Úvod do kryptologie

Digitální podepisování pomocí asymetrické kryptografie

Pavel Novotný, 2010

Obsah prezentace

1. Definice podle zákona
2. Definice dalších pojmů
3. Princip digitálního podpisu
4. Vlastnosti digitálního podpisu
5. Algoritmus DSA

1. Definice podle zákona

Zákon o elektronickém podpisu

- Zákon o elektronickém podpisu č. 227/2000 Sb. a další navazující předpisy
- Definuje za jakých podmínek lze používat elektronické podpisy místo klasických

Zákon o elektronickém podpisu

- Vztahuje se nejen na soukromé subjekty, ale i státní orgány a veřejnou správu
- Upravuje určení certifikačních autorit a autorit časových razítek

Definice dle zákona o elektronickém podpisu

- Elektronický podpis
- Zaručený elektronický podpis
- Digitální podpis
- Kvalifikovaný podpis

Elektronický podpis

„Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.“

Zaručený elektronický podpis

„Zaručeným elektronickým podpisem se rozumí takový elektronický podpis, který splňuje následující požadavky:

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.“

Digitální podpis

„Digitální podpis je zaručený elektronický podpis založený na kryptografické technologii“

Definice dle zákona o elektronickém podpisu

- Elektronický podpis
- Zaručený elektronický podpis
- Digitální podpis
- Kvalifikovaný podpis - EU

Definice dle zákona o elektronickém podpisu

- e-podatelny – adresy, kde daný úřad (instituce) přijímá digitálně podepsané podklady
  - Zaslání správně podepsané zprávy na tuto adresu se považuje za doručení ve smyslu zákona
  - Adresa: posta@<domena_instituce>.cz

2. Definice dalších pojmů

Asymetrické šifrování

- používají se odlišné klíče pro zašifrování a dešifrování
- mnohem pomalejší, než symetrické metody, snaha o zrychlení (viz. PGP nebo Hašovací funkce)
- zastoupení:
  - DH (Diffie-Hellman); RSA;
  - DSS (=digital signature standard) – standardem NIST

Soukromý klíč

- Slouží k vytváření podpisu (jen my můžeme podepsat náš dokument)

Veřejný klíč

- Slouží k ověření autora digitálního podpisu
- Data pro ověření se berou z kvalifikovaného certifikátu

Hašovací funkce (1/3)

- Matematická funkce / algoritmus
- Vytváří otisky textu (obecně libovolných dat)
- Pevná velikost otisku
- Špatná podmíněnost
- Vzor lze jen těžko rekonstruovat
- Malá pravděpodobnost, že 2 zprávy budou mít stejnou hash

Hašovací funkce (2/3)

- Jednosměrnost
  - Vzor -> Otisk
- Bezkolizní
  - X != Y ale platí h(X) = h(Y)

Hašovací funkce (3/3)

- Odvozují se z šifer
  - Např.

