Crypto-World

Informační sešit GCUCMP

Vychází za podpory společnosti AEC-Data security company

Ročník 4, číslo 2/2002 **18. únor 2002**

2/2002

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
(>340 e-mail výtisků)

Obsah : **Str.**

Příloha: Program pro naše čtenáře : „Hašák ver. 0.9“ (viz. letem šifrovým světem) hasak.zip

A. Vyhláška č.366/2001 Sb., bezpečný prostředek pro vytváření elektronického podpisu a nástroj elektronického podpisu

Mgr. Pavel Vondruška (ÚOOÚ)

Anotace

Článek se zabývá rozborem prováděcí vyhlášky 366/2001 Sb. Úřadu pro ochranu osobních údajů, která upřesňuje povinnosti zákona o elektronickém podpisu č.227/2000. Speciálně jsou rozebírány požadavky na nástroj elektronického podpisu (legislativní a právní) a stanovení shody nástrojů elektronického podpisu s požadavky stanovenými zákonem a prováděcí vyhláškou.

1. Vyhláška č.366/2001 Sb.

V říjnu roku 2000 vstoupil v České republice v účinnost Zákon o elektronickém podpisu a o změně některých dalších zákonů č.227/2000 (dále jen Zákon č.227/2000 Sb.). Následovala řada dalších kroků nutných k tomu, aby mohla být realizována komunikace podle tohoto zákona. Na základě zmocnění uvedeného v tomto zákoně připravil Úřad pro ochranu osobních údajů znění návrhu vyhlášky, ale se zahájením legislativních kroků k jejímu přijetí musel počkat do května 2001. Čekalo se na novelu zákona č.101/2000 Sb., která Úřadu (zjednodušeně řečeno) umožnila nejen vyhlášku připravit, ale také publikovat ve sbírce zákonů. Vyhláška byla publikována 10.10.2001. Je určena především poskytovatelům certifikačních služeb a upřesňuje požadavky na ty poskytovatele, kteří hodlají vydávat kvalifikované certifikáty, upřesňuje postup akreditace těch poskytovatelů certifikačních služeb, kteří zažádali ÚOOÚ o akreditaci a dále upřesňuje požadavky na nástroje elektronického podpisu.

Tento příspěvek bude věnován vysvětlení pojmu prostředek pro bezpečné vytváření a ověřování elektronického podpisu (§7 vyhláška), nástroj elektronického podpisu (§8 vyhlášky), vztahu mezi nástrojem elektronického podpisu a prostředkem pro bezpečné vytváření a ověřování elektronického podpisu, postupu při vyslovení shody nástroje s požadavky stanovenými v zákoně o elektronickém podpisu, rozdílu v chápání těchto pojmů v Evropské unii a v českém zákoně o elektronickém podpisu.

2. Prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů

Začněme informací k překladu těchto pojmů z anglicky psaných materiálů Evropské unie. Je potřeba vědět, že v těchto materiálech se používá pro nástroj elektronického podpisu termín „product“ („electronic-signature product“ – nástroj elektronického podpisu), zatímco termín „device“ je určen pro český termín prostředek (např. Secure Signatur-Creation Device - prostředek pro bezpečné vytváření elektronických podpisů).

Prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů jsou definovány v §17 zákona o elektronickém podpisu č.227/2000 Sb. Požadavky na tyto prostředky vycházejí z obdobných obecných požadavků Směrnice 1999/93ES o zásadách Společenství pro elektronické podpisy tak, jak jsou uvedeny v příloze č.III. tohoto dokumentu.

Tyto požadavky mají především zajistit to, aby prostředek pro bezpečné vytváření podpisu za pomoci odpovídajících technických a programových prostředků a postupů zaručil, že data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno, že data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření a že podpis je chráněn proti padělání s využitím existující dostupné technologie. Tento prostředek musí dále zajistit, aby data pro vytváření podpisu mohla být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou. Prostředky pro bezpečné vytváření podpisu nesmí měnit data, která se podepisují, ani zabraňovat tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování.

Obdobné jsou i bezpečnostní a procesní požadavky na prostředek pro bezpečné ověřování podpisu. Nově se zde zavádějí požadavky související se zobrazením výsledku ověření, případně se spolehlivým zobrazením dat uvedených v certifikátu. Zejména to jsou tyto požadavky: podpis musí být spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen, ověřující osoba musí mít možnost spolehlivě zjistit obsah podepsaných dat, spolehlivě musí být zjištěna pravost a platnost certifikátu při ověřování podpisu, výsledek ověření a případné použití pseudonymu musí být řádně zobrazeno.

Uvedené požadavky jsou příliš obecné, a proto je upřesňuje prováděcí vyhláška k zákonu o elektronickém podpisu č. 366/2001 Sb. v paragrafu 7. Konkretizuje zde alespoň některé z požadavků, např. vyžaduje, aby podepisující se osoba byla informována, že používá tento prostředek a musela před jeho použitím zadat přístupové heslo nebo použít jiný obdobný autentizační mechanismus. Upřesněny jsou i požadavky na kryptografické algoritmy a jejich parametry. Tyto požadavky jsou uvedeny v příloze č. 2 této vyhlášky. Příloha byla zpracována podle obdobného dokumentu evropské unie a to podle dokumentu Algorithms and Parameters for Secure Electronic Signatures, který vydala iniciativa EESSI (The European Electronic Signature Standardization Initiative). V tomto dokumentu se stanoví asymetrické kryptografické algoritmy včetně algoritmů založených na eliptických křivkách, které budou pro účely bezpečných elektronických podpisů považovány po dobu 5-ti let za bezpečné. V tomto dokumentu jsou stanoveny i parametry klíčů, způsob generování klíčů a další podrobnosti.

