kupříkladu v certifikačních autoritách.



Obrázek 2: Výsledky 2-poker testů

Závěr

Privátní klíč pro elektronický podpis je prototyp snad dnes nejchoulostivějšího využití náhodných čísel. O nosnosti současného veřejného vnímání elektronického podpisu rozhodne především důvěra v nabídnuté služby certifikačních autorit. Za kvalitou klíčů pro kvalifikovaný elektronický podpis vytvořený na domácím počítači pomocí aplikací stojí stále ještě velký otazník.V uplynulém roce byly akreditované čipové karty, které vytvářejí náhodné číslo přímo ve vlastním čipu a tím garantují, že výsledný klíč opravdu kartu nikdy neopustil. Domníváme se ale, že i zde je potřeba vyčkat praktických zkušeností a dalších nezávislých testů.

Reference:

[1] Anonymus: AIS 31 –Anwendungshinweise und Interpretation zum Schema, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlgeneratoren, Version 1, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 25.9.2001, http://bsi.bund.de/zertifiz/zert/interpr/ais31.pdf

[2] Killmann Wolfgang; Schindler Werner: Ein Vorschlag zu: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlgeneratoren, Version 3.1, T-Systems debis Systemhaus Information Security Services und Bundesamt für Sicherheit in der Informationstechnik, Bonn, 25.9.2001, http://bsi.bund.de/zertifiz/zert/interpr/trngkr.pdf

[3] Grupen Claus; Maurer Ingo; Schmidt Dieter; Smolík Luděk: Generating Cryptographic Keys by Radioactive Decays, Proceedings of the 3rd. International Symposium on Nuclear and Related Techniques (NURT 2001), Havanna (Cuba), November 2001

[4] Schmidt Dieter; Erzeugung echter Zufallszahlen mit Hilfe radioaktiver Zerfälle, Diplomarbeit, Universität Siegen, May 2002

C. Kryptografie a normy
Digitální certifikáty. IETF-PKIX.
Část 3. Řídící protokol CMP.

Jaroslav Pinkava, AEC spol. s r.o.

1.Úvod

Jak již bylo řečeno v první části, součástí materiálů pracovní skupiny IETF-PKIX jsou protokoly určené pro řízení informací, které se vztahují k PKI. Prvním z těchto protokolů je protokol CMP (Certificate Management Protocol). Tento definuje zprávy vztažené k inicializaci, certifikaci, obnově a odvolávání entit PKI a bude mu věnována tato část seriálu.

Dvě pracovní skupiny (IETF-S/MIME a IETF-PKIX) vyvinuly dva různé dokumenty vztahující se k žádostem o certifikát. CRS (Certificate Request Syntax) vyvinula skupina S/MIME, která přitom použila formát dle PKCS-10 (viz dřívejší části seriálu Kryptografické normy v Crypto-Worldu). Jiný typ formátu CRMF (Certificate Request Message Format) vyvinula skupina PKIX. Tento se opírá jak o CMP tak i o přihlášení dle CRS, ale nepoužívá formát žádosti dle PKCS-10.

Těmto specifikacím a také protokolu CMC, který napomáhá využívání protokolu pracovní skupiny S/MIME pro řízení PKI bez nutnosti využití CMP (používá PKCS-10) budou věnovány následující části.

2. Protokol CMP

Praktické řízení činnosti PKI musí být formováno tak, aby nebránilo efektivnímu využití potenciálu PKI. Nezbytné je umožnit podporu interakce jednotlivých komponent PKI a to on-line (například mezi CA a systémem zákazníka, mezi dvěmi CA atd.).

V následujícím je použit popis z [1] , tj. RFC 2510.

Entity PKI

V modelu řízení PKI jsou zahrnuty koncová entita (tj. např. entita pojmenovaná v poli "subject" digitálního certifikátu – v dalším bude nazývána také subjektem) a certifikační autorita. Může zde být i registrační autorita. Koncovou entitou nejsou chápány pouze fyzické osoby jako uživatelé příslušných aplikací, ale také samotné aplikace.

Všechny koncové entity potřebují bezpečný (lokální) přístup k některým informacím (minimálně k vlastnímu jménu a soukromému klíči, jménu odpovídající CA a veřejnému klíči této CA atd.). Forma uložení těchto dat může být různá (od datových souborů k bezpečným fyzickým tokenům) a je nazývána personální bezpečné prostředí (Personal Security Enviroment – PSE).

