Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 4, číslo 4/2002 **18. duben 2002**

4/2002

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adresách
http://www.mujweb.cz/veda/gcucmp/
+ http://cryptoworld.certifikuj.cz
(>360 e-mail výtisků)

Obsah : **Str.**

A. DUBNOVÁ KRYPTO-INSPIRACE

Vítám vás při čtení dubnového čísla. První duben - *apríl* sice již byl, ale přesto jsem se rozhodl do tohoto čísla zařadit alespoň jeden článek trochu lehčího charakteru. Nejprve však jako „rozehřívací kolo“ si zkuste provést následující úkol - spusťte Word, napište do nového dokumentu velkými písmeny Q33NY (příjmový kód letadla, které narazilo 11.9.2001 do WTC) a následně velikost změňte na 72 a písmo nastavte na "Wingdings" (http://www.urbanlegends.com/ulz/wingdings.html) .

Následuje ukázka z knihy VELEDETEKTIV AGATON SAX od spisovatele Olofa Frenzéna. Kniha vyšla v roce 1965 v mé v té době nejoblíbenější edici KOD (Knihy odvahy a dobrodružství). Stala se vůbec první knihou, ze které jsem se dozvěděl něco o krásné vědě – kryptologii. Nedalo mi to, abych se s vámi nepodělil a vyhledal jsem tu část, ve které je popsáno jak Agaton Sax postupuje při analýze šifrového textu. Přeji inspiraci pro vaši práci a příjemný zážitek.

VELEDETEKTIV AGATON SAX
Nils – Olof Franzén

Agaton Sax se posadil k psacímu stolu. Vzal do ruky kresbu, kterou právě dostal, okamžik ji pozoroval a pak ji položil na stolek mikroskopického průzkumu – což byl skvělý vynález, který Agaton Sax sám zkonstruoval, když luštil záhadu létajících talířů, a rozsvítil vysokoreflekční 275wattovou lampu. Intenzívní zář padala téměř strašidelně ostře na kresbu Studa Slogana. Pod mikroskopem zkoumal nyní Agaton Sax na kresbě každý centimetr, ba milimetr čtvereční. Jeho pozornost byla napjata do krajnosti.

Kresba představovala čtyřicet deka bonbónů a šperky ozdobenou ruku, jak se natahuje k misce s bonbóny. Na jednom z bonbónů pozoroval Agaton Sax několik číslic a písmen, která si pozorně zaznamenal. Pod kresbou stál tento text:

„Nezměrně bohatý maharádža Ron-Him-Hok, který žil v letech 1632 – 1710, měl nesmírně rád určitý druh bonbónů. Tyto bylo možno koupit pouze v jistém městě jménem Kr-Djuptgirscha v zemi Hin-Drogdra, 1100 km od maharádžova paláce. Dvě stě ozbrojených jezdců na velbloudech doprovázelo vůz s bonbóny k maharádžovi. Cesta trvala dva měsíce. Následkem toho stály bonbóny dvě stě korun kus. V červenci 1710 velbloudi snědli všechny bonbóny. Zpráva o tom maharádžu tak rozzlobila, že z toho měl smrt.“

Agaton Sax přemýšlel důkladně o tomto vyprávění, napohled tak nevinném. Napřáhl ruku po Velké knize kódů. V tomto tlustém svazku je značný počet číslic, tabulek, výsledků a jiných údajů.Jejich pomocí lze přečíst mnoho tajných šifrovaných sdělení. Agaton Sax je znám jako jeden z nejzdatnějších luštitelů šifer, snad nejlepší vůbec, rozhodně pokud jde o nepříjemně obtížné šifry v řeči grélské nebo brosenské, dále o některé neznámé jazyky a množství jiných.

Položil si před sebe na stůl velký bílý papír, načrtl na něj několik číslic a písmen, přehazoval je, počítal dopředu, pozpátku, nahoru i dolů, srovnával s Velkou knihou kódů, počítal znovu, a po několika hodinách napsal na čtverečkovaný papír tuto řadu písmen:

PNLEKVLEZOÉTJUOSÍBMAOLVERBVOUKLOČLIVDUKO

Během několika minut tato písmena srovnal. Napsal slova, jež vznikla vhodným složením oněch čtyřiceti písmen:

Bramborovou polévku nelze jíst velkou vidličkou.

Agaton Sax upřeně civěl na slova. Pak se rychle zvedl. „Nemožné!“ zvolal.“Velká kniha kódů nestojí za nic !“

Zlobným pohybem hodil knihu na zem.

„Musím vyzkoušet svůj vlastní systém,“ říkal si v duchu a posadil se znovu k psacímu stolu.

„Zkusím systém 627 A-c,“ bručel si. Pak se ponořil opět do pozorování kresby a do svých číslic a písmen.

Hodiny ubíhaly, jedna za druhou. Teta Tilda mluvila ze zdi, ale Agaton Sax nic neslyšel. Na Bykoping se snesla tma. Všude vládlo ticho a klid, ale Agaton Sax seděl trpělivě dál u svého psacího stolu.

Právě když hodiny tloukly dvanáct těžkých úderů označujících půlnoc, Agaton Sax získal tato písmena:

VEJTĚPCYECHVŽABYVÁNIOS

Pro Agatona Saxe bylo dost snadné poznat, že oněch dvaadvacet písmen, která zdánlivě nedávají žádný smysl, ve skutečnosti znamenají zcela prostě:

Sovy v bažinách. Vycpěte je.

Pravým ukazováčkem si hladil svůj elegantní knír. Je to nějaká tajná zpráva ? Pakliže ano, co tedy znamená ?

„Ne,“ vrtěl hlavo Agaton Sax,“ to nemůže být správné. Systémem 627 A-c to nejde. Musím to zkusit systémem B-AC 73 D.“

Vyhledal si tento systém ve své knize šifer, sňal rovněž z přihrádky svou pondělní dýmku – nastávalo už pondělní ráno – a jal se bafat a vyfukoval velké kruhy kouře. Jeden papír po druhém se zaplňoval číslicemi. Hodiny ubíhaly. V jeho kulatém obličeji však nebylo znát únavu. Jeho obdivuhodně zkonstruovaný mozek pracoval pod vysokým tlakem až do dvou hodin čtyřiceti sedmi minut ráno, kdy z papíru před sebou četl tato písmena:

DODINTIGENTEWEMORNIKSNIHOHMADTROPER

V několika okamžicích srovnal písmena do anglické věty:

KOH-MIH-NOR-DIAMOND IN SWEDEN. GET IT. REPORT.

To znamená v překladu: Diamant Koh-Mih-Nor ve Švédsku. Seberte jej. Podejte zprávu.

„Podat zprávu ? Kam? Komu ?“ divil se Agaton Sax.

Aha, už to má. Znovu zkoumal pod mikroskopem malé číslice a písmena, kterých si všiml na jednom z bonbónů na kresbě:

2 ST 7 ENTR 2 ESEALO

Dalo se poměrně snadno zjistit, že číslice a písmena – 2st7entr2esealo – nutno číst:

227 Sloane Street.

„Tak tedy Londýn,“ bručel si Agaton Sax.

Pomalu se zvedl ze židle. V obličeji se mu rozhostil nepopsatelný výraz spokojenosti. Diamant Kon-Mih-Nor ve Švédsku ! Sen všech zlodějů diamantů ! Tomuto neobyčejně jemně broušenému diamantu – který má cenu přibližně 6,8 miliónů švédských korun, byl ukraden před deseti lety v Indii a od té doby se za ním honí policisté a detektivové na celém světě – tedy tomuto diamantu, jejž dosud nedokázal vypátrat pouze pro nedostatek času, je teď na stopě !

