Digitální podepisování pomocí asymetrické kryptografie

Jan Máca, FJFI ČVUT v Praze

26. března 2012

Obsah

Historie

- 1976 – Diffie a Hellman teoreticky popsali možnosti
- 1978 – Rivest, Shamir, Adleman – algoritmus RSA
- 1988 – Goldwasser, Micali, Rivest – teoretické odvození bezpečnostích nároků na digitální podpisy
- 1989 – Lotus Notes 1.0 – první široce rozšířený software pro podepisování, používal RSA
- 1991 – DSA – standart federální vlády USA pro digitální podpis, vychází z metody ElGamal

Použití digitálního podpisu

- Autentizace odesilatele
- Integrita zprávy
- Nepopiratelnost podpisu

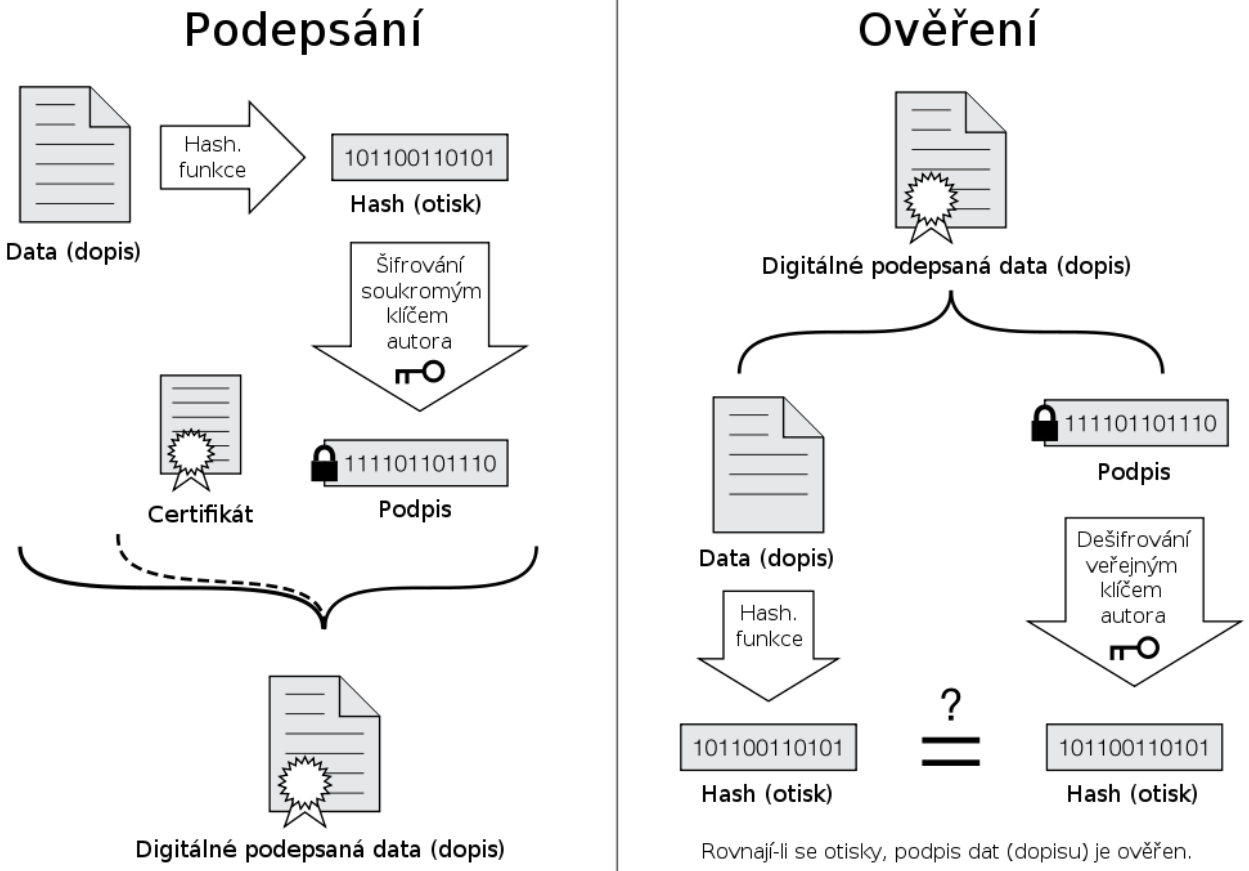
Útoky

- key-only – útočník zná jen veřejný klíč
- known message – útočník zná podpisy k různým zprávám, které si sám nevybral
- adaptive chosen message – útočník se dozví podpisy zpráv, které sám vybral