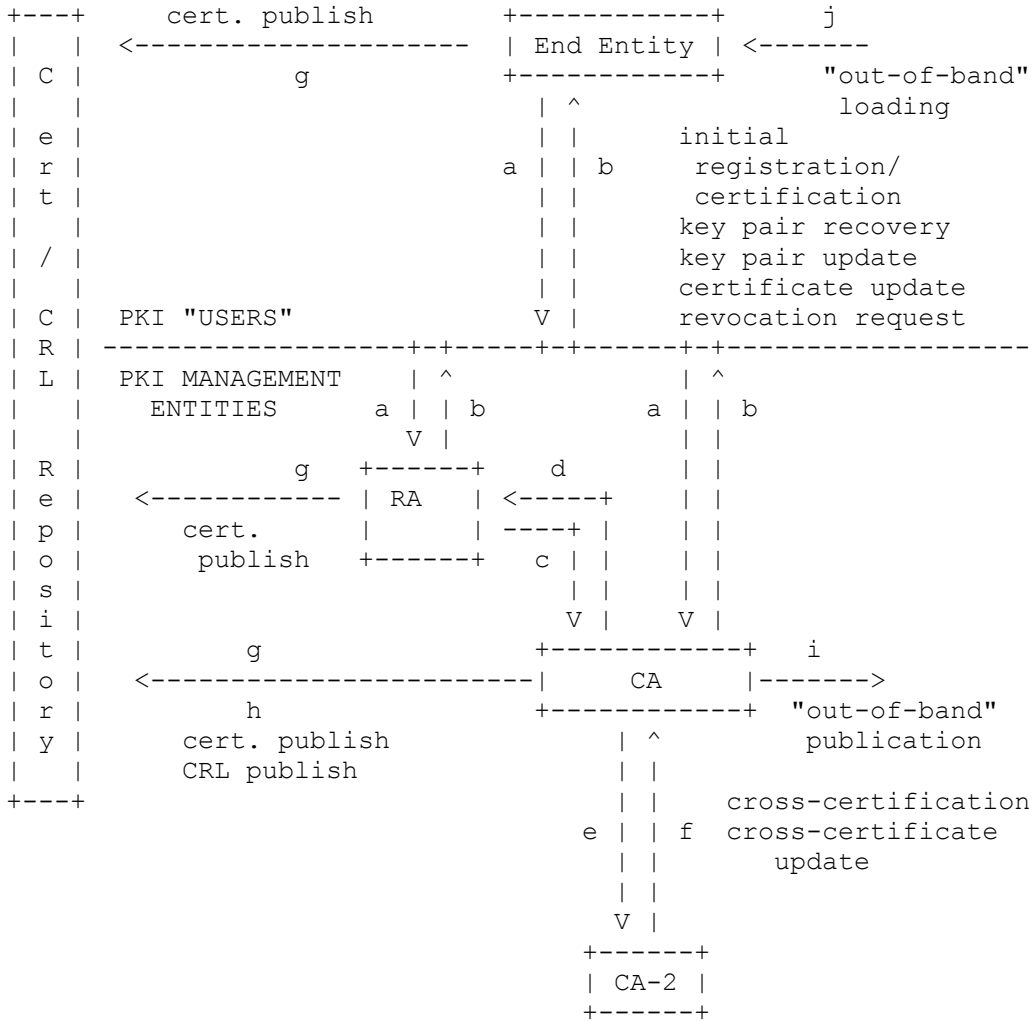
Řízení PKI

Protokoly pro řízení PKI (v rámci materiálů IETF-PKIX) musí vyhovovat celé řadě požadavků. Jedná se např. o podobu rozšíření certifikátů (norma ISO/IEC 9594-8), protokoly musí být také ve shodě s ostatními dokumenty skupiny PKIX. Obnova jednotlivého klíčového páru nesmí ovlivnit jiné klíčové páry, vhodnou cestou je třeba řešit otázky utajení (tyto požadavky nesmí být na překážku regulačních prostředků), řídící protokoly musí umožňovat implementace řady různých kryptografických algoritmů (včetně RS, DSA, MD5, SHA-1) včetně cest ke generování vhodných kryptografických klíčů. Protokoly musí podporovat zveřejňování certifikátů příslušnou koncovou entitou resp. RA či CA, dále vytváření a zpřístupnění CRL. Protokoly musí umožnit svoje využívání prostřednictvím celé

řady různorodých "přepravních" mechanismů (mail, http, TCP/IP a ftp). Existující politiky musí umožňovat všem entitám PKI reakci na certifikát (vydaný CA), který neodpovídá požadavkům v žádosti o certifikát (některé politiky dokonce stanoví, že CA nesmí příslušný certifikát zveřejnit pokud nebyl žadatelem akceptován). Vhodnou cestou musí být podporována obnova (nezkompromitovaného) klíče CA.

Pokud koncová entita požaduje vydání certifikátu s danou hodnotou veřejného klíče, musí být tato koncová entita schopná demonstrovat důkaz, že vlastní odpovídající soukromý klíč.

Následující obrázek ukazuje vztahy mezi jednotlivými entitami v rámci PKI řídících operací.



Množinu operací, pro které jsou definovány řídící zprávy lze rozčlenit následovně:

- ustavení CA (nové CA, např, vydání úvodního CRL, export veřejného klíče CA atd.);
- inicializace koncové entity (import veřejného klíče kořenové CA,…);
- práce s certifikáty (vstupní registrace koncové entity až po vydání certifikátu danou CA, dále obnova klíčového páru, obnova certifikátu, obnova klíčového páru CA, požadavky na křížovou certifikaci, resp. obnova křížového certifikátu).
- publikování certifikátů resp. CRL;
- prostředky obnovy (v situacích, kdy koncová entita "ztratí" své PSE – rozkrytí klíčového páru – "key recovery");
- operace pro odvolání (žádost o odvolání) – vyústí v nový vstup v rámci CRL;
- operace s PSE (fyzický přesun, změna PIN atd.) .

Dále jsou uvedeny základní vstupní údaje a omezení týkající se řízení PKI.

1. *Inicializace koncové entity* (koncová entita jako první krok vznáší požadavek na získání informací o podporovaných PKI funkcí a bezpečnou cestou požádá o vydání veřejného klíče kořenové CA).