KONEC ukázky ☺

B. Kryptografické algoritmy a jejich parametry pro bezpečné vytváření a ověřování zaručeného elektronického podpisu

Mgr. Lada Stachovcová (lada.stachovcova@uoou.cz)

(Výklad k Příloze č. 2 vyhlášky č. 366/2001 Sb. ze dne 3. října 2001 o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu)

Jedním z faktorů významně ovlivňujících bezpečnost elektronického podpisu je použití vhodných kryptografických algoritmů a jejich parametrů. Příloha č. 2 vyhlášky č. 366/2001 Sb. proto upřesňuje požadavky na kryptografické algoritmy a jejich parametry pro bezpečné vytváření a ověřování elektronických podpisů. Tato příloha byla zpracována podle obdobného dokumentu Evropské unie *Algortihms and Parameters for Secure Electronic Signatures* vydaném iniciativou EESSI (The European Electronic Signature Standardization Initiative).

Seznam zde uvedených algoritmů je potřeba pojímat jako otevřený a dočasný. Bude aktualizován a případně pozměněn v závislosti na dosaženém vývoji v oblasti kryptologie a podle zkušeností s praktickým využitím aplikací digitálního podpisu.

1. Kryptografické požadavky

Kryptografické algoritmy a parametry smějí být s ohledem na bezpečnost vytváření a ověřování elektronických podpisů používány pouze v předem definovaných kombinacích, tzv. **podpisových schématech**.
Každé podpisové schéma se skládá z následujících položek:

- Asymetrický podpisový algoritmus a jeho parametry
- Algoritmus pro generování klíčů
- Metoda určená pro padding
- Kryptografická hašovací funkce

Podpisová schémata

Podpisové schéma	Asymetrický algoritmus	Parametry asymetrického algoritmu	Algoritmus na generování klíčů	Metoda určená pro padding	Hašovací funkce
001	RSA	MinModLen=1020	rsagen1	emsa-pkcs #1-v1.5	SHA1
002	RSA	MinModLen=1020	rsagen1	emsa-pss	SHA1
003	RSA	MinModLen=1020	rsagen1	emsa-pkcs #1-v1.5	RIPEMD160
004	RSA	MinModLen=1020	rsagen1	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	dsagen1	-	SHA1
006	ECDSA-F_p	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	-	SHA1
007	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4 MinClass=200	ecgen1	-	SHA1

Každému podpisovému schématu je jednoznačně přiřazen trojciferný záznamový index (001-007). V dokumentu [20] je u podpisového schématu uvedeno rovněž datum, které představuje poslední den, kdy může být příslušné podpisové schéma používáno. Bezpečnost používání těchto schémat je zde stanovena na dobu 5 let (do 31.12. 2005), zdůrazněna je však nutnost pravidelného revidování tohoto data s ohledem na dosažený vývoj v oblasti kryptologie a informačních technologií, a v případě aktualizace, resp. vyřazení jakékoli položky podpisového schématu musí být aktualizováno, resp. vyřazeno celé podpisové schéma.

V případě vyhlášky č. 366/2001 Sb. bude aktualizace, resp. vyřazení podpisového schématu provedena příslušnou novelou.

Jednotlivé položky podpisových schémat jsou popsány v následujících odstavcích. Poznamenejme ještě, že pod pojmem *délka* čísla p v bitech rozumíme číslo r takové, že $2^{r-1} \leq p < 2^r$.

2. Asymetrické podpisové algoritmy

Asymetrický algoritmus pro podpis je společně s daty pro vytváření elektronického podpisu (soukromý klíč) aplikován na otisk dokumentu (viz. hašovací funkce, odst. 4), který má být podepsán, čímž se vytvoří podpis dokumentu. Společně s daty pro ověřování elektronického podpisu (veřejný klíč) je pak algoritmus použit pro ověření podpisu.

Vyhláška č. 366/2001 Sb. schvaluje použití následujících asymetrických algoritmů:

- RSA [6] [7]
- DSA [7] [9]
  - ECDSA-F_p [9] [11] [10] [7] [13]
  - ECDSA-$F2^m$ [9] [11] [10] [7] [13]

Dokument [20] schvaluje navíc použití algoritmů EGDSA-F_p, resp. EGDSA-$F2^m$, které jsou v podstatě variantou algoritmů ECDSA-F_p , resp. ECDSA-$F2^m$ s pozměněnou vytvořující rovnicí podpisu a metodou ověřování. Požadavky na ně kladené jsou stejné jako v případě algoritmů ECDSA-F_p, resp. ECDSA-$F2^m$ (bližší informace viz. [13]).

Při výběru jednotlivých algoritmů a velikosti jejich parametrů je potřeba vzít v úvahu možnosti současných známých algoritmů na faktorizaci celých čísel, resp. metod na odhad diskrétních logaritmů. Dlouhodobější analýza týkající se tohoto tématu je předmětem např. [21].

2.1 RSA

Jedná se o všeobecně známý algoritmus Rivest-Shamir-Adleman. popsaný v dokumentu RSA Laboratories: PKCS #1 RSA Cryptography Standard [6]. Bezpečnost algoritmu RSA je založena na složitosti faktorizace velkých celých čísel.

2.1.1 Parametry

K vytvoření dat pro vytváření elektronického podpisu a dat pro ověřování elektronického podpisu je potřeba náhodně a na sobě nezávisle vygenerovat dvě prvočísla p a q, která splňují následující podmínky:

- délka modulu $n = pq$ musí být alespoň 1020 bitů (MinModLen); tato délka je rovněž označována jako ModLen,
- prvočísla p a q musí mít zhruba stejnou velikost, tj. být v takovém rozmezí, aby platilo $0.5 < |\log_2 p - \log_2 q| < 30$,
- na výběr musí být dostatečně mnoho prvočísel a jejich rozložení musí odpovídat rovnoměrnému rozložení.

Minimální délka číselného modulu pro RSA je stanovena jako 1020 bitů (na rozdíl od „přirozenější“ délky 1024 bitů). Tak lze použít i aplikace, které nepočítají s nejvyššími bity.

Data pro vytváření podpisu sestávají ze soukromého exponentu d a modulu n.

Data pro ověřování podpisu sestávají z veřejného exponentu e a modulu n.

Veřejný exponent e se vybere tak, aby $3 \le e < n-1$ a nsd(e,nsn(p-1,q-1))=1. Ze vztahu $ed \equiv 1 \pmod{\text{nsn}(p-1)(q-1)}$ se vypočítá soukromý exponent d.

2.1.2 Algoritmus pro generování klíčů a parametrů rsagen1

Pomocí tohoto algoritmu se generují čísla p a q. Vyhláška č. 366/2001 Sb. požaduje splnění podmínek pro generátor trueran (viz. 3.1) s hodnotou EntropyBits>=128 bitů, v současné době [20] je tendence tento požadavek zmírnit a povolit rovněž použití generátoru splňujícího podmínky pseuran (viz. 3.2) s odpovídající délkou inicializačních dat SeedLen>=128 bitů. Hodnota EntropyBits, resp. délka seedu SeedLen musí být efektivně využity při generování každého prvočísla. Vygenerovaná náhodná čísla musí být testována na prvočíselnost a vybráno je takové, u něhož je pravděpodobnost chyby (tzn. toho, že je složené) nejvýše 2^{-60}.

2.1.3 Metoda určená pro padding

Algoritmus RSA vyžaduje, aby byl k původní zprávě připojen řetězec náhodných bitů pevné délky (padding), a to způsobem odpovídajícím specifickým požadavkům pro příslušný algoritmus. Podrobněji jsou tyto metody popsány v uvedených normativních odkazech. Schválenými postupy jsou:

- EMSA-PKCS #1-v1.5 [6, kap. 9.2.1]
- EMSA-PSS [17, kap. 9.2.2]

Metoda EMSA-PSS zatím není plně standardizována, je však dlouhodobě stabilní a představuje zdokonalení schématu EMSA-PKCS#1-v.1.5. Očekává se přijetí dalších paddingových metod založených na ISO/IEC 9796-2, které v současné době procházejí procesem schvalování.

