Digitální podepisování

pomocí asymetrické kryptografie

Matěj Klíma

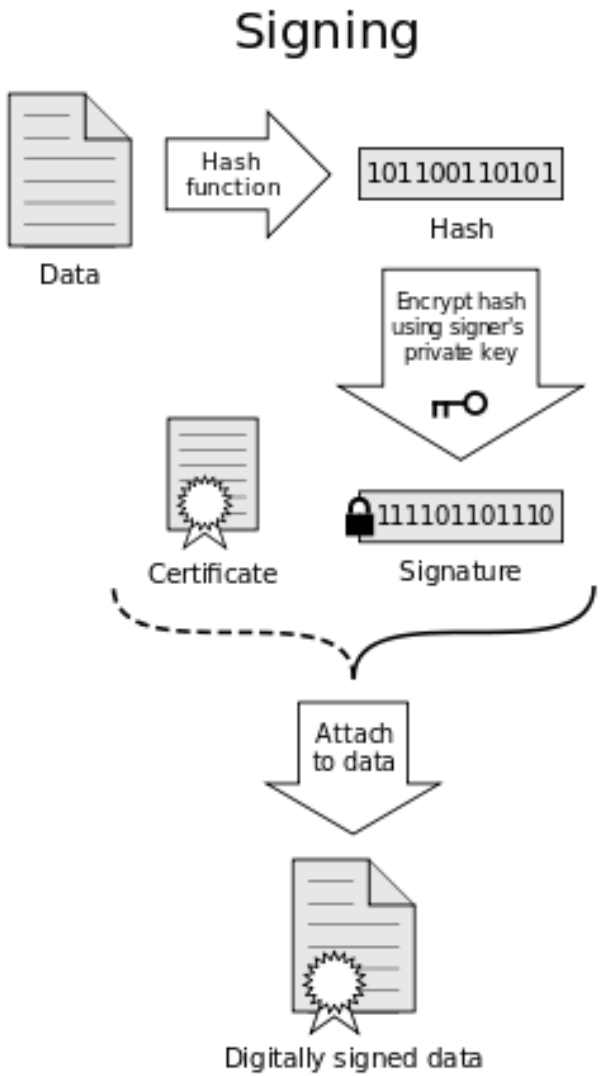
ČVUT v Praze
FJFI
Katedra fyzikální elektroniky

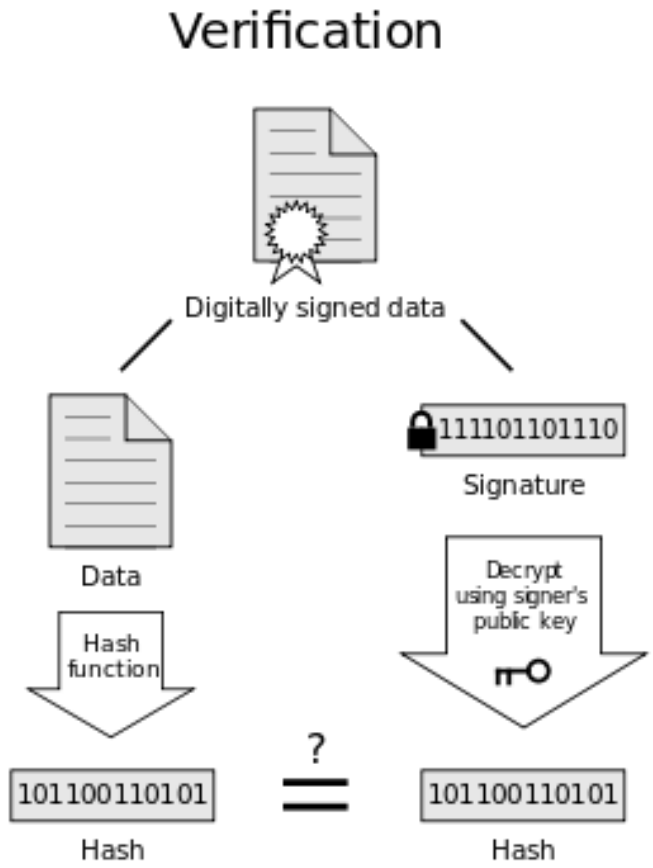
15. dubna 2013

Digitální podpis

- Postup, umožňující ověřit autenticitu a integritu digitální zprávy.
- Symetrické šifry nejsou příliš vhodné
  - Nutnost držet klíč v tajnosti.
  - Případně možnost využití třetí strany (arbitra).
  - Sdílený soukromý klíč nezaručí autenticitu odesílatele.
- Používá se obvykle kombinace asymetrických šifer a jednosměrných hashovacích funkcí.