2. *Vstupní registrace resp. certifikace* (existuje celá řada různých postupů, některé jsou mandatorní, některé nepovinné). Lze je rozčlenit dle místa, kde je vstupní registrace resp. certifikace iniciována, dle autentizace zpráv koncové entity, místa generování klíčů a způsobů schválení úspěšného průběhu certifikace.

3. *Mandatorní (závazná) schémata*. Z hlediska RFC 2510 je závazným schématem tzv. základní autentizační schéma (odstavec 2.2.2.2). Jeho průběh znázorňuje následující obrázek:

```
Koncová entita                                          RA/CA
==========                                           =============
      Vstupní autentizace (jinou cestou)
     Klíč (IAK) a referenční hodnota (RA/CA -> EE)
Generování klíče
Vytvoření žádosti o certifikát
Žádost chráněná s IAK
              -->>--žádost o certifikát-->>--
                                                 ověření žádosti
                                                 zpracování žádosti
                                                 vytvoření odpovědi
              --<<--odpověď--<<--
zpracování odpovědi
vytvoření konfirmace (schválení)
              -->>--konfirmační zpráva-->>--
                                                 ověření konfirmace
```

4. *Důkaz vlastnictví soukromého klíče* (POP - Proof of Possesssion) je nezbytný z hlediska bezpečnosti uváděných postupů, proto PKI řídící operace definují, jak koncová entita prokáže, že příslušný soukromý klíč vlastní. Vlastní průběh POP závisí také na účelu příslušného certifikátu. Podpisový klíč – koncová entita podepíše nějaká data, tím prokáže vlastnictví soukromého klíče. Šifrovací klíč – koncová entita (např.) dešifruje zaslaná data dříve zašifrovaná veřejným klíčem. Tzv. nepřímá metoda postupuje tak, že uživateli je příslušný certifikát zaslán celý zašifrovaný. Klíče pro dohodu na klíči – koncová entita a PKI řídící entita (CA, RA) ustaví spolu sdílený tajný klíč tak, aby bylo prokázáno, že koncová entita vlastní příslušný soukromý klíč.

5. *Obnova klíče kořenové CA*. K ochraně nového veřejného klíče je použit dřívější soukromý klíč. Po vygenerování (operátorem CA) nové dvojice klíčů je vytvořen certifikát, který obsahuje starý veřejný klíč CA podepsaný novým soukromým klíčem. Dále je vytvořen certifkát obsahující nový veřejný klíč CA podepsaný starým soukromým klíče a taktéž certifikát obsahující tento nový veřejný klíč CA podepsaný novým soukromým klíčem. Tyto nové certifikáty jsou zveřejněny resp. předány koncové entitě jinou cestou (out-of-band).Starý soukromý klíč CA již dále není zapotřebí, avšak starý veřejný klíč CA bude ještě nějakou dobu používán (dokud všechny koncové entity CA nezískaly bezpečnou cestou nový veřený klíč CA). Vhodně upraveny musí být samozřejmě i příslušné doby platnosti jednotlivých

certifikátů. V případě obnovy klíče CA se podstatně také rozšiřují cesty pro ověřování digitálních podpisů, totéž platí i pro ověřování CRL.

Datové struktury pro zprávy (řízení PKI).

Všechny zprávy používané pro řízení PKI a pracující ve shodě s RFC.2510 mají následující strukturu:

```
PKIMessage ::= SEQUENCE {
    header           PKIHeader,
    body             PKIBody,
    protection   [0] PKIProtection OPTIONAL,
    extraCerts   [1] SEQUENCE SIZE (1..MAX) OF Certificate OPTIONA   }
```

Hlavička nese informace nezbytné pro zadání adres a identifikaci. Tělo obsahuje vlastní zprávu a pokud je využito pole PKIProtection, pak nese informaci sloužící k ochraně zprávy. Poslední pole obsahuje certifikáty, které mohou být užitečné pro příjemce zprávy.

Podrobnější informace o podobě konkrétních struktur vážících se k jednotlivým typům zpráv (pro řízení PKI) jsou obsaženy v[1] .

Závaznými funkcemi pro řízení PKI jsou následující činnosti:

- inicializace kořenové CA (vydání "self-signed" certifikátu);
- obnova klíče kořenové CA;
- inicializace podřízené CA;
- vytvoření CRL;
- žádost o informace vzhledem k činnosti PKI;
- křížová certifikace;
- inicializace koncové entity;
- žádost o certifikát;
- obnova klíče.

Přenosové protokoly používané pro zprávy vzhledem k řízení PKI jsou následující:

- přenos samostatných souborů (musí obsahovat pouze jednu zprávu DER kódovanou);
- TCP řídící protokol (předpokládá port na CA, RA akceptující zprávy PKI);
- řídící protokol zasílaný e-mailovou poštou (MIME objekt – kódování obsahu - DER+base64);
- protokol zasílaný přes http (MIME objekt obsahující DER kódovanou zprávu).

V přílohách k [1] jsou obsaženy podrobnosti k profilům jednotlivých zpráv pro řízení PKI (základní pravidla, označení a použití vlastních kryptografických algoritmů, self-signed certifikáty, důkaz vlastnictví klíče, obnova klíče kořenové CA atd.). Obsaženy jsou zde také příslušné moduly ASN.1.

3. Literatura

[1] Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510) (158178 bytes)
[2] Internet X.509 Certificate Request Message Format (RFC 2511) (48278 bytes)
[3] Certificate Management Messages over CMS (RFC 2797) (103357 bytes)
[4] Internet X.509 Public Key Infrastructure Certificate Management Protocols (202678 bytes)
[5] Transport Protocols for CMP (22793 bytes)
[6] Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) (49976 bytes)

D. Je 1024-bitová délka klíče RSA dostatečná?

Jaroslav Pinkava, AEC spol. s r.o.