Česká vyhláška dále vyžaduje pro prostředek pro bezpečné vytváření zaručeného elektronického podpisu dostatečnou technickou a kryptografickou záruku bezpečnosti; tento požadavek se považuje za splněný, pokud prostředek odpovídá požadavkům technické normy upravující oblast informační bezpečnosti. Touto normou je ČSN ISO 15408 a příslušná úroveň záruky je EAL 4. Tento požadavek byl stanoven v souladu s dokumenty standardizační komise CEN/ISSS (European Committee for Standardization / Information Society Standardization System) N137-Secure Signature - Creation Device a N141-Security Requirements for Signature Creation Applications.

Splnění požadavků na prostředek pro bezpečné vytváření zaručeného elektronického podpisu stanovených v § 17 zákona o elektronickém podpisu se dokládá výsledkem hodnocení prostředku pro bezpečné vytváření zaručeného elektronického podpisu a seznamem technických norem upravujících oblast informační bezpečnosti, podle kterých byl hodnocen. Nikde není stanoveno, kdo takovéto hodnocení může provést. Předpokládá se přebírání hodnocení ze vznikajících laboratoří v EU. Časem pravděpodobně vznikne nějaké hodnotitelské pracoviště i v ČR. Aby bylo uznáno hodnocení tohoto pracoviště i v zemích EU, je nutné zapojení tohoto pracoviště do evropského akreditačního schématu. Ve Směrnici 1999/93ES Evropského parlamentu a rady ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy se k hodnocení prostředků pro elektronické podpisy píše pouze toto:

„Shoda prostředků pro bezpečné vytváření podpisů s požadavky uvedenými v příloze III bude určena odpovídajícími veřejnoprávními či soukromými organizacemi určenými členskými státy. V souladu s postupem uvedeným v článku 9 stanoví Komise kritéria pro členské státy pro rozhodnutí, zda by tato organizace měla být určena.“

V současné době ještě ve státech EU není zcela shoda v tom, jak bude tento paragraf Směrnice naplněn.

Náš zákon o elektronickém podpisu nestanoví žádnému subjektu povinné používání takovéhoto prostředku. Je pouze na podepisující osobě nebo na osobě, která se spoléhá na podpis, zda takový prostředek (např. z důvodu vyšší bezpečnosti a tedy i právní jistoty) používá nebo ne. Poněkud deklarativně se o tomto podpisu mluví pouze v odstavci 2, paragrafu 3.
„Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.“

V dokumentech Evropské unie se vžilo označení pro takovýto podpis – tedy zaručený elektronický podpis, založený na kvalifikovaném certifikátu a vytvořený pomocí prostředku pro bezpečné vytváření elektronického podpisu - zkrácené označení „kvalifikovaný podpis“. Osoba, která se spoléhá na kvalifikovaný podpis, má samozřejmě velikou důvěru v takovouto komunikaci. Nemá však možnost z podpisu přímo zjistit, zda se jedná o kvalifikovaný nebo nekvalifikovaný podpis (přesněji zda při vytváření podpisu byl nebo nebyl použit prostředek pro bezpečné vytváření elektronického podpisu). Navrhuje se tedy, aby osoba, která vlastní prostředek pro bezpečné vytváření elektronického podpisu, si tuto informaci nechala zapsat do svého kvalifikovaného certifikátu. Pokud by vytvořila podpis založený na tomto certifikátu bez použití tohoto prostředku – musí o tom druhou stranu (např. v podepsaném textu) informovat.

V dokumentech Evropské unie se doporučuje pro tento typ podpisu zavádět v příslušných legislativních úpravách stejnou právní akceptovatelnost jako u podpisu vlastnoručního. Upozorňuji, že pouhé konstatování, že se jedná o kvalifikovaný (bezpečný) elektronický podpis nestačí, aby byl takovýto podpis právně akceptovatelný všude tam, kde se používá vlastnoruční podpis. Toto tvrzení se mylně v médiích uvádí, ale není pravdivé. Je nutné provést příslušné legislativní změny, které použití jakéhokoliv typu elektronického podpisu (tedy případně i kvalifikovaného podpisu) v příslušném procesu umožní.

Shrnutí
1. V českém zákoně o elektronickém podpise není stanovena žádnému subjektu povinnost používat prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů.
2. používáním těchto prostředků se zvyšuje důvěra v tuto komunikaci
3. kvalifikovaný podpis je zaručený elektronický podpis založený na kvalifikovaném certifikátu a vytvářený prostředkem pro bezpečné vytváření elektronického podpisu
4. zjednodušeně řečeno - prostředky pro bezpečné vytváření a ověřování zaručených elektronických podpisů musí splňovat bezpečnostní požadavky podle ISO 15408 , na úroveň záruky EAL 4, v ČR je toto hodnocení uznáváno z libovolné testovací laboratoře, která je schopna tyto testy provádět

3. Nástroj elektronického podpisu

Nástroj elektronického podpisu je širší pojem než prostředek pro bezpečné vytváření a ověřování elektronického podpisu.