2.2 DSA

Digital Signature Algorithm (DSA) je specifikován ve standardu FIPS 186-2: Digital Signature Standard (DSS) [9], který byl vydán National Institute of Standards and Technology (NIST). Bezpečnost algoritmu DSA spočívá v obtížnosti výpočtu diskrétního logaritmu v multiplikativní grupě prvočíselného tělesa F_p.

2.2.1 Parametry

Veřejnými parametry tohoto algoritmu jsou:
- prvočíslo p délky alespoň 1024 bitů (pMinLen),
- prvočíslo q, které dělí p-1 a má minimální délku 160 bitů (qMinLen),
- číslo g, které se vypočítá podle [9].

Data pro vytváření podpisu se skládají z:
- veřejných parametrů p, q, a g,
- náhodně nebo pseudonáhodně generovaného čísla x, $0 < x < q$, které je specifické pro podepisující osobu,
- náhodně nebo pseudonáhodně generovaného čísla k, $0 < k < q$; toto číslo musí být znovu generováno pro každý podpis.

Data pro ověřování podpisu sestávají z čísel p, q, g a čísla y, které se vypočítá jako $y = g^x \bmod p$.

Při vytváření digitálního podpisu zprávy není potřeba na otisk zprávy použít metodu paddingu. Otisk ovšem musí být metodou popsanou v [9, App. 2.2] převeden na celé číslo.

2.2.2 Algoritmus pro generování klíčů a parametrů dsagen1

Čísla p a q jsou generována metodou popsanou v [9, App. 2.2]. Číslo x se generuje použitím metody splňující požadavky trueran (EntropyBits>=128 bitů) nebo pomocí metody splňující pseuran s velikostí inicializačních dat SeedLen>=128 bitů. Číslo k se generuje některou z výše uvedených metod, která nemusí být stejná jako v případě generování čísla x. Pro pseuran se již dále nedoporučuje používat metody uvedené ve FIPS 186-2 [9] (vzhledem k útoku D. Bleichenbachera[1]). V současnosti NIST pracuje na revizi FIPS 186-2 a na odstranění tohoto nedostatku; na místo uvedeného postupu se zatím doporučuje použít generátory popsané v [18].

2.3 ECDSA-F_p

Jedná se o analogii algoritmu DSA v grupě eliptické křivky E nad prvočíselným tělesem F_p, kde p je velké prvočíslo. Bezpečnost algoritmu spočívá v obtížnosti výpočtu diskrétního logaritmu v eliptických křivkách.

2.3.1 Parametry

Veřejnými parametry jsou:
- velké prvočíslo p,
- velké prvočíslo q ($p \neq q$) délky alespoň 160 bitů (qMinLen),
- eliptická křivka E nad konečným tělesem F_p, jejíž řád je dělitelný q,
- pevný bod P řádu q na eliptické křivce E .

[1] Dosud nepublikováno, viz. např. http://www.lucent.com/press/0201/010205.bla.html

Tyto parametry musí splňovat následující podmínky:

- počet tříd maximálního řádu okruhu endomorfismů křivky E musí být alespoň 200 (MinClass),
- hodnota r_0=min(r; q dělí p^r-1) by měla být větší než 10^4 (r0Min).

V publikaci FIPS 186-2 [9] je definováno pět eliptických křivek nad prvočíselnými tělesy. Všechny tyto křivky výše popsané požadavky splňují.

Data pro vytváření podpisu sestávají z:

- veřejných parametrů E, q, a P,
- statisticky jednoznačného a nepředvídatelného čísla x, $0 < x < q$, které je specifické podepisující osobě,
- statisticky jednoznačného a nepředvídatelného čísla k, $0 < k < q$; toto číslo musí být znovu generováno pro každý podpis.

Data pro ověřování podpisu sestávají z E, q, P a bodu Q křivky E, který se vypočítá jako $Q=xP$.

2.3.1.1 Algoritmus pro generování klíčů a parametrů ecgen1 pro ecdsa-Fp

Prvočíslo p, které určuje počet prvků tělesa F_p, se doporučuje generovat podle [11]. Druhou možností je použít některé z pěti zobecněných Mersennových prvočísel uvedených v [9]. Eliptickou křivku nad F_p je třeba zvolit tak, aby byl její řád dělitelný prvočíslem q délky alespoň qMinLen>=160 bitů (viz. [11]). Číslo x se generuje použitím metody splňující požadavky trueran (EntropyBits>=128 bitů) nebo pomocí metody splňující pseuran s odpovídající velikostí inicializačních dat SeedLen>=128 bitů. Hodnota EntropyBits, resp. délka seedu SeedLen musí být efektivně využity při generování každého parametru x. Číslo k se generuje některou z výše uvedených metod, která nemusí být stejná jako v případě generování čísla x.

2.4 ECDSA-F2^m

Jedná se opět o analogii algoritmu DSA v grupě eliptické křivky E, a to nad číselným tělesem $F_2{}^m$, kde m je prvočíslo. Bezpečnost algoritmu spočívá v obtížnosti výpočtu diskrétního logaritmu v eliptických křivkách.

2.4.1 Parametry

Veřejnými parametry jsou:

- prvočíslo m,
- velké prvočíslo q délky alespoň 160 bitů (qMinLen),
- eliptická křivka E nad konečným tělesem $F_2{}^m$, jejíž řád je dělitelný q,
- pevný bod P řádu q na eliptické křivce E.

Tyto parametry musí splňovat následující podmínky:

- E není možné definovat nad F_2,
- počet tříd maximálního řádu okruhu endomorfismů křivky E musí být alespoň 200 (MinClass),

- hodnota r_0=min(r; q dělí 2^{mr}-1) by měla být větší než 10^4 (r0Min).

V publikaci FIPS 186-2 [9] je definováno pět pseudonáhodně generovaných eliptických křivek nad tělesem F_2^m. Všechny tyto křivky výše popsané požadavky splňují. Poznamenejme ještě, že Koblitzovy křivky uvedené v [9] jsou definovány nad F_2 a nesplňují tedy první požadavek.

Data pro vytváření podpisu sestávají z:
- veřejných parametrů E, q a m,
- statisticky jednoznačného a nepředvídatelného čísla x, $0 < x < q$, které je specifické podepisující osobě,
- statisticky jednoznačného a nepředvídatelného čísla k, $0 < k < q$; toto číslo musí být znovu generováno pro každý podpis.

Data pro ověřování podpisu sestávají z E, q, m a bodu Q křivky E, který je vypočítán jako $Q=xP$.

2.4.2 Algoritmus pro generování klíčů a parametrů ecgen1 pro ecdsa-F2^m

Prvočíslo m, které určuje těleso F_2^m, je třeba volit pevně podle [11]. Eliptickou křivku nad F_2^m je třeba zvolit tak, aby byl její řád dělitelný prvočíslem q délky alespoň qMinLen >= 160 (viz. [11]).
Požadavky na generování parametrů x a k jsou stejné jako v případě algoritmu ecdsa-Fp .

Algoritmy pro generování klíčů

Označení generátoru klíčů	Používané označení	Asymetrický algoritmus	Metoda generování náhodných čísel	Parametry náhodného generátoru
4.01	rsagen1	Rsa	trueran	EntropyBits≥128
4.02	dsagen1	Dsa	trueran nebo pseuran	EntropyBits≥128 nebo SeedLen≥128
4.03	ecgen1	ecdsa-F_p	trueran nebo pseuran	EntropyBits≥128 nebo SeedLen≥128

3. Generování náhodných čísel

Generování náhodných čísel je důležité při vytváření dat pro vytváření elektronického podpisu a při generování náhodných parametrů pro některé z kryptografických algoritmů (např. DSA). V některých případech může být zásadní i pro padding otisku. Proto jsou společně s metodou pro padding a s algoritmem pro generování parametrů uváděny rovněž požadavky na generátory náhodných čísel.