Pokud si tuto otázku položíme v tom smyslu, zda dnes někdo umí rozbít RSA algoritmus při délce ***n*** (součin dvou prvočísel) rovné 1024 bitů, pak odpověď je nepochybně záporná. Ani pan Bernstein ani nikdo jiný **neprokázal**, že má k dispozici takovýto algoritmus.

Jiná otázka je, že algoritmus RSA je dnes využíván v praxi tak intenzivně, že je třeba se zamýšlet i nad jeho perspektivou. Samozřejmě podstatou se tato otázka se netýká jen jeho, ale týká se celé symetrické i asymetrické kryptografie.

Vhodné je zde připomenout zvolenou filosofii při přípravě americké normy AES. Algoritmy, z nichž byla norma vybírána, byly koncipovány tak (a to bylo již předem zadáno), že každé ze schémat mělo umožňovat volitelné tři stupně bezpečnosti dle použité délky klíče (128, 192 a 256 bitů). Přitom i nejkratší délka klíče (128 bitů) má v sobě zabudovanou určitou „bezpečnostní rezervu“ (samozřejmě navíc mocnina dvojky má výhodu v implementacích). Obdobný postup volí i evropská iniciativa Cryptonessie (s tím rozdílem, že jsou tu jen dva stupně). Pokud dojde k nějakým významným posuvům ve výpočetních technologiích, je tu stále šance, že můžeme pracovat s týmiž algoritmy při větší délce klíče.

Tato filozofie rezerv se zdá být velmi rozumná a nikdo jiný než NIST na svých stránkách dokonce oznámil, že jí hodlá přizpůsobit i připravovanou novou verzi normy pro podpisové algoritmy (http://csrc.ncsl.nist.gov/encryption/tkdigsigs.html). Týká se to i hashovacích funkcí, kde již v tomto směru byl vydán předběžný návrh (s délkami hashe 256, 384 a 512 bitů).

Filozofie rezerv není v kryptologii ničím novým. Už v první polovině minulého století byla konstruována různá kryptografická zařízení obsahující např. kromě běžného směnného prvku i např. tzv. záložní směnný prvek, který měl být využíván v situacích, kdy základní schéma se stalo slabým (v důsledku rozvoje kryptoanalytických metod).

Naopak pokud pracujeme s délkou klíče, která má pouze malou rezervu z hlediska dnešních možností, pak sice lze vyhlašovat, že pracujeme s bezpečnou délkou klíče, ale vzniká otázka jak dlouho takovéto naše tvrzení vydrží. Typickým příkladem byla původní americká norma DES s délkou klíče 56 bitů. Zde právě tato malá délka klíče byla již vlastně od samého vzniku normy předmětem celé řady diskusí a kritiky.

Z tohoto hlediska je nespornou výhodou algoritmů na bázi *eliptických křivek*, že takováto přizpůsobení (v návaznosti např. na AES – obdobné rozdělení na třídy bezpečnosti) se zde dají provést velice snadno (současná doporučení se shodují na tom, že zhruba řečeno pro dosažení analogické bezpečnosti – jako pro symetrický algoritmus - je třeba použít dvojnásobnou délku klíče).

Pro algoritmus RSA je ovšem celá situace poněkud složitější. Jaké máme doporučit délky klíče (přesněji čísla ***n=pq***)? Pokud chceme aplikovat výše uvedenou filozofii, pak nejprve potřebujeme stanovit doporučení pro první bezpečnostní stupeň a to tak, aby zde byly dostatečné bezpečnostní rezervy a následně stanovit i obdobná doporučení pro vyšší bezpečnostní stupně.

Jaké by to měly být délky klíčů? Odpověď na tuto otázku vyžaduje určitě poměrně pečlivou analýzu a je proto nejlépe (pokud to lze) se odkázat na analýzy odborníků.

V roce 1995 se skupina známých kryptografů a vědců pokusila odhadnout minimální délku klíče pro symetrické šifry. Opublikovali svůj odhad v článku [3]. Jejich tehdejší závěr: Klíče symetrických šifrovacích algoritmů (použitých pro ochranu dat) by měli mít délku minimálně 75 bitů. Pro takové potřeby, kde je nutno zachovat bezpečnost zašifrovaných informací ještě pro období následných 20 let, doporučují používat symetrické algoritmy s minimální délkou klíče 90 bitů.

Velice fundovaně a na základě značně sofistikovaných argumentů se problematikou délky klíče zabývají v článku [4] pánové Arjen K. Lenstra and Eric R. Verheul. Následně je uvedena část tabulky, která shrnuje jejich závěry:

The Table from the Lenstra/Verheul research (část)