V zákoně o elektronickém podpisu č.227/2000 Sb. je definován v §2, písmeno o) takto: „Pro účely tohoto zákona se rozumí nástrojem elektronického podpisu technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů“.

Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty podepisuje svým zaručeným elektronickým podpisem kvalifikované certifikáty a seznamy kvalifikovaných certifikátů, které byly zneplatněny. Nástroj elektronického podpisu používaný pro toto podepisování nelze z důvodu vyšší bezpečnosti použít pro jiné než tyto účely (§3 vyhlášky č.366/2001 Sb.) !

Poskytovatel certifikačních služeb vydávající kvalifikované certifikáty musí používat bezpečný nástroj elektronického podpisu a toto musí být ověřeno Úřadem pro ochranu osobních údajů.
Toto je stanoveno v českém zákoně o elektronickém podpisu v §6, odst.1, písm. j) „… nástroj elektronického podpisu je bezpečný, pokud odpovídá požadavkům stanoveným tímto zákonem a prováděcí vyhláškou; toto musí být ověřeno Úřadem pro ochranu osobních údajů (dále jen "Úřad")" ,

Úřad pro ochranu osobních údajů vyhodnocuje na základě písemné žádosti shodu nástrojů elektronického podpisu určených pro podepisování vydávaných kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, s požadavky stanovenými zákonem o elektronickém podpisu.

V žádosti o vyhodnocení shody musí být obsaženy informace, které vyhodnocení umožní. Úřad zveřejňuje požadavky na bezpečnost příslušných kryptografických modulů ve Věstníku Úřadu. Tento způsob byl zvolen především s ohledem na možnost rychle reagovat na skutečnost, že standard FIPS 140-1 je v současné době nahrazován standardem FIPS 140-2 a dále, že Evropská společenství vyvíjejí vlastní ekvivalentní standard.

Ve Věstníku Úřadu č.12/2001 a na svých webových stránkách Úřad zveřejnil požadavek na kryptografické funkce: nástroj elektronického podpisu musí splňovat požadavky na Security Level 3 podle standardu pro hodnocení bezpečnosti kryptografických modulů vydaného National institute of standards and technology v USA - FIPS PUB 140.

Kromě povinných součástí žádosti (podrobný popis funkce, technická dokumentace, výsledek hodnocení kryptografických funkcí) se doporučuje v zájmu urychlení správního řízení současně s podáním žádosti dodání následujících dokumentů::

- přesná identifikace nástroje
- obecné informace k dovozu, výrobě a prodeji nástroje
- manuál (v českém jazyce, případně v anglickém jazyce)
- seznam a parametry kryptografických funkcí a jejich přesnou identifikaci ve vztahu k algoritmům a parametrům uvedeným v příloze č. 2 vyhlášky
    - § podpisová schémata
    - § algoritmy pro generování klíčů
    - § metody generování náhodných čísel

- popis použitého generátoru náhodných čísel
- popis, jak lze při použití nástroje realizovat požadavek § 3 odst. 3 vyhlášky č. 366/2001 Sb. (uvádění do provozu a změna pracovního módu dvěma pracovníky v odlišných rolích)
- V rámci správního řízení může Úřad požádat o doplnění předložených dokumentů, případně o doplnění informací či o prokázání dalších souvisejících skutečností.

Požadavek na výsledek hodnocení kryptografických funkcí se považuje za splněný, pokud byl nástroj hodnocen podle Standardu pro hodnocení bezpečnosti kryptografických modulů vydaného National institute of standards and technology v USA - FIPS PUB 140, Security Level 3, a provedené hodnocení je doloženo příslušným certifikátem, notářsky ověřeným a je připojen úřední překlad certifikátu do českého jazyka.

Pokud nástroj elektronického podpisu splnil požadavky stanovené zákonem o elektronickém podpisu a Úřad vyslovil shodu, je nástroj považován za bezpečný. Seznam nástrojů, u nichž byla vyslovena shoda, zveřejňuje Úřad ve Věstníku Úřadu a na svých www stránkách. V příloze č.2 je uveden seznam nástrojů u nichž byla vyslovena shoda (aktuální stav k 11.2.2002).

Žádné jiné subjekty (tj. např. podepisující se osoba, elektronická podatelna, poskytovatel certifikačních služeb, který nevydává kvalifikované certifikáty) nemají za povinnost takovýto nástroj používat. Cena takovéhoto nástroje je vysoká a pohybuje se v tisících USD.

Za podání žádosti o vyhodnocení shody nástrojů elektronického podpisu s požadavky se platí správní poplatek 10 000,- Kč.

Shrnutí
1.Nástroj elektronického podpisu je prostředek pro vytváření elektronického podpisu, který lze používat k podepisování kvalifikovaných certifikátů a seznamu certifikátů, které byly zneplatněny.
2. Poskytovatelé certifikačních služeb, kteří vydávají kvalifkované certifikáty, musí takovýto nástroj používat.
3. Shodu nástroje s požadavky zákona o elektronickém podpisu vyslovuje v České republice Úřad pro ochranu osobních údajů.

4. Evropská unie

Základní informace byly uvedeny již v odstavcích 2 a 3. Zde tedy pouze shrneme.