3.1 Požadavky na generátor trueran

Fyzikální generátor náhodných čísel se skládá ze zdroje fyzikálního šumu (primárního šumu) a kryptografického nebo matematického mechanismu, který primární šum následně

zpracovává. Primární šum musí projít příslušnými statistickými testy na odpovídající úrovni (viz. např. [8], část 4.11.1. Statistical random number generator tests). Složitost odhadu kryptografického klíče by mělo být přinejmenším ekvivalentní složitosti výběru náhodné hodnoty o délce EntropyBits bitů.

3.2 Požadavky na generátor pseuran

Jedná se o generátor pseudonáhodných čísel, který musí být inicializován pomocí skutečného náhodného čísla. Tato inicializační data se nazývají *seed*, jejich délku v bitech udává SeedLen. Výstup generátoru musí splňovat následující podmínky:

- předem není možno zjistit žádnou informaci o výstupních bitech,
- částečná znalost výstupní posloupnosti neumožňuje vyvodit cokoli o zbývajících bitech,
- neexistuje metoda, pomocí níž by bylo možné na základě částečné znalosti výstupních dat určit některé z předchozích nebo následujících výstupů, některý z vnitřních stavů či inicializační data.

Generátory pseudonáhodných čísel odpovídající těmto požadavkům jsou popsány např. v [22]. Složitost získání informace o vnitřním stavu generátoru by mělo být minimálně ekvivalentní složitosti výběru náhodné hodnoty o délce SeedLen.

3.3 Generátor FIPS 186 [9]

Standard [9] (Digital Signature Standard) navrhuje dva druhy generování pseudonáhodných čísel pro získání veřejných parametrů, tajného a dočasného tajného klíče pro použití algoritmu DSA. První z nich, FIPS 186-2-31, je založen na hašovací funkci (SHA-1), druhý, FIPS 186-2-32, používá blokovou šifru (DES). Dokument [20] však vzhledem k útoku D. Bleichenbachera již nedoporučuje jejich použití pro generování tajného klíče a místo toho jsou doporučeny generátory cr_to_X9.30_x, resp. cr_to_X9.30_k, které jsou podrobněji popsané v [18, B.2.1, resp. B.2.2].

Metody generování náhodných čísel

Označení náhodného generátoru	Používané označení	Parametry náhodného generátoru
5.01	trueran	EntropyBits
5.02	pseuran	SeedLen
5.03	FIPS 186-2-31	SeedLen
5.04	FIPS 186-2-32	SeedLen

4. Hašovací funkce

Hašovací funkce se při elektronickém podepisování využívá k vytvoření tzv. otisku podepisovaného dokumentu. K zaručení bezpečnosti elektronického podpisu musí být použita **bezkolizní** hašovací funkce, tzn. musí být prakticky nemožné najít dva různé dokumenty se stejným otiskem. Vyhláška č. 366/2001 Sb. v současní době schvaluje použití dvou hašovacích funkcí:

- SHA-1 (viz.[4],[5])
- RIPEMD-160 (viz.[4])

5. Literatura

[1] "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures," December 1999.
[2] International Organization for Standardization, "ISO/IEC 9979: Information technology - Security techniques - Procedures for the registration of cryptographic algorithms," 1999.
[3] Housley,R., et al., "Internet X.509 Public Key Infrastructure. Certificate and CRL Profile," Internet Request for Comment (RFC) 2459, January 1999.
[4] International Organization for Standardization, , "ISO/IEC 10118-3: Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions," 1998.
[5] National Institute of Standards and Technology, "NIST: FIPS Publication 180-1: Secure Hash Standard (SHS-1)," May 1995.
[6] RSA Laboratories, "PKCS #1 v2.0: RSA Cryptography Standard," October 1998.
[7] International Organization for Standardization, "ISO/IEC 14888-3: Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms," 1999.
[8] National Institute of Standards and Technology, "NIST: FIPS Publication 140-1: Security requirements for cryptographic modules," January 1994.
[9] National Institute of Standards and Technology, "NIST: FIPS Publication 186-2: Digital Signature Standard (DSS)," January 2000.
[10] The Institute of Electrical and Electronics Engineers, Inc, "Standard Specifications for Public-Key Cryptography," IEEE P1363, 2000.
[11] American National Standards Institute, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)," ANSI X9.62-1998, 1998.
[12] International Organization for Standardization, "ISO/IEC 9796-3: Information technology - Security techniques - Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms, " 2000.
[13] International Organization for Standardization, "ISO/IEC FCD 15946-2: Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures," Final Committee Draft, 1999.
[14] International Organization for Standardization, "ISO/IEC CD 15946-4: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery," Committee Draft 2001-03-08.
[15] Eastlake, D., et al., "Randomness Recommendations for Security," Internet Request for Comment (RFC) 1750, December 1994.
[16] American National Standards Institute, "Financial Institution Key Management (wholesale)," ANSIX9.17-1985, 1985.
[17] RSA Laboratories, "PKCS #1 v2.1 draft 2: RSA Cryptography Standard," January 2001.
[18] Change Recommendation for ANSI X9.30-1995, (Part 1), Draft, April 2001.
[19] Adams, C., et al., "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)," Internet Request for Comment (RFC) 3161, August 2001.
[20] European Electronic Signature Standardization Initiative, "Algorithms and Parameters for Secure Electronic Signatures," V.2.1 Oct 19th 2001
[21] A.K. Lenstra, E.R. Verheul: *Selecting Cryptographic Key Sizes*, www.cryptosavvy.com
[22] Blum, M. a Micali, S.,"*How to generate cryptographically strong sequences of pseudo-random bits*,"SIAM Jourmal on Computing, Vol. 4, No. 13, pp. 850-863, 1984

C. Kryptografie a normy
Digitální certifikáty. IETF-PKIX část 2.
Jaroslav Pinkava, AEC spol. s r.o.

1.Úvod

V minulém díle byl čtenář seznámen s celkovým pohledem na materiály pracovní skupiny IETF-PKIX. Práce skupiny je orientována na (digitální) certifikáty veřejných klíčů dle normy X.509. Historicky jedním z prvních dokumentů vzniklých v této skupině byly drafty (a následně rfc), které se zabývali (logicky) nejprve profilem samotných certifikátů veřejných klíčů a profilem CRL (Certificate Revocation List) – profilem seznamu odvolaných certifikátů. Jen malá poznámka - autor se ve výkladu bude přidržovat terminologie používané v pracovní skupině, viz předešlý díl seriálu.

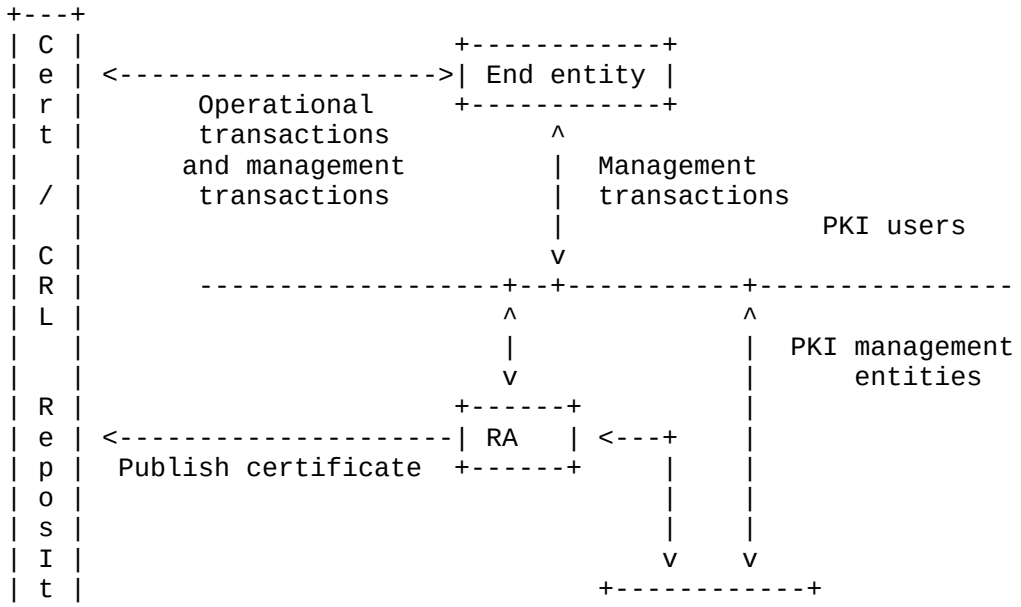
Obsahem dnešního výkladu bude tedy především rfc.2459 (Certificate and CRL Profile) resp. budou zmíněny vznikající odlišnosti v draftu nové verze – dokumentu <draft-ietf-pkix-new-part1-12.txt>.