Výsledky útoků

- total break – získání podpisového klíče
- universal forgery – schopnost falšovat klíče k libovolným zprávám
- selective forgery – schopnost podepisovat zprávy dle protivníkova výběru
- existencial forgery – získání podpisu ke zprávě, kterou protivník ještě neuměl podepsat

Digitální podpis



Obrázek: Postup podepisování a ověření podpisu

Certifikační autority

- subjekt, který vydává digitální certifikáty
- usnadňuje tvorbu veřejných klíčů a jejich bezpečné předávání
- CSCA – česká národní certifikační agentura
- CVCA – česká národní verifikační autorita
- na starosti Ministerstvo vnitra

Metoda RSA

- veřejný klíč (N, e), soukromý klíč (N, d)
- podepsání

$$s = h(M)^d \mod N$$

- ověření podpisu

$$h(M) = s^e \mod N$$

Rizika metody RSA

- mějme zprávu m, kterou chceme podepsat a veřejný klíč (N, e)
- nechť máme náhodné zprávy splňující

$$m_2 := \left[\frac{m}{m_1} \bmod N \right]$$

- k těmto zprávám získáme podpisy s_1, s_2

Rizika metody RSA

- zfalšování podpisu – tvrdíme, že $s = s_1 \cdot s_2$ je platný podpis pro m

$$s^e = (s_1 \cdot s)^e = \left(m_1^d \cdot m_2^d\right)^e = m_1^{ed} \cdot m_2^{ed} = m_1 m_2 = m \bmod N$$

Metoda ElGamal

- soukromý klíč (p, g, x)

$$\text{Náhodné } x, \text{tak, že } 1 < x < p - 1$$

- veřejný klíč (p, g, y)

$$y = g^x \bmod p$$

Podpis a jeho ověření

- podepsání

$$r = g^k \bmod p, \text{ kde } \gcd(k, p-1) = 1$$

$$s = (h(M) - xr)\, k^{-1} \bmod (p-1)$$

- ověření podpisu

$$h(M) = xr + sk \bmod (p-1)$$

$$g^{h(M)} = y^r r^s \bmod p$$

Hlavní rizika ElGamal

- nutno volit různá k pro každý podpis a nenechat uniknout informace
- potřeba hlídat kolize u hashovací funkce modulo $p - 1$

Metoda DSA

- standart federální vlády USA pro digitální podepisování (DSS)
- tvůrce David W. Kravitz

Veřejné parametry

- hashovací funkce SHA-1, resp. SHA-2
- délky klíčů L a M, podle FIPS 186-3 dvojice (1024,160), (2048,224), (2048,256), (3072,256)
- vyber N-bitové prvočíslo q, N musí být menší než výstup hashové funkce
- vyber L-bitové prvočíslo p, tak že $q \,|\, p-1$
- číslo g, tak že g má multiplikativní řád q modulo p

$$g = h^{(p-1)q} \bmod p, \text{ kde } 1 < h < p-1$$

Generování klíčů

- soukromý klíč x

$$0 < x < q$$

- veřejný klíč (p, q, g, y)

$$y = g^x \bmod p$$

Podepisování

- vybere se náhodně $0 < k < q$ pro danou zprávu
- podpis

$$r = \left(g^k \bmod p\right) \bmod q$$

$$s = \left(k^{-1}\left(h(M) - xr\right)\right) \bmod q$$

Ověření podpisu

- musí platit $0 < r < q$ a $0 < s < q$, jinak je podpis zamítnut
- jinak se zpočítá

$$w = s^{-1} \bmod q$$

$$u1 = (h(M)w) \bmod q$$

$$u2 = (rw) \bmod q$$

$$v = \left(\left(g^{u1}y^{u2}\right) \bmod p\right) \bmod q$$

- podpis přijat, pokud $v = r$

Metoda ECDSA

- využívá podobný princip jako DSA, ale pracuje nad eliptickými křivkami, místo konečnými tělesy
- generované klíče pro stejně dlouhé zprávy jsou kratší

Děkuji za pozornost.

Zdroje

- Katz J., Lindell Y.: Introduction to Modern Cryptography.
- www.wikipedia.org
- www.mvcr.cz