Ve Směrnici 1999/93ES Evropského parlamentu a rady ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy se rozlišují prostředky pro bezpečné vytváření elektronického podpisu (SSCD – Secure signature electronic device) a nástrojem elektronického podpisu (electronic signature product). Požadavky na prostředky pro bezpečné vytváření elektronického podpisu jsou uvedeny v příloze Směrnice číslo III. Shoda prostředků pro bezpečné vytváření podpisů s požadavky uvedenými v příloze III má být určena odpovídajícími veřejnoprávními či soukromými organizacemi určenými členskými státy. O tom, zda má být také hodnocen nástroj elektronického podpisu, není ve Směrnici stanoveno.

Závěrem uvádím e-mail z 8.2.2002, ve kterém odpověděl Hans Nilsson – jeden z předních odborníků na elektronický podpis v EU, člen komise EESSI (European Electronic

Signature Standardization Initiative) na dotaz, zda by pomohl objasnit pojmy nástroj a prostředek a otázku jejich hodnocení.

„…Yes, interpreting the Directive is certainly very difficult…The EESSI and industry „Interpretation“ is the following:

The SSCD (Annex III) is the smart card or other hardware device protecting the private key. And this SSCD needs to be evaluated and approved in order to be sold and marketed as a SSCD.

The German and Austrian SiG requires evaluation and approval for software products distributed by ACCREDITED CAs, which is a „higher level“ of CA approval. However, Germany and Austria are alone with this interpretation, and I think it will actually disappear in those two countries“.

Na základě výše uvedených faktů se domnívám, že interpretace pojmů nástroje a prostředku elektronického podpisu je v českém zákoně o elektronickém podpisu č.227/2000 Sb. a prováděcí vyhlášce č.366/2001 Sb. v zásadě v souladu se Směrnicí 1999/93ES Evropského parlamentu.

Shrnutí

1) prostředky pro bezpečné vytváření elektronického podpisu musí být hodnoceny v EU i ČR a to podle stejných kritérii, v ČR chybí hodnotitelské pracoviště, hodnocení je možné převzít ze zahraničí
2) nástroje elektronického podpisu nemusí být v současné době hodnoceny ve všech státech EU, musí být hodnoceny v Německu a Rakousku, v ČR musí být hodnoceny pouze nástroje, které používá poskytovatel vydávající kvalifikované certifikáty a to jen ty, které používá k podpisům kvalifikovaných certifikátů a seznamu kvalifikovaných certifikátů, které byly zneplatněny, shodu s požadavky vyslovuje ÚOOÚ

Příloha č.1

Kryptografické algoritmy a jejich parametry pro vytváření párových dat poskytovatele a pro prostředky pro bezpečné vytváření a ověřování zaručeného elektronického podpisu

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Algoritmus pro 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

Příloha č.2

Seznam nástrojů, u nichž byla vyslovena shoda s požadavky zákona o elektronickém podpisu č.227/2000 Sb. (stav k 11.2.2002).

Tento seznam je zveřejněn Úřadem pro ochranu osobních údajů ve Věstníku Úřadu a na www stránce Úřadu (http://www.uoou.cz/ep_nastroje.php3).

Poř. čís.	Nástroj elektronického podpisu	Výrobce
1.	**CSA8000;** Hardware Revision: G, Firmware Version 1.1, pracující ve FIPS módu	Eracom Technologies Australia, Pty. Ltd. Burleigh Heads Queensland Austrálie
2.	**nShield F3 SCSI;** Firmware 5.0, Hardware verze nC4032W-150, pracující ve FIPS módu	nCipher Corporation Ltd. Jupiter House Station Road Cambridge CBI 2JD, United Kingdom

Literatura

[1] Matejka,J.,Vondruska,P.: The basic terms and legal aspects of the ESA from the practical use and security points of view, sborník mezinárodní konference IDET, Brno 2001

[2] Vondruška,P.: Typy elektronických podpisů, Sborník konference Bezpečnosť dát 2001, Bratislava

[3] Vondruška,P.: Bezpečnostní aspekty elektronického podpisu, sborník Konference Security 2001, Praha

[4] Vondruška,P.: Anatomie prováděcí vyhlášky ÚOOÚ k zákonu o elektronickém podpisu č.227/2000 Sb., Sborník, Konference Současnost a budoucnost krizového managementu, Praha 2001

[5] Vondruška,P.: Elektronický podpis, publikace nakladatelství RAABE, v tisku, 2002

[6] Directive EU: Evropská komise DG XV - Directive 1999/93/EC of 13 December 1999 on a community framework for electronic signatures, *http://www.ict.etsi.org/eessi/e-sign_directive.pdf*

[7] CEN/ISSS, European Committee for Standardization / Information Society Standardization System, *http://www.ni.din.de* , *http://www.cenorm.be/isss/worksho/e-sign*

[8] EESSI, European Electronic Signature Standardization Initiative *http://www.ict.etsi.org/eessi/EESSI-homepage.htm*

[9] Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) č.227/2000 Sb., http://www.mvcr.cz/sbirka/2000/sb068-00.pdf

[10] Vyhláška ÚOOÚ 366/2001 Sb. (k Zákonu o elektronickém podpisu č.227/2000 Sb.), http://www.mvcr.cz/sbirka/2001/sb138-01.pdf

B. RUNS TESTY

RNDr. Petr Tesař

Při hodnocení kvality generátorů náhodných bitů (dále též ang. RNG) pro kryptologické účely se využívají statistické testy. Publikovaných testů je nepřeberně, a každý si může případně zkonstruovat vlastní. Z historického hlediska se některé testy označují jako klasické (základní, standardní). Mezi klasické testy řadíme zejména test frekvencí bitu jedna (nebo nula), poker testy (= testy výskytu n-tic bitů pro n = 2, 3, ….), autokorelační testy a také runs testy (česky – testy sérií). Pro praktické použití se vybrané testy sdružují do testovacích baterií - NIST 800 (viz [3]), FIPS 140 (viz [4] a [5]), DIEHARD (viz [6]) nebo VANAD (viz [7]) a test sérií (v různých variantách) je pochopitelně obsažen v každé z uvedených baterií.