2.Certifikáty veřejných klíčů

Dokument rfc.2459 definuje formáty a sémantickou strukturu certifikátů a CRL pro použití v rámci internetového PKI a jsou zde popsány postupy pro vyhodnocování příslušných certifikačních cest. Popsané postupy lze aplikovat např. pro přístupy na webovské stránky, elektronickou poštu, autentizaci uživatelů a IPSEC.

Zde popsané profily slouží pak dále pro vývoj systému řízení práce s certifikáty, vývoj různých aplikací a příslušných nástrojů, v závislosti na použité politice mohou sloužit i k interoperabilitě různých systémů. Profil samotný nepředpokládá ani nevynucuje použití adresářů dle normy X.500 – pro distribuci certifikátů a CRL mohou být použity i jiné prostředky.

Následující obrázek z dokumentu [2] dává pohled (zjednodušený) na použitou architekturu:



Komponentami modelu jsou tedy: koncová entita (uživatel certifikátu, resp. systém uživatele, který je předmětem certifikátu), certifikační a registrační autority a dále sklad (certifikátů a CRL).

Uživatelé systémů s veřejným klíčem musí být ubezpečení, že soukromý klíč asociovaný s daným veřejným klíčem vlastní příslušný subjekt (osoba či systém) vztažený k použitému šifrování či digitálnímu podpisu. Toto ubezpečení probíhá prostřednictvím certifikátů veřejných klíčů, a to jsou datové struktury, které propojují hodnotu veřejného klíče a příslušný subjekt. Propojení vzniká na základě podpisu certifikátu důvěryhodnou certifikační autoritou. Příslušné „prohlášení“ CA je přitom založeno na použití určitých technických prostředků, které umožňují ověřit, že příslušná osoba (subjekt) je vlastníkem daného soukromého klíče. Certifikát má omezenou dobu platnosti vyznačenou v podepsaném obsahu certifikátu. Takto vytvořený certifikát může cestovat i prostřednictvím nezabezpečených komunikací a serverů.

Norma X.509 poprvé publikovaná v roce 1988 definuje standardní formát certifikátu (rok 1988 – verze 1, rok 1993 – verze 2).

Spoléhající se strana (ověřující uživatel) potřebuje k ověření daného veřejného klíče získat příslušný certifikát a mít možnost tento certifikát ověřit. Nemusí mít také přitom k dispozici spolehlivou cestou získanou kopii veřejného klíče dané CA, která certifikát podepsala. K tomuto může být zapotřebí i nějaká řada dalších certifikátů podepsaných jinými CA. Vzniká tak určitý řetězec certifikátů, který je v materiálech PKIX nazýván certifikační cestou. Existuje dnes několik architektur pro vytváření takovýchto certifikačních cest. Dané rfc jednu takovou popisuje, přitom je volená architektura, která má poměrně flexibilní charakter.

Když je certifikát vydán, předpokládá se, že bude používán po celou dobu jeho platnosti (vyznačenou v certifikátu). Mohou však vzniknout některé okolnosti, které mohou způsobit, že daný certifikát přestane být platný. Např. – změna jména, změna nějaké podstatné skutečnosti uvedené v certifikátu (zaměstnání, funkce atd.) resp. to může být i kompromitace (skutečná či podezřívaná) příslušného soukromého klíče. Při vzniku takovýchto okolností je třeba, aby CA daný certifikát odvolala.

Norma X.509 jednu takovou metodu odvolání certifikátu definuje. Tato metoda předpokládá, že CA vydává periodicky určitou jí podepsanou datovou strukturu – seznam odvolaných certifikátů (CRL). CRL obsahuje seznam (s časovým údajem) definující odvolané certifikáty, tento seznam je volně dostupný ve veřejném skladu. Každý odvolaný certifikát je v CRL identifikován pořadovým číslem certifikátu. Systém, který ověřuje platnost daného certifikátu, pak nejen ověřuje podpis certifikátu a jeho dobu platnosti, ale vyžádá si rovněž tak i příslušné CRL a ověří zda toto CRL neobsahuje sériové číslo ověřovaného certifikátu. Které je „příslušné“ CRL závisí na místní politice, obvykle se jí rozumí poslední aktuální CRL.

Pro práci s certifikáty a CRL jsou definovány protokoly různých typů . Tzv. *operační protokoly* slouží k distribuci certifikátů (CRL) do systémů, které tyto certifikáty používají. Využívají přitom různé prostředky (LDAP, HTTP, FTP a X.500). Jejich popis je obsahem jiných PKIX dokumentů. Tzv. *řídící protokoly* (management protocols) slouží k vytváření on-line interaktivního spojení mezi uživatelem PKI a řídící entitou. Takto mohou být

zabezpečovány např. následující funkce: registrace uživatelů, inicializace (dvojice klíčů), certifikace (proces během kterého CA vydá a zveřejní certifikát veřejného klíče uživatele),. Může se také jednat o obnovu dvojice klíčů (vydání jiné dvojice s novým certifikátem témuž uživateli), žádost o odvolání certifikátu, křížovou certifikaci atd.

Samotným profilem certifikátu (a rozšíření certifikátu) se zabývá kapitola. 4. ([2]). Definice ASN certifikátu (kódování DER, [X.208]) je následující:

```
Certificate  ::=  SEQUENCE  {
        tbsCertificate       TBSCertificate,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }
   TBSCertificate  ::=  SEQUENCE  {
        version         [0]  EXPLICIT Version DEFAULT v1,
        serialNumber         CertificateSerialNumber,
        signature            AlgorithmIdentifier,
        issuer               Name,
        validity             Validity,
        subject              Name,
        subjectPublicKeyInfo SubjectPublicKeyInfo,
        issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version shall be v2 or v3
        subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version shall be v2 or v3
        extensions      [3]  EXPLICIT Extensions OPTIONAL
                             -- If present, version shall be v3
        }
```

Certificate je tedy posloupnost tří vyžadovaných polí

- tbsCertificate (obsahuje jméno subjektu a vydavatele certifikátu, veřejný klíč propojený se subjektem, dobu platnosti certifikátu popř. další informace)
- signatureAlgorithm (obsahuje identifikátor kryptografického algoritmu, který CA použila k podepsaní certifikátu)
- signature Value (obsahuje digitální podpis pole tbsCertificate - zakódovaného dle ASN.1 DER)

Rozšíření (extensions) certifikátů poskytují cesty, jak spojit s daným certifikátem nějaké další přídavné atributy. Důsledněji tyto otázky řeší tzv. atributové certifikáty.

