

Výklad k příloze č. 2 vyhlášky č. 366/2001 Sb.

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

Výklad k příloze č. 2 vyhlášky č. 366/2001 Sb., 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 *Algorithms and Parameters for Secure Electronic Signatures* [20] 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- F_2^m	qMinLen=160 r0Min= 10^4 MinClass=200	ecgen1	-	SHA1

Každému podpisovému schématu je jednoznačně přiřazen třiciferný 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] [12] [11] [7] [14]
 - ECDSA- F_2^m [9] [12] [11] [7] [14]

Dokument [21] schvaluje navíc použití algoritmů EGDSA- F_p , resp. EGDSA- F_2^m , které jsou v podstatě variantou algoritmů ECDSA- F_p , resp. ECDSA- F_2^m s pozměněnou vytvářející rovnicí podpisu a metodou ověřování. Požadavky na ně kladené jsou stejné jako v případě algoritmů ECDSA- F_p , resp. ECDSA- F_2^m (bližší informace viz. [14]).

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 diskretních logaritmů. Dlouhodobější analýza týkající se tohoto tématu je předmětem např. [21].

2.1 RSA

Jedná se o všeobecně známý algoritmus Rivest-Shamir-Adleman, popsáný 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 $3 \leq e < n-1$ a $\text{nsd}(e, \text{nsn}(p-1, q-1))=1$. 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]
- EMSA-PSS [6, kap. 9.1]

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 vzhledem k útoku D. Bleichenbachera¹ doporučuje používat metody uvedené v [10], kterou se pozměňují postupy definované ve FIPS 186-2 [9, App. 3.1, resp. App. 3.2].

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 diskretního 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 .

Tyto parametry musí splňovat následující podmínky:

- počet tříd maximálního řádu okruhu endomorfismů křivky E musí být alespoň 200 (MinClass),
- hodnota $r_0 = \min(r; q \text{ dělí } p^r - 1)$ 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,

¹ <http://www.lucent.com/press/0201/010205.bla.html>.

- 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 [12]. 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 $qMinLen \geq 160$ bitů (viz. [12]). 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 diskretního 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 $r_0 = \min(r; q \text{ dělí } 2^{mr} - 1)$ 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-F2m

Prvočíslo m , které určuje těleso F_2^m , je třeba volit pevně podle [12]. Eliptickou křivku nad F_2^m je třeba zvolit tak, aby byl její řád dělitelný prvočíslem q délky alespoň $qMinLen \geq 160$ (viz. [12]). 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 \geq 128
4.02	dsagen1	Dsa	trueran nebo pseuran	EntropyBits \geq 128 nebo SeedLen \geq 128
4.03	ecgen1	ecdsa-F _p	trueran nebo pseuran	EntropyBits \geq 128 nebo SeedLen \geq 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][10]

Standard [9] (Digital Signature Standard) navrhuje dva druhy generování pseudonáhodných čísel pro získání veřejných parametrů, tajného a dočasněho 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). Z tohoto standardu a z doporučení iniciativy EESSI se vycházelo při tvorbě vyhlášky č. 366/2001 Sb. a jejích příloh. V současné době se však metody uvedené v [9, App. 3.1, resp. App. 3.2] vzhledem k útoku D. Bleichenbachera nepovažují za bezpečné a doporučuje se použít jejich pozměněné verze uvedené v [10]. Dokument [20] rovněž doporučuje generátory cr_to_X9.30_x, resp. cr_to_X9.30_k, které jsou podrobněji popsány v [18, B.2.1, resp. B.2.2].

Metody generování náhodných čísel

Označení náhodného generátoru	Používané jméno	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 současné 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 v2.1: RSA Cryptography Standard," June 2002.
- [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] National Institute of Standards and Technology, "NIST: FIPS Publication 186-2: Digital Signature Standard, Change Notice 1," October 2001.
- [11] The Institute of Electrical and Electronics Engineers, Inc, "Standard Specifications for Public-Key Cryptography," IEEE P1363, 2000.
- [12] American National Standards Institute, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)," ANSI X9.62-1998, 1998.
- [13] 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.
- [14] 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.
- [15] 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.
- [16] Eastlake, D., et al., "Randomness Recommendations for Security," Internet Request for Comment (RFC) 1750, December 1994.
- [17] American National Standards Institute, "Financial Institution Key Management (wholesale)," ANSI X9.17-1985, 1985.
- [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 Journal on Computing, Vol. 4, No. 13, pp. 850-863, 1984