Pro účely tohoto článku se budeme zabývat pouze binární verzí testu sérií (pro kryptologické účely má tato verze největší smysl). Sérií délky j rozumíme úsek bitové posloupnosti stejných binárních znaků o počtu j-bitů, který je z obou stran ohraničen opačným binárním znakem nebo koncem (resp. začátkem) posloupnosti. Například následující binární posloupnost:

1 1 0 1 0 0 0 1 1 1 1 1 1 0 1 0 1 0 0 1 1 0 1 1 0 0 1 0 1 0 1 1 1 0 0 0

obsahuje celkem 20 sérií, z toho sérií bitu jedna délky 1 je 5, sérií bitu jedna délky 2 jsou 3, sérií bitu jedna délky 3 je 1, sérií bitu jedna délky 6 je 1, sérií bitu nula délky 1 je 6, sérií bitu nula délky 2 jsou 2, sérií bitu nula délky 3 je 2. Zapsáno do tabulky

Délka série	Počet sérií nul	Počet sérií jedniček	Počet sérií dané délky
1	6	5	11
2	2	3	5
3	2	1	3
4	0	0	0
5	0	0	0
6	0	1	1
> 6	0	0	0
Celkem	10	10	20

Z tabulky je vidět, co všechno lze v různých variantách runs testů testovat:

V1. Celkový počet sérií v posloupnosti bez ohledu na jejich délku a “barvu” (= nuly, jedničky). Tato nejjednodušší varianta testu sérií je například použita v baterii NIST 800.
Na tomto místě si autor článku nemůže odpustit krátký názor na baterii NIST 800. Výběr použitých testů je pro autora článku zklamáním. Na jedné straně je zde mnoho exotických testů, jejichž využití pro kryptoanalýzu autor nevidí (např. testy náhodných procházek – používané spíše pro RNG v oblasti simulačních metod Monte Carlo), na druhé straně např. Univerzální test (viz Maurer [1]), jehož kryptografický význam je zřejmý i laikovi v oboru, je aplikován v původní verzi popsané v [1], zatímco i autoři baterie NIST 800 přiznávají, že je jim známo radikalní vylepšení tohoto testu, publikované Coronem již v roce 1998.

(viz [8]). Za hlavní přínos této NIST publikace lze považovat nejspíše kapitolu 4 (4. Testing Strategy And Result Interpretation) dávající jisté náměty v oblasti, které se většina ostatních autorů freewarových testovacích baterií taktně vyhýbá.

V2. Počty sérií daných délek bez ohledu na "barvu". Tato varianta je použita např. v baterii VANAD, a pochopitelně mnohem citlivěji měří kvalitu generované posloupnosti.

V3. Počty sérií daných délek s rozlišením jejich barvy. V tomto případě je informace o sériích využita maximálně. Tato varianta je použita například v bateriích FIPS 140 (zde se ovšem každá délka a "barva" testuje extra). Globální varianta (tj. kdy je spočtena jedna statistika) je popsána např. v pracech [1] a [2]. V obou pracech je používána následující testová statistika:

$$S = \sum_{i=1}^{L} \frac{1}{E_i}(S1(i) - E_i)^2 + \sum_{i=1}^{L} \frac{1}{E_i}(S0(i) - E_i)^2$$

kde S1(i) je počet sérií jedniček délky i
S0(i) je počet sérií nul délky i
E_i je očekávaný počet sérií délky i (u kvalitní posloupnosti je pochopitelně stejný pro nuly i jedničky).
L je horní délka série, která se ještě počítá. Většinou se volí tak, aby očekávaný počet sérií délky L (E_L) byl aspoň pět.

Pokud testovaná posloupnost je výběrem z náhodné veličiny řídící se rovnoměrným rozdělením znaků nula a jedna, bude se statistika S asymptoticky řídit rozdělením chí-kvadrát o Q stupních volnosti.
A nyní se dostáváme ke stěžejní části tohoto článku. V Maurerově práci [1] je uvedeno:

$E_i = N / 2^{i+2}$ kde N je celková délka posloupnosti v bitech a
Q = 2 L

Naopak v práci [2] (Vanstone et al.) se dočteme, že

$E_i = (N - i + 3) / 2^{i+2}$ kde N je celková délka posloupnosti v bitech a
Q = 2L – 2

Čtenář se oprávněně zeptá – „Kde je pravda ?"
Při pohledu na obě varianty je vidět, že pro velká N budou očekávané hodnoty E_i v obou případech velmi podobné. To ovšem zaručeně neplatí pro stupně volnosti Q. Rozdíl v asymptotickém chování statistiky S uvedený v pracích [1] a [2] je tak velký, že se můžeme pokusit experimentálně rozhodnout, která z uvedených variant se více blíží realitě.