3.Profily CRL

Definice ASN.1 DER seznamu odvolaných certifikátů je následující:

```
CertificateList  ::=  SEQUENCE  {
        tbsCertList          TBSCertList,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }
   TBSCertList  ::=  SEQUENCE  {
        version                 Version OPTIONAL,
                                     -- if present, shall be v2
        signature               AlgorithmIdentifier,
        issuer                  Name,
        thisUpdate              Time,
        nextUpdate              Time OPTIONAL,
        revokedCertificates     SEQUENCE OF SEQUENCE  {
             userCertificate         CertificateSerialNumber,
             revocationDate          Time,
             crlEntryExtensions      Extensions OPTIONAL
                                           -- if present, shall be v2
                                   }  OPTIONAL,
```

```
    crlExtensions           [0]  EXPLICIT Extensions OPTIONAL
                                        -- if present, shall be v2
                              }
```

Smysl jednotlivých tří požadovaných polí je tedy obdobný jako v definici Certificate. Pole tbsCertList obsahuje jméno vydávající strany, datum vydání, datum vydání následujícího seznamu, seznam odvolaných certifikátů a možná další rozšíření. Každý prvek seznamu odvolaných certifikátů je popsán následujícími údaji: sériové číslo certifikátu, datum odvolání certifikátu a opět mohou být připojena další rozšíření.

Ověření certifikační cesty vychází z popisu v normě X.509. Kapitola 6. ([2]) popisuje jeden z možných algoritmů pro takovéto ověření. Na implementacích kompatibilních s daným rfc je vyžadováno obdobné funkční chování, nikoliv však nutně použití popsaného algoritmu.

Podporovány jsou následující kryptografické algoritmy:

- hashovací funkce: preferována je SHA-1, ale mohou být použity také MD5 resp. dokonce MD2 (popsáno pro PEM v rfc.1422);
- podpisové algoritmy: RSA (zde dle PKCS 1, rfc.2313), DSA

Certifikáty nemusí být samozřejmě pouze certifikáty veřejných klíčů určených k digitálnímu podpisu, ale mohou podporovat i jiná použití veřejných klíčů. V dokumentu jsou popsána dvě takováto použití: RSA šifrování a Diffie-Hellmanova výměna klíčů.

4.Další poznámky

Dokument [3] má za svůj cíl nahradit rfc.2459. Liší se od něho především v následujících oblastech:

- pro usnadnění interoperability vznikajících implementací je popsán detailní algoritmus k ověření certifikační cesty;
- je doplněn algoritmus pro určení statutu certifikátu na základě použití CRL;
- je zde obsažena detailní informace týkající se popisu delta CRL (smyslem delta CRL je distribuce pouze změn oproti minulému CRL, to snižuje nároky na objem přenášených dat);
- identifikace a kódování samotného veřejného klíče byly přeneseny do jiného dokumentu [4] ;
- jsou zde specifikována čtyři nová rozšíření, tři certifikátová (subject info access, inhibit any policy, and freshest CRL) a jedno rozšíření CRL (je to rovněž freshest CRL);
- v dokumentu byla přidána rovněž celá řada vysvětlivek. Jejich cílem je usnadnit slučitelnost s požadavky normy X.509 a tím zlepšit interoperabilitu řešení na bázi daného dokumentu s řešeními na bázi ryze normy X.509.

5.Literatura

[1] PKIX Working Group: http://www.ietf.cnri.reston.va.us/html.charters/pkix-charter.html
[2] RFC 2459: http://www.ietf.cnri.reston.va.us/rfc/rfc2459.txt
[3] http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-pkix-new-part1-12.txt
[4] Representation of Public Keys and Digital Signatures, http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-pkix-ipki-pkalgs-05.txt

D. Kritika článku "Bezpečnost RSA - význačný posun?"

RNDr. Vlastimil Klíma, kryptolog, ICZ a.s., vlastimil.klima@i.cz

Tento článek by měl uklidnit všechny uživatele RSA, kteří mohli znejistět po přečtení článku Ing. Jaroslava Pinkavy, CSc. "Bezpečnost RSA - význačný posun?" v minulém čísle Crypto -Worldu. Pokud neznejistěli, je to v pořádku, pokud ano, v tomto příspěvku bych jim chtěl poskytnout jiné názory na význam Bernsteinovy práce pro současnost.

Úvodem připomeňme, že NFS (respektive její zobecnění GNFS) je v současnosti nejvýkonnější metoda pro faktorizaci velkých čísel. Bernstein [4] přinesl náměty na některá její zlepšení. V kritizovaném článku (dále stručně jen "JP") se uvádí, že tento výsledek může mít dopad na obrovskou řadu praktických aplikací. Pro nezasvěcené také uvádí příklad složitosti faktorizace (tj. de facto rozbití) 1024bitového modulu RSA. Protože uvedená čísla (čas řádu 2^53, paměť 2^36) jsou směšně nízká, jenom hlupák by po takovém vysvětlení neudělal závěr, že algoritmus RSA padl. V JP se to také nepřímo potvrzuje - "už se spekuluje o tom, co s RSA a asymetrickou kryptografií", a když by ještě někdo pochyboval, připojuje se poznámka, že i "NSA převádí citlivá data na ECC". Co k tomu dodat? Snad jen tolik: Je to jinak.

Článek JP (doporučuji ho mít před sebou) by si zasloužil více analýzy, ale mým cílem je pouze vysvětlit dvě jeho klíčové chyby. První chybou je uváděný příklad pro modul RSA 1024 bitů, kdy srovnává klasickou metodu NFS a "Bernsteinovu NFS". Je to velice zavádějící, protože **Bernsteinovy vzorce pro výpočet složitosti nelze na modul 1024 takto aplikovat. Tyto vzorce jsou limitní povahy a týkají se čísel, blížících se nekonečnu.** Navíc je jejich cílem popsat asymptotické chování dané funkce, nikoliv konkrétní funkční hodnoty. Vidíme z nich, *jakého druhu* je závislost času (resp. času krát paměti, což je tzv. "cena" za faktorizaci) na délce modulu, *nikoliv konkrétní počet* vteřin, megabajtů paměti nebo dolarů, nutných pro faktorizaci modulu dané délky. Bernsteinovy vzorce nelze tedy mechanicky použít ani na modul o délce 1024 bitů, ani na modul 512 bitů nebo 8192 bitů, protože tyto vzorce se prostě těchto čísel netýkají. V článku JP jsou ale uvedeny právě výpočty pro modul 1024 "pro přiblížení", aby čtenář pochopil. Ve skutečnosti je ale takové "objasnění" právě tím nejhorším, co článek JP mohl udělat pro čtenáře, který nechtějí číst originální práci. Protože uváděná výpočetní a paměťová náročnost na faktorizaci 1024bitového RSA je v tomto příkladu velmi nízká, vzniká silný dojem, že už stačí jen nakoupit příslušný HW. Abychom nebyli v pokušení, že se jedná jen o fiktivní příklad, který nemá se skutečností nic společného, v JP se dodává, že Bernstein shání peníze na své experimenty a že "*Podle předběžných odhadů se takto posun bezpečné délky parametrů RSA dostává nad hranici 2000*.". Tato věta je druhou klíčovou chybou, neboť pohřbívá zbylé čtenářovy naděje, že by jeho 1024bitový modul (klíč) RSA mohl snad ještě nějakou dobu vydržet. Současně s tím se autor článku zároveň popřel, protože v úvodu velmi správně začal větou, že se nejedná o nový a zásadní objev, ale o optimalizaci známých technik. Bez komentáře už ponechávám celý zbytek článku, alespoň prozatím, a shrnuji velmi krátce: **1024bitový modul je v tom samém bezpečí, jako byl dříve.**

