Digitální podepisování pomocí asymetrické kryptografie

Ondřej Soroka

11. dubna 2011

- Trocha historie
- Digitální podpis
- Asymetrické metody
- Podpisová schémata

Historie

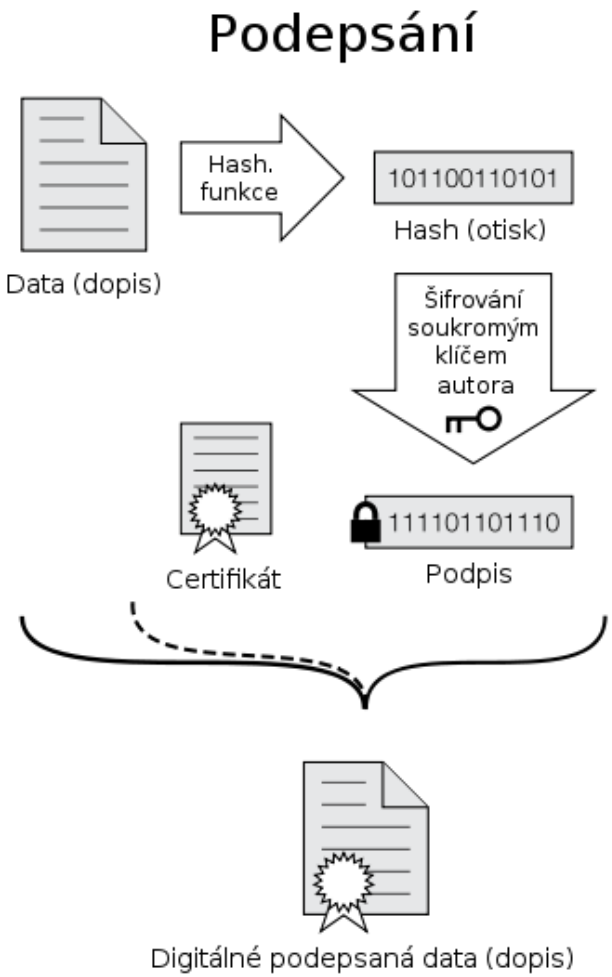
- 1976 Whitfield Diffie a Martin Hellman první teoretický popis podpisového schématu
- 1978 RSA první podpisové schéma
- 1984 ElGamal předchůdce dnes používaných DSA a ECDSA
- 1989 Lotus Notes první komerčně rozšířený softwarový balík, který nabízel digitální podpis(využíval RSA)
- 1991 DSA (Digital Signature Algorithm) součástí návrhu standardu DSS
- 1992 navrhnut ECDSA využívá přenesení problému diskrétního logaritmu na eliptické křívky

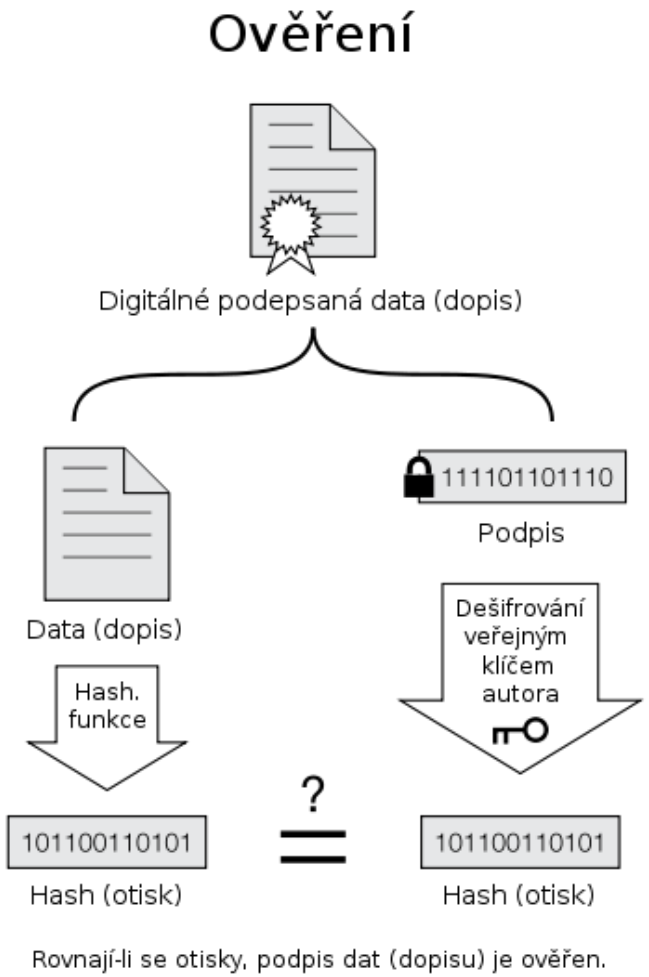
Digitální podpis

1. Identifikace - digitální podpis musí odpovídat konkrétní entitě, která podpis vytvořila
2. Autentizace - ověření toho, že podepsaný je skutečně tím za koho se vydává.
3. Integrita - zajištění toho, že zpráva nebyla na cestě od odesílatele změněna
4. Nepopiratelnost

Asymetrické šifrování

- vytvoření klíčů soukromý klíč (podepisující) veřejný klíč (ověřující)
- podpisový algoritmus, pomocí zprávy a soukromého klíče vznikne digitální podpis
- ověřovací algoritmus, z věřejného klíče, zprávy a podpisu ověří správnost podpisu


Podepsání
Hash. funkce
101100110101
Hash (otisk)
Data (dopis)
Šifrování soukromým klíčem autora
Certifikát
111101101110
Podpis
Digitálné podepsaná data (dopis)


Ověření
Digitálné podepsaná data (dopis)
111101101110
Podpis
Data (dopis)
Dešifrování veřejným klíčem autora
Hash. funkce
?
101100110101
Hash (otisk)
101100110101
Hash (otisk)
Rovnají-li se otisky, podpis dat (dopisu) je ověřen.