Year	Symmetric Key Size (bits)	Classical Asymmetric Key Size (RSA, Elg, DH) (in bits)	Subgroup Discrete Logarithm Key Size (DSA, Schnorr) (bits)	Elliptic Curve Key Sizes (in bits)		Security Margin (Mips Years)	Corresponding no. of Years on 450MHz PentiumII PCs	Corresponding (minimal) Budget for Attack in 1 Day (USD)
				Progress				
				no	yes			
1982	56	417	102	105		$5.00 * 10^5$	$1.11 * 10^3$	$3.98 * 10^7$
1985	59	488	106	110		$2.46 * 10^6$	$5.47 * 10^3$	$4.90 * 10^7$
1990	63	622	112	117		$3.51 * 10^7$	$7.80 * 10^4$	$6.93 * 10^7$
1995	66	777	118	124		$5.00 * 10^8$	$1.11 * 10^6$	$9.81 * 10^7$
2000	70	952	125	132	132	$7.13 * 10^9$	$1.58 * 10^7$	$1.39 * 10^8$
2002	72	1028	127	135	139	$2.06 * 10^{10}$	$4.59 * 10^7$	$1.59 * 10^8$
2005	74	1149	131	139	147	$1.02 * 10^{11}$	$2.26 * 10^8$	$1.96 * 10^8$
2010	78	1369	138	146	160	$1.45 * 10^{12}$	$3.22 * 10^9$	$2.77 * 10^8$
2015	82	1613	145	154	173	$2.07 * 10^{13}$	$4.59 * 10^{10}$	$3.92 * 10^8$
2020	86	1881	151	161	188	$2.94 *$	$6.54 * 10^{11}$	$5.55 * 10^8$

						10^{14}		
2025	89	2174	158	169	202	$4.20 * 10^{15}$	$9.33 * 10^{12}$	$7.84 * 10^{8}$
2030	93	2493	165	176	215	$5.98 * 10^{16}$	$1.33 * 10^{14}$	$1.11 * 10^{9}$
2035	97	2840	172	184	230	$8.53 * 10^{17}$	$1.90 * 10^{15}$	$1.57 * 10^{9}$
2040	101	3214	179	191	244	$1.22 * 10^{19}$	$2.70 * 10^{16}$	$2.22 * 10^{9}$

(všimněme si, že dle Lenstrovy tabulky budou současná doporučení pro symetrickou šifru respektovaná v návrzích pro AES vyhovovat i v roce 2040, resp. vyhovovat bude dokonce i 3-DES se 112 bitovým klíčem).

Po opublikování Lenstrova a Verheulova článku následovala odpověď [5] R. Silvermana z RSA. Pan Silverman se ve svých argumentech opírá především o vývoj existujících faktorizačních technik.

Např. určitě zajímavý je odhad potenciálu Shamirova zařízení TWINKLE.

- jedno takové zařízení by stálo 5000 dolarů
- k faktorizaci 768-bitového čísla by bylo třeba 5000 zařízení TWINKLE, tato zařízení by měla být podporována 80 000 PC
- této technice by trvalo řešení potřebné matice 3 měsíce, přitom by zde muselo fungovat jedno ústřední PC mající alespoň 160 Gbytů paměti.

Silverman uvádí dále následující tabulku (jeho rozbor je prováděn z hlediska finančních nároků na kryptoanalýzu – tabulka se nazývá „**Cost Equivalent Key Sizes**“):

Symmetric Key	EC Key	RSA Key	Time to Break	Machines	Memory
56	112	430	méně než 5 minut	10^{5}	trivial
80	160	760	600 month	4300	4 Gb
96	192	1020	3 miliony let	114	170 Gb
128	256	1620	10^{16} let	.16	120 Tb

Tabulka byla spočtena za předpokladu, že je k dispozici 10 milionů dolarů na nákup potřebného hardware. Celý jeho pohled a argumenty vychází ze současných technologií a cen. Jeho závěrem je, že 1024 bitové RSA bude ještě nejméně 20 let bezpečné.

Mimochodem, při vší úctě k panu Robertu Silvermanovi a jeho argumentům, musí nezaujatý pozorovatel brát do úvahy i fakt, že R. Silverman jako zaměstnanec firmy RSA Security není v zcela nezávislé poloze (a pozor - pan Robert Silverman není totožný se známým odborníkem na teorii čísel a eliptické křivky panem Josephem Silvermanem).

Přístup pánů Lenstry a Silvermana je odlišný především v následujícím. Zatímco, jak je vidět z výše uvedené tabulky, na základě Lenstrova přístupu si lze vytvořit i příslušné „rezervy“, pan Silverman se omezuje na obhajobu dnešní bezpečnosti RSA. Samozřejmě

v tomto zúženém pohledu nelze jinak než s ním souhlasit. Ale pohled Lenstry je širší a poskytuje navíc i možnosti posouzení vhodné délky RSA klíče v různých aplikacích.

Jedním z užitečných materiálů poslední doby, které se nějakým způsobem dotýkají délky klíče kryptografických algoritmů je draft [7] . Materiál sám však doporučení na délky klíčů příliš dopodrobna (z hlediska vhodných argumentů) nerozebírá, je ale užitečný svým rozborem velice široké škály jednotlivých typů klíčů (z pohledu na využití v různých aplikacích). V kapitole 3. tohoto materiálu se objevují určitá dnes již existující či zvažovaná doporučení. Např. pro DSA se hovoří v návaznosti na připravované FIPS 186-3 o velikosti klíče mezi **1024** a **15 360** bitů, samotný podpis bude mít délku mezi **320** a **1024** bity.