Základní schéma





RSA

Vytvoření klíče:

$$n = pq,\ \phi(n) = (p-1)(q-1)$$

$$1 < e < \phi(n),\ \gcd(e, \phi(n)) = 1$$

$$de \equiv 1 \mod \phi(n)$$

n, e ... veřejný klíč, d ... soukromý klíč, p, q ... velká prvočísla

Šifrování a dešifrování:

$$c_i = m_i^e \bmod n,\ m_i < n$$

$$m_i = c_i^d \bmod n$$

m_i ... blok zprávy, c_i ... blok šifrového textu

Podepisování pomocí RSA

1. Vygenerujeme hash naší zprávy (MD-5, SHA-1...).
2. Hash zašifrujeme pomocí **soukromého** klíče - digitální podpis.
3. Spolu s dokumentem zašleme podpis a veřejný klíč (a hashovací funkci).
4. Příjemce dešifruje podpis pomocí **veřejného** klíče.
5. Pokud je tato hodnota stejná jako hash zprávy, má příjemce jistotu, že jsme držiteli odpovídajícího soukromého klíče.

Podepisování pomocí RSA

- RSA se pro podepisování používá obráceně než k šifrování zpráv.
- Je součástí standardu ISO/IEC 9796.
- Pro bezpečnost RSA je zásadní dobrý generátor náhodných prvočísel.
- Důležité je nepoužívat stejný klíč n (Common Modulus Attack).
- RSA vypršel v USA patent v r. 2000 (RSA Security inc.).

RSA - Chosen Ciphertext Attack

- Podepisovat musíme vždy jen jednosměrnou hash. funkci.
- Při podepisování libovolných zpráv se vystavujeme riziku útoku, např:
  - Útočník vytvoří zprávy m_1, m_2 a m_3 tak, že

$$m_3 = m_1 m_2 \bmod n$$

.

  - Přiměje nás podepsat tyto zprávy soukromým klíčem d.
  - Posléze padělá podpis zprávy m_3, protože

$$m_3^d = (m_1^d \bmod n)(m_2^d \bmod n)$$

Schnorrův algoritmus

- Bezpečnost je založena na obtížnosti řešení diskrétního logaritmu.
- Považován za nejjednodušší algoritmus, jehož bezpečnost byla dokázána pro dokonale náhodnou hashovací funkci.
- Podpis je více než 2x kratší než u RSA / ElGamal.

Diskrétní logaritmus

Nechť a, g, n jsou přirozená čísla, pak nejmenší přirozené číslo μ, pro které platí $a = g^{\mu} \bmod n$ nazýváme (pokud existuje) **diskrétním logaritmem** čísla a o základu g modulo n.

Schnorrův algoritmus

Vytvoření klíče:

$$p, q \text{ prvočísla}, (p-1) \bmod q = 0, a^q \bmod p = 1, a \neq 1$$

$$s < q \text{ náhodné}, v = a^{-s} \bmod p$$

p, q, a, v ... veřejný klíč, s ... soukromý klíč

Podpis:

$$r < q \text{ náhodné}, x = a^r \bmod p \quad \text{... (preprocessing)}$$

$$e = H(M, x), y = (r + se) \bmod q$$

$H(M, x)$ ... hashovací funkce aplikovaná na zprávu doplněnou o x
e, y ... vlastní podpis

Schnorrův algoritmus

Verifikace:

$$x = a^y v^e \bmod p, \text{ ověříme } e = H(M, x)$$

$H(M, x)$ ... hashovací funkce aplikovaná na zprávu doplněnou o x
e, y ... vlastní podpis

DSA

- Algoritmus pouze pro podepisování.
- Vychází ze starších schémat založených na diskrétním logaritmu (Schnorr, ElGamal).
- Vzniká jako konkurence již zavedeného RSA na přelomu 80. a 90.let.
- V r. 1993 je americkým NIST uznán jako standard pro podepisování úředních dokumentů.