Na podporu tohoto tvrzení bych chtěl uvést názory tří odborníků. Čtenářům Crypto-Worldu doporučuji přečíst si celá jejich vyjádření, z nichž zde uvádím pouze nejnutnější citace. Prvním zdrojem je jakoby "poškozený" Bernsteinovým příspěvkem, tj. společnost RSA Security, která odpovídá ústy RSA Laboratories. Druhým je známý bezpečnostní specialista Bruce Schneier, kterého bychom mohli považovat za nezávislého v tomto "sporu", a třetím je sám profesor Bernstein, snad dostačující kapacita k výkladu své práce. Je možná s

podivem, že všichni tři, tj. "poškozený", "nezávislý expert" a "viník", se na rozdíl od článku JP shodují v následujícím faktu (italikou):

*Označme f(n) délku modulu, které Bernsteinova zlepšení metody NFS zvládají faktorizovat ve stejném čase jako předchozí stroje zvládaly faktorizovat n-bitové moduly metodou NFS bez Bernsteinových zlepšení (*pozn.: oba hypotetické stroje považujeme za univerzální, což znamená, že zvládají faktorizovat moduly pro všechny délky n, n > k, k ∈ **Z**). *Vše, co víme, je, že f(n) pro n blízká nekonečnu může být v ideálním případě nejlépe 3n. Avšak nevíme nic o f(n) pro malá čísla, například 512, nevíme, zda f(512) není dokonce větší než 512.*

Mimo jiné tedy pro malá čísla jako jsou 512, 1024 nebo 4096 mohou Bernsteinova zlepšení ve skutečnosti zhoršovat výkonnost NFS. Proto **Bernsteinův příspěvek o konkrétních zajímavých délkách modulů (tisíce bitů) nečiní žádné závěry. Zejména nečiní závěry, že by jeho příspěvek pro tyto konkrétní malé délky (tisíce bitů) zlepšoval nebo zhoršoval metodu NFS a nedává ani jakékoliv jiné číselné odhady pro ně**. Bernstein to přímo navíc stvrzuje ve svém e-mailu [2] slovy: "*v současné době nelze ani stanovit cenu za faktorizaci 1024, 1536 nebo 2048bitového modulu*" a podobně reaguje Bruce Schneier [1]: "*Je nepravděpodobné, že by Bernsteinova zlepšení byla využitelná ke zlepšení rychlosti faktorizace prakticky použitelných modulů.*" i RSA Laboratories [3]: "*Bernsteinův příspěvek nepřinesl pro 1024bitové moduly žádné nové ohrožení*."

Pochopitelně, že tyto závěry si mohl udělat každý, kdo si podrobně prostudoval Bernsteinův příspěvek [4]. Tím méně pochopitelný je směr, kam zavedl čtenáře článek JP, který [4] také cituje. JP se ale také odvolává na "komentátory", a v tom zřejmě tkví zakopaný pes. Komentátoři a internetové zdroje totiž z Bernsteinova poměrně starého příspěvku (11/2001) udělali v únoru a březnu t.r. aféru, která mohla vyústit v masové výměny klíčů (viz návody jako v JP: "...nepoužívat již dnes RSA s délkou n kratší než 2048 bitů").

Pan profesor Bernstein za ony výklady ani za senzacechtivost komentátorů nemůže. Zaslouží si naopak ocenění za skvělé nápady, kde by se dalo co dolaďovat při *realizaci* metody NFS pro faktorizaci. Jsou to nové myšlenky, které osvěžují výzkum na tomto poli. Možná z nich vzejde něco většího, možná o nich za pár let nebude nikdo vědět. Faktem ale je, že jeho příspěvek RSA nepohřbil, na čemž se odborníci vzácně shodují.

Literatura

[1] Bruce Schneier: CRYPTO-GRAM, March 15, 2002, dostupné na http://www.counterpane.com/crypto-gram.html

[2] e-mail, 28 Feb 2002, From: "D. J . Bernstein" <djb@cr.yp.to>, Subject: What's going on with factorization (na požádání zašlu, vlastimil.klima@i.cz)

[3] Has the RSA algorithm been compromised as a result of Bernstein´s paper?, April 8, 2002, dostupné na www.rsasecurity.com/rsalabs/technotes/bernstein.html

[4] Bernstein D.J: Circuits for integer factorization: a proposal, http://cr.yp.to/papers/nfscircuit.ps , původní článek

E. Letem šifrovým světem

1. Velikonoční kryptologie

V pěkném a moderním prostředí konferenčního sálu Moravské zemské knihovny v Brně proběhl 3.-4.4.2002 mezinárodní workshop - Velikonoční kryptologie.

Největší ohlas mezi účastníky měla přednáška ing. Tomáše Rosy. Velký zájem byl i o aktuální informace k nově přijatému zákonu o elektronickém podpisu na Slovensku.
Setkání probíhalo v příjemné poklidné atmosféře a díky výborné práci organizačního výboru zcela bezproblémově.

Na závěr ohlásil Dr.Václav Matyáš, že příštího setkání – Mikulášské kryptobesídky 2002 se pravděpodobně zúčastní i hvězdy první velikosti Adi Shamir (RSA, TWINKLE,…) a Vincent Rijmen (AES). Takovéto setkání si jistě nemůžete nechat ujít, a proto si již teď ve svém kalendáři tuto plánovanou akci zaznamenejte.

3. dubna 2002 (středa)
Elektronický podpis
Daniel Olejár, Jaroslav Janáček, UK Bratislava - Aktuálne o návrhu slovenského zákona o elektronickom podpise
Tomáš Rosa, ICZ a ČVUT Praha - O klíčových kolizích v podpisových schématech

Panelová diskuze "Kvantová kryptologie"
Luděk Smolík, seculab - moderátor
Panelisté: Martin Hendrych, SLO UP a FZÚ AV ČR , Jaroslav Hrubý, GCUCMP , Tomáš Rosa, ICZ

4. dubna 2002 (čtvrtek)
Trendy a problémy
Werner Koch, g10 Code GmbH a projekt Aegypten - The Modular Architecture of the Aegypten Project

Michal Sasínek, NBÚ SR - Národný bezpečnostný úrad SR - poslanie a perspektívy

Mark Harris, nCipher - Cryptographic Module "Secure Signature Creation Device"

Karel Dolník, Ministerstvo obrany - Hlediska výběru vhodných eliptických křivek pro asymetrické kryptosystémy

Nové algoritmy a postupy
Jiří Dvorský, Eliška Ochodková, Václav Snášel, VŠB Ostrava - Hashovací funkce založená na kvazigrupách - pokračování

Jaroslav Hrubý, GCUCMP - Matematizace komplexní bezpečnosti a Lorentzův model

Panelová diskuze "Stanovení míry kryptografické bezpečnosti a přijatelná rizika kryptografické bezpečnosti"
Pavel Vondruška, ÚOOÚ - moderátor
Panelisté: Jindřich Kodl, ÚV ČR , Tomáš Rosa, ICZ , Michal Sasínek, NBÚ SR , Luděk Smolík, seculab , Jozef Vyskoč, VaF

Většina přednesených příspěvků je dostupná na
http://ecom-monitor.cz/velikonoce/vk_program.html

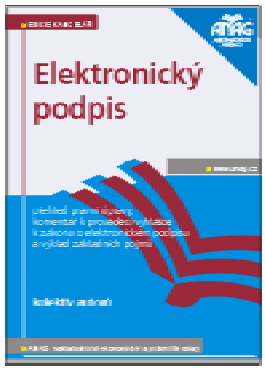
Malou galerii momentek z konference najdete na domovské stránce Crypto-Worldu.

2. Elektronický podpis autorů Bosáková, Kučerová, Peca, Vondruška

http://www.anag.cz/shop/index.php?page=product&id=21&pid=3370

Jan Hobza http://www.volny.cz/honzahobza

V tomto čase se na pult knihkupectví ANAG dostává nová kniha s jednoduchým názvem Elektronický podpis. Je to vůbec poprvé, kdy v České republice vychází takto ucelený přehled právní úpravy elektronického podpisu s komentářem k prováděcí vyhlášce a s výkladem základních pojmů této problematiky. Autory knihy jsou odborníci z Úřadu pro ochranu osobních údajů, kteří stáli i u zrodu prováděcí vyhlášky k zákonu o elektronickém podpisu.