Pro RSA z hlediska již existujících doporučení je zde pouze odkaz na ANSI X9.31, kde je doporučeno používat klíče v délce

$$1024 + 256\,i, \quad i = 0, 1, 2, \ldots$$

V kapitole 5.2.2. je pak uvedena tabulka (č.4), která obsahuje doporučení dvojího typu, do roku 2015 a po roce 2015. Jsou zde však uvedeny pouze minimální délky klíčů. Pro DSA je to 1024+160 a po roce 2015 pak 2048+224 bitů. Pro algoritmus RSA to je do roku 2015 minimální délka klíče 1024 bitů a po tomto roce je minimální délka klíče 2048 bitů. Tj., abychom správně chápali i tyto závěry: pokud chráníme nějaká data algoritmem RSA a je naším záměrem, aby tato ochrana byla funkční i po roce 2015, pak tabulka doporučuje použít minimálně 2048 bitové RSA.

V dubnovém číslo Cryptogramu se touto otázkou zabývá i Bruce Schneier [8] a konstatuje, že přestože oproti jeho původním odhadům je vývoj faktorizačních metod pomalejší, přesto setrvává na svých dřívějších odhadech a doporučeních. Jeho tabulka z roku 1995 (!) rozlišuje alespoň jednotlivé typy konkrétních uživatelů:

Recommended Public-Key Key Lengths (in bits)

Year	Ind.	Corp.	Govt.
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

Ve svém článku dále hovoří o tom, že požadavky na asymetrické šifry jsou trochu jiné než na symetrické, vystupují v řade protokolů, mají více účelů atd. To klade i **větší** nároky na jejich vlastnosti. Také různé implementace jsou předmětem velice různorodých útoků.

Logický závěr – pokud s RSA uvažujeme pro seriozní aplikace, je třeba se jím seriozně zabývat a to vyžaduje i seriozní rozbor požadavků na délku klíče (z hlediska vlastních implementací je třeba se samozřejmě zabývat i celou řadou dalších otázek). Můžeme se samozřejmě především pokusit aplikovat na délku klíče RSA výše zmíněnou filosofii rezerv.

Avšak zde již vzniká první kámen úrazu. Jakmile totiž začneme tímto způsobem nad RSA uvažovat (budeme chtít i té nejnižší úrovni bezpečnosti dát dostatečnou rezervu), zjistíme, že příslušné délky klíčů nám poněkud vybočí z řady, téměř přestávají být prakticky použitelné. Zvyšují se nároky na nezbytnou paměť, obtížněji se dosahuje požadovaná rychlost atd.

Druhým kamenem úrazu je právě samotná intenzivní praxe využívání RSA. Pochopitelně jestliže prakticky funguje např. RSA nasazené v čipových kartách (s délkou klíče – buďme optimisty – 1024 bitů), pak samozřejmě pro provozovatele těchto komerčních systémů je důležitou otázkou výše nákladů, které by musely do svých systémů vnést pro využívání RSA s delším klíčem. A samozřejmě zcela oprávněný je požadavek na řádné zdůvodnění takovéto investice. Jakmile někdo vydá normu, kde např. by stanovil minimální délku klíče rovnou 2048 bitů, zcela nepochybně vznikne velká diskuse nad oprávněností takovéhoto požadavku a to právě ze strany zástupců provozovatelů praktických systémů.

A ještě jinak, pokud bych měl zvažovat např. zda sám budu používat 512 bitové RSA či 1024 bitové RSA např. pro ochranu běžných mailů (použité pro přenos klíče pro symetrickou šifru), kde mě jde jen o to, aby do nich nikdo zbytečně nekoukal a nejde mě o ochranu citlivých informací (ať už např. z finančního či jiného důležitého hlediska) a věděl bych, že tato volba význačně ovlivní cenu použité technologie, pak se nesporně spokojím s 512 bity.

Na druhou stranu je třeba vědět, že námi diskutovaná otázka se netýká jen komerčních aplikací, ale její zodpovězení požadují i pracovníci odpovědných vládních institucí. Navíc je právě u asymetrických šifer dneška třeba zvažovat pro celou řadu aplikací i otázky požadavků na dlouhodobou rezistanci délky klíče vůči potenciálním útokům – např. dnes často citovaná otázka archivace digitálních podpisů (požadavky u smluv se objevují např. až na dvacet ale i více roků).

Jak tedy odpovědět na otázku položenou v nadpisu? Pozitivně a pro všechny aplikace? Takto odpovědět, jak soudím, by si už dnes troufl jen málokdo.

Diskuse nad délkou klíče algoritmu RSA není nová. Stačí jen připomenout výše zmíněný článek Lenstry z roku a odpověď pana Silvermana z firmy RSA, nebo situaci na pražském Eurocryptu (1999) po Shamirově vystoupení s TWINKLE (přibližně v téže době bylo také poprvé faktorizováno 512 bitové číslo). Určitě není také jednoduché odpovědět jakýmsi definitivním (alespoň pro nejbližší roky či desetiletí) výrokem. Samotnému RSA by jistě velmi pomohlo, kdyby bylo pro stanovení potřebné délky klíče možné jednoduše využít výše uvedenou „filozofii rezerv“. Z řady důvodů to však není tak průzračná záležitost a tedy odpověď není tak přímočará jako je u jiných kryptosystémů. Jsem však jednoznačně pro kroky obdobné krokům pana Bernsteina. Už jen proto, že umožní zpřesnit náš náhled na bezpečnostní vlastnosti RSA a tím zpřesnit podmínky pro jeho bezpečné využívání.

Určité shrnutí

(vyjadřuje autorův názor na danou problematiku).