DSA - algoritmus

Vytvoření klíče:

- p ... prvočíslo délky 512-1024 bitů
- q ... prvočíslo délky 160 bitů, dělitel $p - 1$
- $g = h^{p-1/q} \mod p$, $h < p - 1$, $g > 1$
- parametry p, q, g mohou být sdíleny skupinou uživatelů
- x ... soukromý klíč, číslo délky 160 bitů, $x < q$
- y ... veřejný klíč, $y = g^x \mod p$

DSA - algoritmus

Podpis:

- k ... náhodné číslo, $k < q$
- $r = (g^k \mod p) \mod q$
- $s = (k^{-1}(H(m) + xr)) \mod q$

$H(m)$ ... hashovací funkce aplikovaná na zprávu

Verifikace:

- $w = s^{-1} \mod q$
- $u_1 = (H(m) * w) \mod q$
- $u_2 = (rw) \mod q$
- $v = ((g^{u_1} * y^{u_2}) \mod p) \mod q$
- Pokud v = r, je podpis ověřen.

DSA

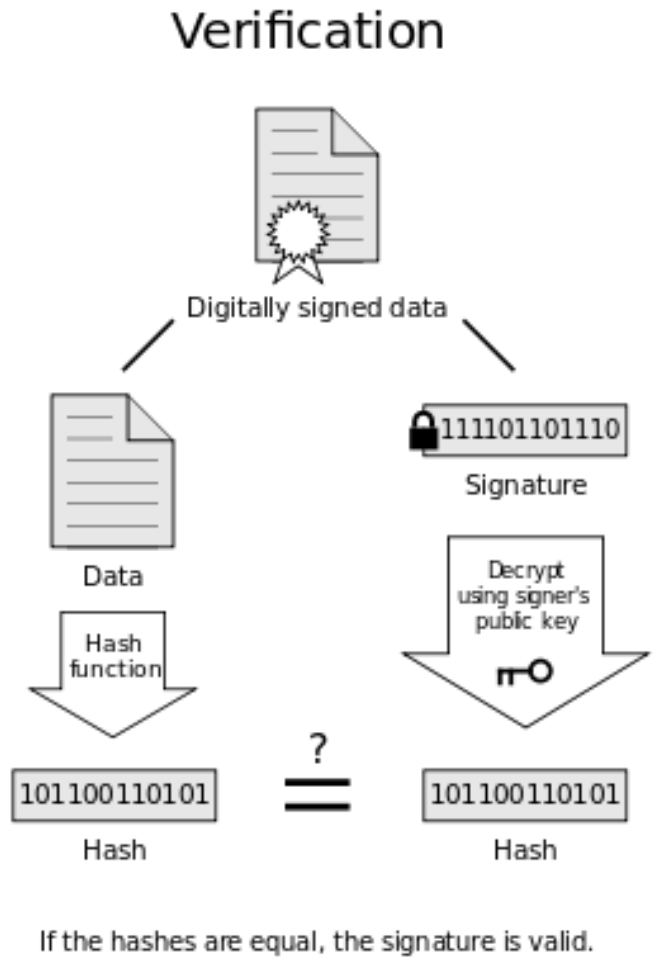
Výhody:

- Zveřejnění čísel p, q nebo jejich generátoru algoritmus příliš neoslabuje.
- Řádově rychlejší podepsání než u RSA.
- Mnoho různých variant a rozšíření.

Kritika:

- Zaváděno v době, kdy RSA už bylo v podstatě standard.
- Vyvíjeno americkou národní bezpečnostní agenturou (NSA).
- Pomalejší ověřování podpisu (nejčastěji prováděná operace).

Přenos důvěry



Public Key Infrastructure

- Veřejný klíč často získáváme od odesílatele zprávy - jak ověřit jeho identitu?
- Nejčastěji se využívají komerční digitální certifikáty - veřejný klíč je podepsaný od autority.
- Toto schéma má několik úrovní - tzv. Chain of Trust.
- Na vrcholu kořenové certifikáty např. v úložištích prohlížečů.