Nakladatelství ANAG si k vydání této naučné publikace nemohlo vybrat lepší chvíli. Před několika dny nabylo účinnosti rozhodnutí Úřadu pro ochranu osobních údajů, kterým se uděluje vůbec první společnosti u nás akreditace k působení jako akreditovaný poskytovatel certifikačních služeb podle zákona o elektronickém podpisu. Od 1. 10. 2000, kdy vstoupil v účinnost zákon o elektronickém podpisu, tak uplynulo téměř jeden a půl roku, než byly překonány všechny legislativní a administrativní překážky užívání zaručeného elektronického podpisu podle zákona. Široké veřejnosti se tak otevírá možnost platně činit řadu právních úkonů elektronicky a jistě v dohledné době i využívat elektronické prostředky ke komunikaci s úřady státní správy.

Nutnou podmínkou je však znalost občanů alespoň základních práv a povinností spojených s používáním elektronického podpisu a také elementárních technických postupů vytváření a ověřování elektronického podpisu. Kniha Elektronický podpis poskytuje nejen tyto informace, ale je adresována i čtenářům, kteří se elektronickým podpisem zabývají profesionálně. Převážná část knihy je určena rozboru právních aspektů elektronického podpisu a povinností jednotlivých subjektů, které figurují v procesu poskytování a užívání certifikačních služeb. Autoři se pak především soustředili na poskytovatele certifikačních služeb, kteří působí či hodlají působit v rámci zákona o elektronickém podpisu. Součástí knihy je i velice kvalitní překlad Směrnice Evropského parlamentu o zásadách společenství pro elektronické podpisy, která představuje primární motiv, ale i cílovou šachovnici přijímaných právních předpisů pro elektronické podpisy.

Druhá část knihy je určena především širokému okruhu čtenářů. Jsou zde vysvětleny základní pojmy, které nabývají v současné době na popularitě i díky propagaci elektronického podpisu v masmédiích. Ve své profesní praxi se často setkávám s neznalostí či

neporozuměním ať už základních či složitějších institutů elektronického podpisu a to jak na straně laické veřejnosti, tak ze strany některých odborníků. Příčina těchto nejasností však není chybou posluchačů, ale spatřuji ji v neexistenci kvalitní literatury, která by korektním způsobem dokázala popsat a vyložit tyto pojmy. Kniha elektronický podpis má jistě ambice tuto znalostní mezeru vyplnit. Čtenář má možnost pochopit, co znamená a jaké důsledky má tzv. akreditace, co je elektronická podatelna, k čemu slouží certifikáty, jaké jsou povinnosti podepisující osoby apod.

V České republice, jako v jednom z mála evropských států, existuje komerční subjekt, který vydává tzv. kvalifikované certifikáty pro zaručené elektronické podpisy. Pouze málo občanů však ví, k čemu lze těchto služeb využít a jaké výhody přinášejí. Naopak nepřiměřené politické proklamace a víra, že elektronický podpis dokáže spasit státní správu, působí na obecné povědomí o tomto kryptografickém pojmu kontraproduktivně. Publikace Elektronický podpis odborníků na danou problematiku se vyrovnává s tímto nedostatkem a věřím, že v budoucí době přispěje k vyjasnění veřejného povědomí.

Elektronický podpis – přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů , Mgr. Dagmar Bosáková, JUDr. Alena Kučerová, JUDr. Jaroslav Peca, Mgr. Pavel Vondruška. Nakladatelství ANAG, 4/2002. Počet stran 144. Cena 169,- Kč.

3. EUROCRYPT 2002

Amsterdam, April 28 - May 2, 2002

Koncem tohoto měsíce proběhne nejvýznamnější evropské setkání kryptologů – EUROCRYPT. V tomto roce se koná v nizozemském Amsterdamu.

PROGRAM
Session 1: Cryptanalysis I
Session 2: Public-Key Encryption
Session 3: Invited Talk (AES and the wide trail design strategy , Joan Daemen , Vincent Rijmen)
Session 4: Information Theory & New Models
Session 5: Implementational Analysis
Session 6: Stream Ciphers
Session 7: Digital Signatures I
Session 8: Cryptanalysis II
Rump Session
Session 9: Key Exchange
Session 10: Modes of Operation
Session 11: Invited Talk
Session 12: Digital Signatures II
Session 13: Traitor Tracing & Id-based Encryption
Session 14: Multiparty and Multicast
Session 15: Symmetric Cryptology

http://www.ec2002.tue.nl/program.htm

PŘEDSTAVUJEME

4. e-Government v Dolním Sasku

V Dolním Sasku byl zahájen projekt "automatizovaných systémů pro hospodaření s rozpočtem". Tento projekt, který patří do oblasti e-Government, je zaváděn v 750 státních subjektech celkem s 15 000 pracovníky a je jednoznačně nejširším uplatněním elektronického podpisu dle německého zákona.

Základem automatizace "systémů pro hospodaření s rozpočtem" je využití softwaru "Public Performance Management" (PPM) firmy Baan. Všechny zápisy ve státních subjektech týkající se dolnosaského zemského rozpočtu se budou provádět elektronicky. Současně zanikne vyplňování dosavadních papírových dokladů. Systém umožňuje elektronicky podepsat pokladní příkazy a zaručuje nedotknutelnost a důvěrnost zpracovávaných dat. Použitá metoda pomáhá jak k zabezpečení celého systému, tak i k ochraně před riziky ze strany zaměstnanců, kteří se na práci podílejí.

Garantem projektu je Centrum informatiky Dolního Saska ("Informatikzentrum Niedersachsen" - IZN) ve spolupráci s dolnosaským ministerstvem financí.

5. ČESKÉ FÓRUM PRO INFORMAČNÍ SPOLEČNOST

České fórum pro informační společnost (dále ČFIS) je poradním orgánem Rady vlády ČR pro SIP (státní informační politiku). Bylo zřízeno v roce 1999 a je složeno z vlivných aktérů rozvoje IS a ovlivňovaných skupin veřejnosti. Jeho posláním je podporovat dialog o vývoji informační společnosti, technických, technologických, vzdělanostních, společenských, kulturních, náboženských, sociálních, ekonomických, etických, bezpečnostních, ekologických a obranných aspektech tohoto vývoje, rizicích a příležitostech a o roli vlády a veřejnosti v tomto procesu.

Pro realizaci odborné činnosti ČFIS vytváří pracovní skupiny, ve kterých vznikají podněty určené nejen Radě vlády ČR pro SIP.

Informace: http://www.info-forum.cz
Diskusní fórum: http://cfis.uvis.cz
Kontakt: forum@uvis.cz

Funkci sekretariátu ČFIS vykonává Sekretariát Rady vlády ČR pro státní informační politiku, který sídlí v budově Úřadu pro veřejné informační systémy, Havelkova 22, Praha 3.

PRACOVNÍ SKUPINY

Pracovní skupina 1 – Gramotnost pro 21. století	psl@uvis.cz
Pracovní skupina 2 – Elektronický obchod	winter@brezen.cz
Pracovní skupina 3 – Transformace podniků a firem do 21. století	ps3@uvis.cz
Pracovní skupina 4 – Zdravotní péče v informační společnosti	ps4@uvis.cz
Pracovní skupina 5 – Stát jako služba pro občana	owner-skupina-l@ecn.cz
Pracovní skupina 6 - Harmonický rozvoj informační společnosti	cfis6@mlp.cz

6. O čem jsme psali v dubnu roku 2000 a 2001

Crypto-World 4/2000

Crypto-World 4/2001

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