A. Téma diskuse – vhodná délka klíče RSA – se v posledních letech objevuje poměrně často. Zcela jistě to souvisí s určitými objektivně existujícími pochybnostmi.
B. Nesporně by přispělo zformulování takových doporučení pro délku klíče RSA, které by respektovalo výše zmíněnou filosofii rezerv. Takováto doporučení by umožnila stanovit i východiska pro různé typy aplikací RSA.
C. Jakýkoliv výzkum, který je prováděn s cílem zpřesnit hodnocení bezpečnosti RSA je vítán - a také „Samozřejmě je nutné vyčkat s objektivním hodnocením až na výsledky příslušných experimentů“.

Poznámka 1.: Kvantové počítače a jejich potenciál nebyly v článku zvažovány, proto jen malé připomenutí. Veškerá kryptologie se dostane do jiné dimenze, pokud by se podařilo implementovat qubitové řetězce dostatečných délek. Toto není strašení, ale pouhé konstatování objektivního faktu. Z týchž důvodů objektivity je ale třeba poukázat na to, že pokud se něco takového někdy podaří, pak to nebude v nejbližších dnech a doufejme ani v letech. Střízlivé odhady hovoří o minimálně dvacetileté perspektivě pro současnou kryptografii bez reálného ohrožení ze strany kvantových počítačů.

Poznámka 2.: Děkuji RNDr. Vlastimilu Klímovi za podněty [2], které mě vedly k napsání výše uvedeného článku.

Poznámka 3. V článku [9] se objevily následující informace. Na konferenci Financial Cryptography (březen 2000) byl Bernsteinův článek jedním z hlavních předmětů diskuse. Experti se zde shodli na tom, že obdobné zařízení by mohla postavit agentura s dostatečným rozpočtem – např. NSA – za cenu menší než jedna miliarda dolarů. Kaliski (ředitel RSA Laboratories) s tímto závěrem nesouhlasil. Říká mj., že 1024 bitové RSA vytváří stále adekvátní ochranu dat pro průměrného uživatele. Na druhou stranu, pokud někdo chce používat delší klíče, dodavatelé kryptografických technik již posouvají své produkty směrem k silnějšímu šifrování.

Poznámka 4. (informace od Mgr.Pavla Vondrušky): Na konferenci Eurocrypt 2002 vystoupil v Rump Session Arjen Lenstra (název příspěvku - Integer factorization circus) a řekl, že Bernsteinův výsledek je vynikající, ale nelze jej "slučovat" s praktickými možnostmi faktorizovat "RSA čísla". Nicméně příspěvek ukazuje, že GNFS ještě není zcela jako metoda vyčerpána a existují cesty, jak ji zlepšovat.

Literatura:

[1] D.J.Bernstein : *Circuits for Integer Factorization: A Proposal*. Manuscript, November 2001. http://cr.yp.to/papers.html#nfscircuit.
[2] Klíma, V.: Kritika článku „Bezpečnost RSA – význačný posun?“, Crypto-World 4/2002
[3] Blaze, M., Diffie, W., Rivest, R.L., Schneier, B., Shimomura, T., Thompson, E., Wiener, M. : Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, January 1996.
[4] Arjen K. Lenstra and Eric R. Verheul : Selecting cryptographic key sizes. *Journal of Cryptology*, to appear
[5] Robert D. Silverman : *A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths*. RSA Laboratories Bulletin #13, April 2000.
[6] Has the RSA algorithm been compromised as a result of Bernstein's Paper?, April 2002, http://www.rsasecurity.com/rsalabs/technotes/bernstein.html
[7] NIST. *Key Management Guideline - Workshop Document*. Draft, October 2001. http://csrc.nist.gov/encryption/kms/key-management-guideline-(workshop).pdf.
[8] Schneier, Bruce: Cryptogram, April 2002
[9] http://www.vnunet.com/News/1131452

E. Studentská bezpečnostní a kryptologická soutěž - SBKS'02

Základní informace

Organizační výbor společně s firmou ecom-monitor.com, časopisem DSM a e-zinem Crypto-World vyhlašují první ročník soutěže o nejlepší studentský příspěvek v oblasti aplikované kryptologie a bezpečnosti.

Studentská kryptologická a bezpečnostní soutěž (SBKS) má dva základní úzce související cíle. Prvním cílem je podpořit studenty vysokých a středních škol v jejich samostatné práci a pomoci jim překonat bariéru mezi školou a odbornou veřejností v České republice. Tím druhým cílem je demonstrovat firmám působícím v oblasti IT České republice možnosti českých škol při řešení konkrétních projektů, které mají kromě teoretické hodnoty i vlastnosti potřebné pro využití v komerčních aplikacích.

Nejlepší příspěvky budou doporučeny k uveřejnění v časopise DSM, nebo e-zinu Crypto-World a vybraní autoři budou moci prezentovat svou práci i na kryptologickém workshopu *Mikulášská kryptobesídka 2002* či *Velikonoční kryptologie 2003*.

Pokyny pro autory

Soutěže se mohou zúčastnit studenti středních škol a bakalářského a magisterského studia všech českých vysokých škol, případně absolventi s datem ukončení studia po 1. lednu 2002. Podmínkou je, aby článek vycházel z práce provedené autorem v době studia. Rozsah příspěvků by měl být přibližně 4 strany (maximální hranicí je 6 stran) v písmu 11pt (jak LaTeX, tak MS Word) s řádkováním 1,2. Samotný text soutěžního příspěvku může být doplněn přílohami, jestliže je to vhodné pro dokumentaci experimentálních či jiných výsledků.