PKI - Web of Trust

- Alternativou je model založený na předávání důvěry mezi uživateli vzájemným podepisováním klíčů.
- Plně decentralizovaný model.
- Více parametrů - požadovaný počet "přátel", maximální hloubka důvěry.
- Je třeba volit kompromis mezi úrovní zabezpečení a rozsahem použití.
- Pomalejší zapojení se do sítě (je třeba aktivně získat podpisy).

Elektronické podpisy

- Používány už od 19.století - telegrafické smlouvy.

> *It makes no difference whether [the telegraph] operator writes the offer or the acceptance in the presence of his principal and by his express direction, with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office.*
>
> *- Precedentní rozsudek nejvyššího soudu v New Hampshire, 1869*

- 80. léta 20. stol - potřeba autentizace faxovaných dokumentů.
- Klasický podpis zde postupně doplňuje digitální.
- V r. 1998 první elektronicky podepsaná mezinárodní dohoda - Irsko a USA.

Digitální podpisy v USA

- Uznání digitálních podpisů při komunikaci se státní správou v 90.letech.
- Digital Signature and Electronic Authentication Law (SEAL) - 1998.
- Electronic Signatures in Global and National Commerce Act (ESIGN) - 2000.
- Government Paperwork Elimination Act (GPEA) - 2003.
- Vývoj od soudního uznání, přes standardizaci až po podporu.
- Jedinec má vždy právo digitální podpisy nepoužívat.

Právní postavení v ČR

- Zejména zákon č. 227/2000 Sb. , o elektronickém podpisu - vychází z evropské direktivy 1999/93/EC.
- Zaručený elektronický podpis - má stejnou platnost jako klasický.
- Kvalifikovaný certifikát - od komerčních organizací s akreditací MV ČR.
- Zákon neobsahuje technické požadavky, norma ČSN odkazuje na odpovídající normy ETSI.
- Soudy vyžadovaly zaslání papírového originálu do 3 dnů, tuto praxi zrušil v r. 2005 ústavní soud.

Datové schránky

- Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů.
- Motivace - e-government a fikce doručení, celosvětově unikátní projekt (což není nutně pozitivní).
- Povinné pro orgány veřejné správy a právnické osoby vedené v obchodním rejstříku.
- Kontroverzní start, provozovatel Česká pošta s.p..
- Přístup přes webové rozhraní `www.mojedatovaschranka.cz`.
- Existuje svobodný klientský software komunikující s API.

TLS/SSL

- Transport Layer Security a jeho předchůdce Secure Sockets Layer.
- Šifrovací protokol aplikační vrstvy, nejčastěji používán jako HTTPS.
- Používá asymetrickou kryptografii pro autentizaci a výměnu klíčů.
- K vlastnímu šifrování zpráv používá symetrické šifry (rychlejší).
- CipherSuite - použitá sada algoritmů, liší se v závislosti na serveru a typu certifikátu.
- K podepisování lze použít RSA, DSA a ECDSA.

PGP/GPG

- Pretty Good Privacy (1991) / open source GNU Privacy Guard (1999)
- Programy pro jednoduché šifrování/podepisování zpráv, především e-mailů.
- Klíče se šifrují pomocí asymetrické šifry, text pomocí symetrické šifry.
- Algoritmy RSA, DSA, GPG navíc ElGamal.

Bitcoin

- Decentralizovaná digitální kryptoměna, snaha o napodobení zlatého standardu.
- Místo účtu vlastníte soukromý klíč (používá se ECDSA).
- Veřejný klíč pak představuje adresu, na kterou lze posílat peníze.
- Transakce jsou ověřovány P2P sítí počítačů (miners), kteří za vynaložený výpočetní výkon získávají nově emitované peníze.
- Momentálně spíše extrémně nestabilní spekulativní nástroj než použitelná měna.
- Celková kapitalizace trhu přes 1 mld. $, značnou část tvoří černý trh.

Zdroje

- Bruce Schneier: Applied Cryptography (zejména algoritmy)
- `http://www.isaacbowman.com/the-history-of-electronic-signature-laws`
- `http://www.mvcr.cz/datove-schranky.aspx`
- Wikipedia
- `http://en.bitcoin.it/wiki/`

Děkuji za pozornost.