Jako testovací množiny náhodných bitů byly použity následující dva balíky:

Balík A. - 9600 posloupností o stejné délce 64 KB (tj. 524288 bitů). Tyto posloupnosti byly vygenerovány pseudonáhodným generátorem (angl. PRNG) společnosti Algorithmic Research. Jde o FIPS 140-1 level 3 certifikované zařízení, kde PRNG je na bázi fyzikálního seedu expandovaného algoritmem TDES (3-DES).

Balík B. - 10000 posloupností o stejných délkách 100 KB (tj. 819200 bitů). Tyto posloupnosti byly generovány PRNG společnosti Microsoft, obsaženém v operačního systému Windows 98.

Oba balíky byly prověřeny testovací baterií VANAD (sledovaný runs test byl vypnut) s výsledkem: Známka 1 – VYHOVUJE bez výhrad.

Oba balíky byly testovány oběma variantami runs testu pro různé hodnoty stupňů volnosti Q. Pro schodu empirické distribuční funkce testové statistiky S a příslušného chí-kvadrát rozdělení byl použit Kolmogorov – Smirnovův test (viz např. [9]). V tabulkách jsou navíc uvedeny tak zvané p-value (p-hodnoty). Běžně slouží k rozhodnutí, zda příjmeme hypotézu na dané hladině významnosti. Pokud je například hladina významnosti 0.01 (jedno procento), přijmeme hypotézu, pokud příslušné p-value je větší než 0.01.

A. Balík (9600 posloupností)

Maurerova varianta E_i

Počet stupňů volnosti	Smirnov Mínus	(p-value)	Smirnov Plus	(p-value)
2L	0.00001	(0.999991)	0.09034	(0.000000)
2L – 1	0.00008	(0.999836)	0.03658	(0.000000)
2L – 2	0.02328	(0.000030)	0.00083	(0.986266)
2L – 3	0.07911	(0.000000)	0.00004	(0.999939)

Vanstoneova varianta E_i

Počet stupňů volnosti	Smirnov Mínus	(p-value)	Smirnov Plus	(p-value)
2L	0.00001	(0.999991)	0.09042	(0.000000)
2L – 1	0.00008	(0.999836)	0.03657	(0.000000)
2L – 2	0.02331	(0.000029)	0.00083	(0.986266)
2L – 3	0.07922	(0.000000)	0.00004	(0.999939)

pro velikost 64 KB bylo zvoleno L = 14.

B. Balík (10000 posloupností)

Maurerova varianta E_i

Počet stupňů volnosti	Smirnov Mínus	(p-value)	Smirnov Plus	(p-value)
2L	0.00017	(0.999271)	0.08359	(0.000000)
2L – 1	0.00338	(0.793948)	0.03196	(0.000000)
2L – 2	0.02917	(0.000000)	0.00001	(0.999988)
2L – 3	0.08235	(0.000000)	0.00001	(0.999988)

Vanstoneova varianta E_i

Počet stupňů volnosti	Smirnov Mínus	(p-value)	Smirnov Plus	(p-value)
2L	0.00017	(0.999271)	0.08373	(0.000000)
2L – 1	0.00341	(0.790379)	0.03194	(0.000000)
2L – 2	0.02921	(0.000000)	0.00001	(0.999988)
2L – 3	0.08241	(0.000000)	0.00001	(0.999988)

pro velikost 100 KB bylo zvoleno L = 15.

Co lze vyčíst ze získaných výsledků?

1. Varianty předpokládaných četností E_i , se opravdu na finálních hodnotách p-value projevily nepatrně.
2. Výsledky pro oba balíky jsou vzhledem k hodnotě Q konzistentní, a tedy získané výsledky jsou odrazem vlastností testu nikoliv konkrétních dat.
3. Výsledky testů ohodnocených p-value 0.000000 (výstup byl zaokrouhlen na 6 desetinných míst) drasticky zamítají hypotézu náhodnosti (což evidentně není pravda).
4. Překročení statistiky Smirnov Plus lze interpretovat např. tak, že test založený na statistice S se chová příliš „jemně“ – zamítá hypotézu významně méně často, než-li by odpovídalo zvolené hladině významnosti. Tak se například bude chovat test který se asymptoticky řídí rozdělením chí-kvadrát o Q stupních volnosti, ale kritické hodnoty budou brány pro W > Q stupňů volnosti. Při překročení statistiky Smirnov Mínus je tomu právě naopak. Tato tvrzení pochopitelně platí za předpokladu, že testované posloupnosti jsou kvalitní – což je náš případ.
5. Přestože runs test zamítl hypotézu náhodnosti ve všech případech, lze z hodnot statistik vypozorovat, že relativně nejpřijatelnější výsledky jsou pro hodnotu Q = 2L – 2 (Vanstoneova varianta). Hodnoty pro Q = 2L jsou podstatně horší. Rozdělení statistiky S je zřejmě pro běžné velikosti testovaných souborů značně odchýleno od rozdělení chí-kvadrát.
6. Při pohledu na výsledkové tabulky může čtenáře oprávněně napadnout, že při výpočtech se mohly uplatnit numerické chyby např. při výpočtech hodnot distribučních funkcí. Této oblasti věnoval autor mimořádnou pozornost, a zcela postačuje, pokud si uvědomíme, že úplně stejné numerické procedury byly použity i v dalších testech, které souhlasně potvrdily hypotézu náhodnosti (včetně runs testu podle varianty V2 !).