RSA

- viz předešlá přednáška :)

RSA podpis

- Veřejný klíč se složí z dvojice (N, e) a soukromý klíč z dvojice (N, d).
- Podpis zprávy je proveden operací $s_M = h(M)^d \mod N$, je nutné nejprve výsledek hashovací funkce upravit na patřičnou délku k tomu slouží doplnění Odesílatel používá svůj soukromý klíč (N, d).
- Při ověření podpisu zprávy se nejprve spočítá hodnota hashe přijaté zprávy $h(M)$. Dále je proveden výpočet $s_M^e \mod N$. Pokud se výsledky obou operací rovnají je podpis považován za platný.
- Standardy RSA
  1. ANSI X9.62
  2. PKCS #1 v2.1

ElGamal

- Základem metody je úloha diskrétního logaritmu modulo p.
- Momentálně se nepoužívá, je nahrazen svými nástupci DSA a ECDSA.

ElGamal

Generování klíčů

- Tajný klíč je zvolen náhodně $1 < x < p - 1$.
- Vypočítá se $y = g^x \mod p$
- Veřejný klíč je pak volen (p, g, y)

ElGamal

Vytvoření podpisu

Vygenerujeme podpis zprávy m za pomoci hashovaci funkce H.

- Náhodně zvolíme k $1 < k < p - 1$ a $gcd(k, p - 1) = 1$.
- $r \equiv g^k \mod p$
- $s \equiv (H(m) - xr) k^{-1} \mod p - 1$
- Pokud vyjde $s = 0$ vše opakujeme.

Dvojice (r, s) je pak digitálním podpisem zprávy m.

ElGamal

Ověření podpisu

Podpis (r, s) přiložený ke zprávě m ověříme:

- $0 < r < p$ a $0 < s < p - 1$-byli počítány modulo p resp $p - 1$
- $g^{H(m)} \equiv y^r r^s \mod p$

DSA

1991 NIST(The National Institute of Standards and Technology) cíle DSS(Digital Signature Standard):

- Použití asymetrických kryptografických technik pro zajištění integrity a autentizace podepsané osoby.
- Snadná implementace jak v hardware, tak v software. Možnost exportu mimo USA (nikoliv ovšem volného export reguluje Ministerstvo obchodu).
- Volná použitelnost kýmkoliv. Míní se tím absence použití patentem chráněných technologií, jejichž použití vyžaduje platbu licenčních poplatků.

parametry DSA

- Hashovací funkce - SHA-1, SHA-2
- Volíme délky klíčů L a N, kde L je násobkem 64 s dopručenými délkami 2048 a 3072(původně 512-1024).
- Volíme prvočíslo q délky N menší než je výstup Hashovací funkce.
- Volíme prvočíslo p délky L takové, že $(p-1)$ je násobkem q. Tento parametr určuje budoucí velikost soukromého klíče.
- Nalezneme g číslo z otevřeného intervalu $(2, p-2)$, které má v Z_p^* řád q.

DSA

Generování klíčů

- Tajný klíč je zvolen náhodně $1 < x < q$.
- Vypočítá se $y = g^x \mod p$
- Veřejný klíč je pak volen (p, q, g, y)

Vytvoření podpisu

Vytváření podpisu je skoro totožné s ElGamalovým algoritmem.

- Náhodně zvolíme k $1 < k < q$.
- $r \equiv \left(g^k \mod p\right) \mod q$
- $s \equiv \left(H(m) - xr\right) k^{-1} \mod q$

k je tzv. klíč zprávy nebo nonce(number used once) generuje se pro každou zprávu nové, a je nutné ho utajit.
Dvojice (r, s) je pak digitálním podpisem zprávy m.

Ověření podpisu

- Přijatá zpráva je opět nějaká trojice (M', r', p'). Příjemce zprávy nejprve ověří, zda $0 < r' < q$ a $0 < s' < q$. Pokud tomu tak není, je podpis zprávy odmítnut.
- Příjemce dále vypočítá
  - $w = (s')^{-1} \mod q$
  - $u_1 = h(M')w \mod q$
  - $u_2 = r'.w \mod q$
  - $v = (g^{u_1}.y^{u_1} \mod p) \mod q$

Pokud platí, že $v = r'$, pak je podpis platný.

ECDSA

- Elliptic Curve Digital Signature Algorithm (ECDSA) na rozdíl od DSA nevyužívá konečná tělesa Z_p, ale konečná tělesa dána eliptickými křívkami na niž se
- Velikost klíče při zachování stejné úrovně bezpečnosti je menší než u DSA a RSA(160 bitů odpovídá 1024 bitům).

V ČR odovozené z EU Zaručený elektronický podpis splňuje:

1. Je jednoznačně spojen s podepisující osobou.
2. Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě.
3. Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.
4. Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

- *Certifikátem* datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,
- *Kvalifikovaný certifikát* je certifikát, který má náležitosti podle § 12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb.

Zdroje:

1. http://crypto.hyperlink.cz/cryptoprax.htm
2. Petr Svoboda, Systémy elektronických podpisů, diplomová práce, MUNI
3. http://www.wikipedia.org
4. http://business.center.cz/business/pravo/zakony/epodpis/