Výzva pro autory

Stručná - jednostránková výzva pro autory je v pdf formátu dostupná v souboru cfp.pdf a je přílohou k tomuto sešitu Crypto-Worldu. Aktuální informace hledejte na stránkách www.ecom-monitor.cz/sbks. Případné dotazy na vše, co vás zajímá ohledně soutěže, je možné směrovat na adresu:

Daniel Cvrček
e-mail: cvrcek@fit.vutbr.cz
tel.: 05 / 411 41238

Zaslání příspěvků	21. červenec 2002
Vyhodnocení příspěvků	22. září 2002
Případná úprava příspěvků	27. říjen 2002

F. Letem šifrovým světem

Přehled vybraných důležitých zahraničních akcí

6th National Conference on Applications of Cryptography ENIGMA 2002
14th - 17th May 2002,
Warsaw, Poland
Conferences site : http://www.enigma.com.pl

Third Conference on Security in Communication Networks
September 12 – 13 2002, Amalfi, Italy
Conferences site : http://www.dia.unisa.it/SCN02/
Important Dates:
Submission: June 15th.
Acceptance: July 5th.

The 6th Workshop on Elliptic Curve Cryptography (ECC 2002)
September 23 – 25 , 2002
University of Essen, Essen, Germany
First Announcement: April 5, 2002
Conferences site : www.cacr.math.uwaterloo.ca
University of Essen site : www.exp-math.uni-essen.de/~weng/ecc2002.html

Information Security Conference 2002
September 30 – October 1 – 2,
University of São Paulo, Brazil
Conferences site : http://www.ime.usp.br/~isc2002

CRYPTOGRAPHY Fundamentals and Applications
(advanced technology seminars)
Lecturer : Ueli Maurer, ETH Zurich
October 14 – 17, 2002 , Engelberg, Switzerland
E-mail: seminars@dplanet.ch
Tel.: + 41 – 71 – 911 99 15 , Fax: + 41 – 71 – 911 99 16

ICISC 2002
The 5th Annual International Conference on Information Security and Cryptology
November 28-29, 2002, Seoul, Korea
Conferences site : http://oberon.postech.ac.kr/icisc02/
Important Dates:
Submission deadline September 2, 2002
Acceptance notification October 28, 2002
Proceedings version due November 11, 2002

ASIACRYPT 2002

December 1-5, 2002, Queenstown, New Zealand
Conferences site : www.sis.uncc.edu/ac02/
Important Dates:
Submission deadline: May 24, 2002
Notification of decision: August 2, 2002
Proceedings version dadline: August 30, 2002
Conference: December 1-5, 2002

INDOCRYPT 2002

3rd International Conference on Cryptology in India
December 16-18, 2002, Hyderabad, India
Conferences site : http://www.isical.ac.in/~indocrypt/
Important Dates:
Submission: August 7, 2002 (Wed.)
Notification: September 27, 2002 (Fri.)
Final version: October 4, 2002 (Fri.)
Conference: December 16-18, 2002 (Mon. – Wed.)
Tutorial: December 14-15, 2002 (Sat. – Sun.)

Financial Cryptography ´03
January 27 – 30 , 2003
La Creole Beach Hotel, Gosier, Guadeloupe
Sponsored by the International Financial Cryptography Association
Conferences site : http://ifca.ai
Important Dates :
Conference January 27 – 30, 2003
Submission deadline September 13, 2002, 23 h.59 EST
Author notification November 11, 2002
Camera-ready papers due December 16, 2002

Konference Security 2002

Ve čtvrtek **6. června** tohoto roku se uskuteční již sedmý ročník konference pořádané společností AEC - **Security 2002**.

Odborný garant - společnost **AEC, spol. s r.o (http://www.aec.cz/)** a mediální partner konference, **Vogel Publishing**, jsou dostatečnou zárukou kvalitních znalostí a seriózních informací.

Konference českých matematiků

pořádá Matematická vědecká sekce JČMF
24. - 26. června, Znojmo
Více podrobností ke konferenci (včetně abstraktů zvaných přednášek)
naleznete na stránkách konference http://kam.mff.cuni.cz/mvs-jcmf/znojmo

SOFSEM 2002 STUDENT RESEARCH FORUM

November 27, 2002
Milovy, Czech Republic

Conferences site :	http://www.sofsem.cz (http://osa.dcs.elf.stuba.sk/sofsem/submit.html http://www.dcs.elf.stuba.sk/~bielik/ e-mail: bielikova@dcs.elf.stuba.sk)
Deadline for paper submission:	July 9, 2002
Notification to authors:	September 6, 2002
Camera ready version:	September 23, 2002
PhD Student Research Forum:	November 27, 2002

Elektronický podpis a aplikace zákona o elektronickém podpisu

MÍSTO	TERMÍN	LEKTOR
Olomouc	18. červen 2002	Mgr. Pavel VONDRUŠKA (Úřad pro ochranu osobních údajů, Praha)

Bližší informace:
http://www.anag.cz/shop/index.php?page=seminar&id=12&name=Elektronick%FD+podpis+a+aplikace+z%E1kona+o+elektronick%E9m+podpisu

O čem jsme psali v květnu roku 2000 a 2001

Crypto-World 5/2000

Crypto-World 5/2001

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

G. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "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

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 k otištění** , informace
pavel.vondruska@uoou.cz (**vondruskap@uoou.cz**)
pavel.vondruska@post.cz
vondruska.p@seznam.cz