Závěr:

Je vidět, že informace i od renomovaných autorů je potřeba prověřovat. Popis runs testu v práci Maurera [1] je nepochybně chybný. Praktické experimenty prokázaly, že použití této varianty runs testu i s parametry podle [2] může vést k chybnému závěru o kvalitě produkce daného RNG, a to i při velkých objemech testovaných dat (balík B měl mohutnost 1 GB).

Jako nejvhodnější variantu testu sérií lze proto doporučit variantu V2 (testování počtu sérií podle délky série, bez ohledu na „barvu“).

Poděkování:

Autor děkuje panu RNDr. Stanislavu Bajerovi za upozornění, které vedlo k sepsání tohoto článku.

LITERATURA

[1] Maurer, U.M.: "A Universal Statistical Test for Random Bit Generators“, Journal of Cryptology, vol. 5, no. 2, 1992, pp. 89 – 105

[2] Menezes,A. J., Oorschot,P.C.,Vanstone,S.A.: "Handbook of Applied Cryptography", CRC Press, 1997, p. 182

[3] Ruhkin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S.: “A Statistical Test Suite For Random And Pseudorandom Number Generatoes For Cryptographic Applications“, NIST Special Publication 800 – 22 (with revisions dated May 15, 2001)

[4] FIPS 140 – 1 – Security Requirements for Cryptographic Modules
[5] FIPS 140 – 2 – Security Requirements for Cryptographic Modules
[6] Marsaglia,G.: “DIEHARD“ geo@stat.fsu.edu
[7] Tesař, P.: “Generátory náhodných bitů“, Seminář Vojenská kryptografie III, Praha, 2000
[8] Coron, J-S.: "On The Security Of Random Sources", Technical Report IT02-1998, GEMPLUS Corporate Product R&D Division
[9] Knuth, D.E.: "The art of computer programming - Volume 2", 1969, Addison-Wesley Publishing Company

C. Velikonoční kryptologie - 3.-4. duben 2002, Brno

Informace o chystané akci získáte na adrese www.ecom-monitor.cz/velikonoce .
Hlavní téma tohoto workshopu je „Stanovení míry kryptografické bezpečnosti a přijatelná rizika kryptografické bezpečnosti“.

Zasílání příspěvků
Preferujeme elektronické podání příspěvků.
E-mail: Vaclav.Matyas@ecom-monitor.cz
Předmět: "VKB 2002"

Důležitá data
Podání rozšířených abstraktů: 20. února 2002
Oznámení o přijetí/odmítnutí: 4. března 2002
Pracovní verze příspěvků: 18. března 2002
Workshop: 3. - 4. dubna 2002

D. Termimologie

(se svolením Dr.Klímy převzato z konference security@underground)

Od: Klíma Vlastimil [vlastimil.klima@i.cz]
Odesláno: 12. února 2002 11:57
Komu: security@underground.cz
Předmět: terminologie

Vsiml jsem si, ze se tu obcas pouzivaji nespravne terminy. Bojuji proti nim uz pres deset let a zatim slavim jen drobne uspechy. Dokonce i v me materske firme se stale jeste tyto nespravne terminy pouzivaji.
Terminologii jsem konzultoval pouze s Ustavem pro jazyk cesky (nevim jak je to ve slovenstine). Takze :

spravne : **autentizace**
spatne: autentifikace, autentikace,

spravne: **sifrovani, desifrovani, zasifrovani**
spatne: kryptovani, enkrypce, zakryptovat, odkryptovat, zakryptovane, kryptovat, dekryptovat, dekrypce, dekryptace,...
(poznamka: docela me prekvapilo, ze slovo odsifrovani sice není spatne, ale slovo desifrovani prevazuje v pomeru 305:1)

spravne (pristroj na sifrovani): **sifrator**
zridka - zatim nezavedeno: sifrovac

spravne (clovek, ktery obsluhuje sifrator): sifrer (pozn. dlouhe e) nebo sifrant
spatne: krypter

to, co je uvedeno jako spatne, je skutecne cesky spatne, je to proste chyba

dalsi poznamka: casto se zamenuje take *kodovani, dekodovani, zakodovani* za vyznamove odlisne *sifrovani, odsifrovani a zasifrovani*, jiste ze na urovni obecne cestiny (v romanu) je mozne napsat, ze něco bylo zakodovano, jakmile se ale jedna o odborny text, slova kodovani a sifrovani znamenaji diametralne neco jineho a nemela by se povazovat za synonyma

kdyz ministr vnitra (Ruml) rekl, ze v pripade ztraceneho zpravodajskeho notebooku se nemusime obavat uniku utajovanych informaci, protoze tam byla zakodovana, bylo to dost usmevne

bohuzel i v odbornych kruzich se bohuzel dost "kryptuje", protoze ono to vypada, ze se tam neco deje, zatimco "sifrovani" neni tak exoticke tahle hantyrka vyplyva ze dvou veci: bud z lenosti neboz nevedomosti, kdo "kryptuje" a "autentifikuje", necht si vybere, do ktere skupiny patri, v kazdem pripade je to cesky spatne

na druhou stranu uznavam a sam tyhle prohresky pouzivam v jinych oblastech nez je kryptologie, ze podobna hantyrka usnadnuje zivot a ze by clovek nekdy mohl vypadat skrobene, kdyz bude pouzivat spravny termin, v kazdem pripade je o tom ale dobre vedet a v kruhu odborniku se vyjadrovat spravne
Vlastimil Klima

E. Letem šifrovým světem

1) Zpráva o ochraně osobních údajů při používání čipových karet

(ÚOOÚ informuje, bulletin 1/2002)

Na internetových stránkách Rady Evropy na adrese www.legal.coe.int./dataprotection byla k veřejné diskusi publikována „Zpráva o ochraně osobních údajů při používání čipových karet“, připravená předsedou Úřadu pro ochranu osobních údajů RNDr. Karlem Neuwirtem, který je členem vedení projektové skupiny (CJ-PD) zabývající se v RE problematikou ochrany osobních údajů.

V úvodu zprávy je fenomén čipových karet konfrontován s fenoménem „sítě“, reprezentované především Internetem. Čipové karty jsou zde dále představeny jako nástroj pro zvýšení bezpečnosti dat v rámci off-line spojení.

Ve druhé části, věnované technickým hlediskům, jsou nejprve definovány jednotlivé kategorie čipových karet, dále je zde nástin historie karet a přehled použitelných technologií.

Třetí část zprávy je věnována hlediskům právním. Zde jsou jednotlivé body zaměřeny na přijetí principů Úmluvy rady Evropy č. 108 a požadavky na národní legislativu jednotlivých zemí.

Publikovaná zpráva bude doplněna o zásady použití čipových karet s ohledem na ochranu osobních dat. Tyto zásady (Guiding Principles) byly schváleny koordinačním výborem CJ-PD, avšak Rada Evropy je zveřejní teprve po schválení na plenárním zasedání, které se uskuteční až v říjnu 2002.

2) Certifikační autorita na Úřadě pro ochranu osobních údajů

(Mgr. Vladimír Sudzina)

Na Úřadě pro ochranu osobních údajů (ÚOOÚ) vzniká v současné době vlastní certifikační systém. Celkově se skládá z pěti certifikačních autorit (typu standalone a enterprise), které tvoří tři nezávislé systémy.

První systém bude sloužit pro úkoly, které pro ÚOOÚ vyplývají ze zákona o elektronickém podpisu (Zákon č.227/2000 Sb., §10 odst. 7, § 13 odst. 2, …).

Druhý systém tvoří certifikační autorita pro vydávání certifikátů zaměstnancům ÚOOÚ pro vnitřní komunikaci a potřeby úřadu.

Třetím systémem je testovací, školící a předváděcí linka. Jde o lokální síť, která se skládá z DNS serveru (Windows 2000 server) a MS Exchange serveru (Windows 2000 server). Další tři počítače jsou uživatelské stanice. Na první je nainstalován systém Windows 2000 a prohlížeče MS Explorer 5.0, Netscape 6.2, Opera 6.0. Druhá stanice je postavená na Windows XP s Office XP a MS Explorerem CZ 6.0. Na třetí stanici je Linux Red Hat 7.1 CZ, prohlížeč Opera 5.0 a Nestcape Navigator 4.77.

Certifikační autorita ÚOOÚ byla postavena podle topologie navržené Mgr. Pavlem Vondruškou. Systém byl instalován ve spolupráci s KSI MFF UK Praha (RNDr. Vojtěch Jákl, CSc., RNDr. Antonín Beneš, PhD.). Správcem certifikační autority je Mgr. Vladimír Sudzina (vladimir.sudzina@uoou.cz) a Jakub Lukáš (jakub.lukas@uoou.cz).

3) Pro zájemce o legislativně právní otázky elektronického podpisu doporučuji nově zřízený web mého kolegy Bc.Honzy Hobzy http://www.volny.cz/honzahobza . V časopise Veřejná správa můžete od března sledovat jím připravený 15-ti dílný seriál o elektronickém podpisu.

4) Užitečný software pro čtenáře Crypto-Worldu

Software viz příloha k tomuto e-zinu.

Hašák ver. 0,90

Detaily viz. dokumentace a uživatelská příručka
Autor Libor Tvrdík (14.2. 2002)
hashe@centrum.cz
http://hashe.zde.cz/

Program určen potřebu Crypto-Worldu (www.mujweb.cz/veda/gcucmp) **a jeho čtenářů.**

Hašák je aplikace určená pro výpočet otisků dat pomocí hashovacích funkcí (SHA-1, MD5 a MD4). Komunikace s uživatelem probíhá v konzolovém prostředí - řízena je parametry. Umožněný je přímý výpočet z řetězce, nebo čtení dat ze souboru, to je prováděno bufferem o velikosti 4 096 bytů. Vlastní výpis je prováděn na obrazovku a pokud je uveden správný parametr tak také do sou-boru. Programový kód je vytvořen v jazyku Java.

Požadavky programu: Hašák je přeložen pro 32-bitovou Windows platformu. V systémech Win98/Me, WinNT4.0 a W2k je možné spouštět program bez omezení. Pro Win95 a WinXP je nutná instalace JavaRunTime (http://java.sun.com/j2se/1.3/jre/ cca 9 MB) která je distribuována zdarma. V případě zájmu je možné získat nativní formát (class), který lze spustit na jakémkoliv stroji s nainstalovanou podporou Javy.

Licenční podmíky:
Veřejné šíření (například CD, sharwarové banky, …) je podmíněno souhlasem autora !

O čem jsme psali v únoru roku 2000 a 2001

Crypto-World 2/2000

Crypto-World 2/2001

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

Pokud se zajímáte pouze o sešit Crypto-World, můžete jej najít na lépe dostupné adrese:

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