    bloková šifra DN -> hašovací funkce HDN

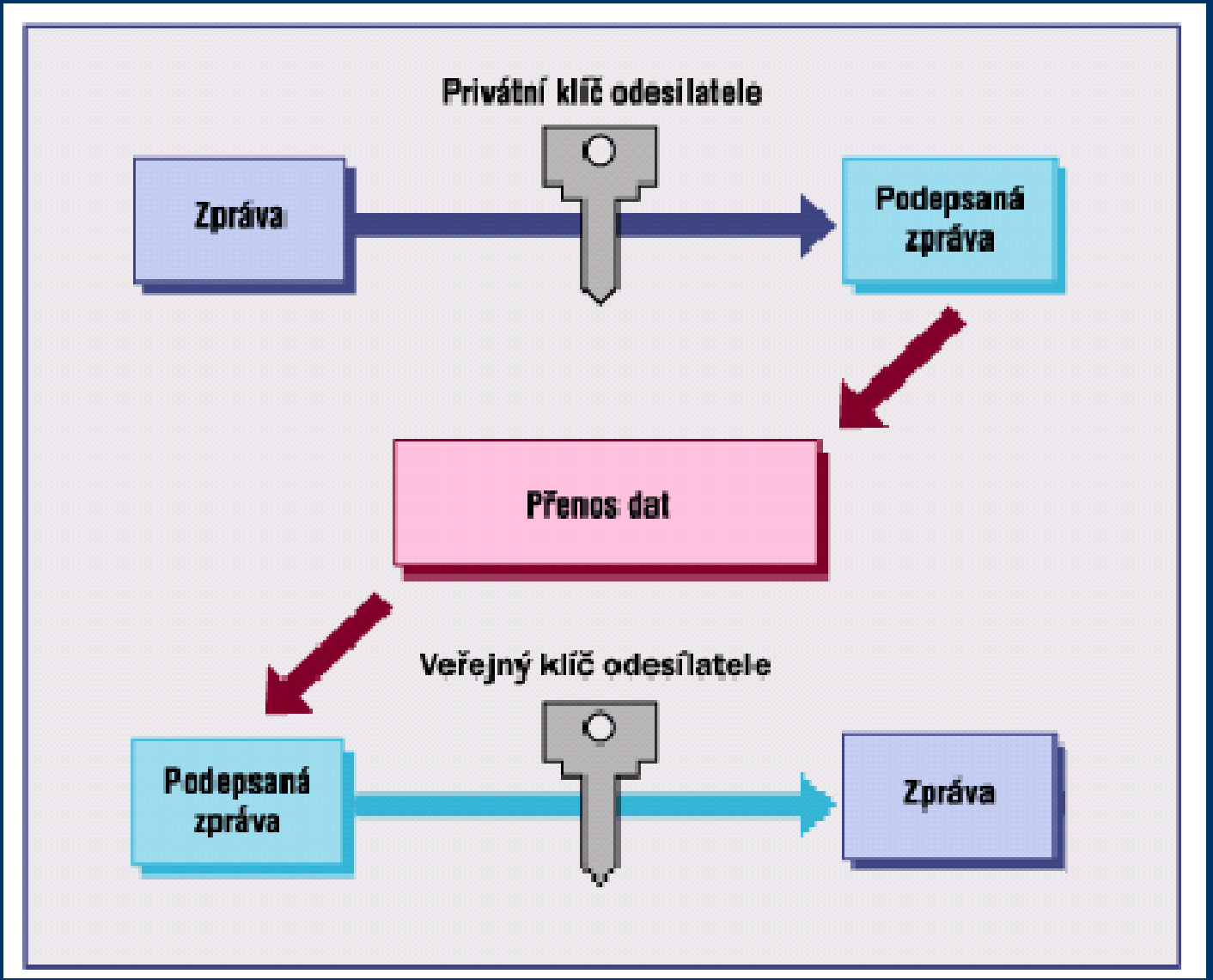
více na http://crypto-world.info

Časové razítko

- stvrzuje existenci zprávy/dokumentu před přidáním tohoto razítka/značky, ale neříká kdy zpráva vznikla
- musí ho tam umístit někdo nezávislý a důvěryhodný, tzn. „Autorita časových razítek“
- slouží k potvrzení, že zpráva byla podepsána “tehdy” platným certifikátem

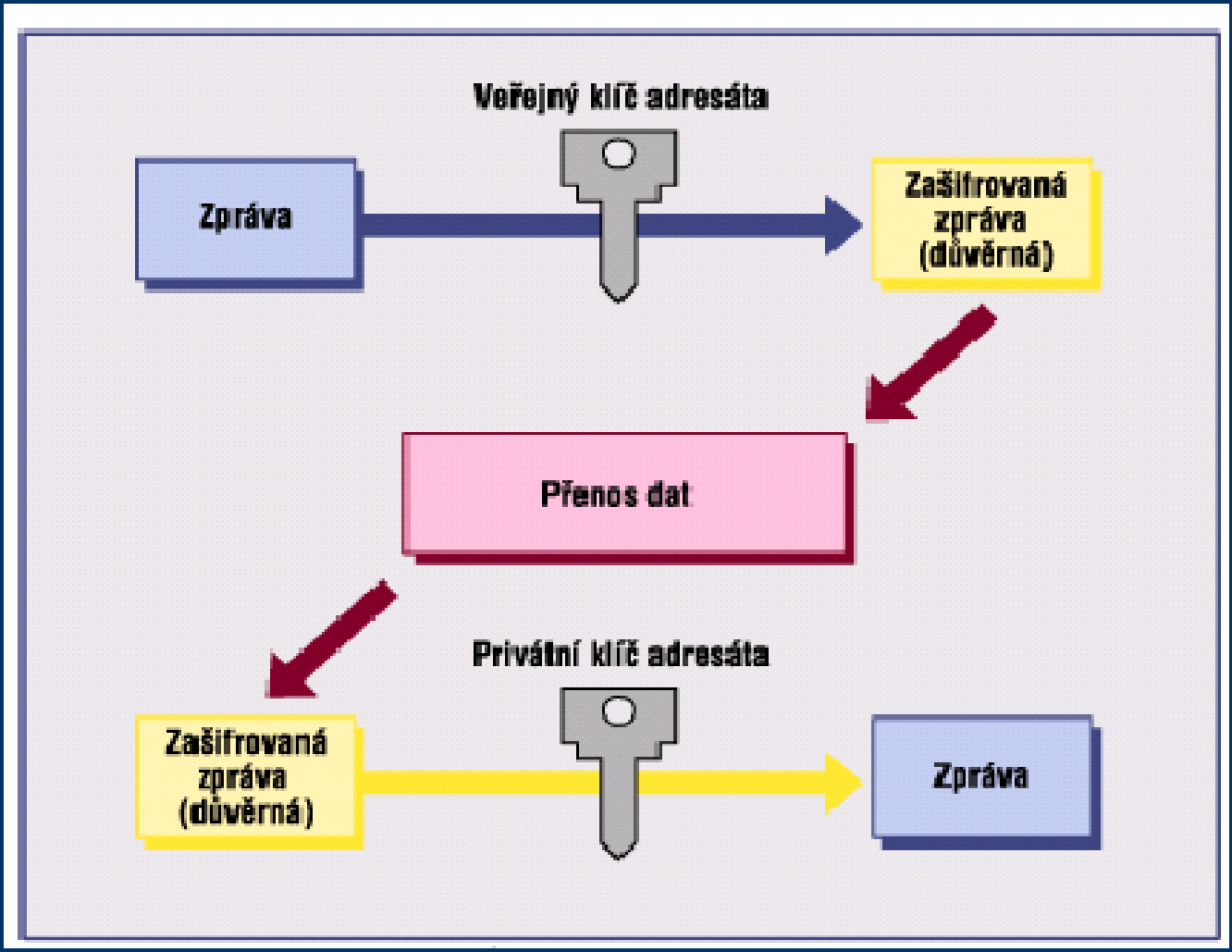
3. Princip digitálního podpisu

Princip digitálního podpisu

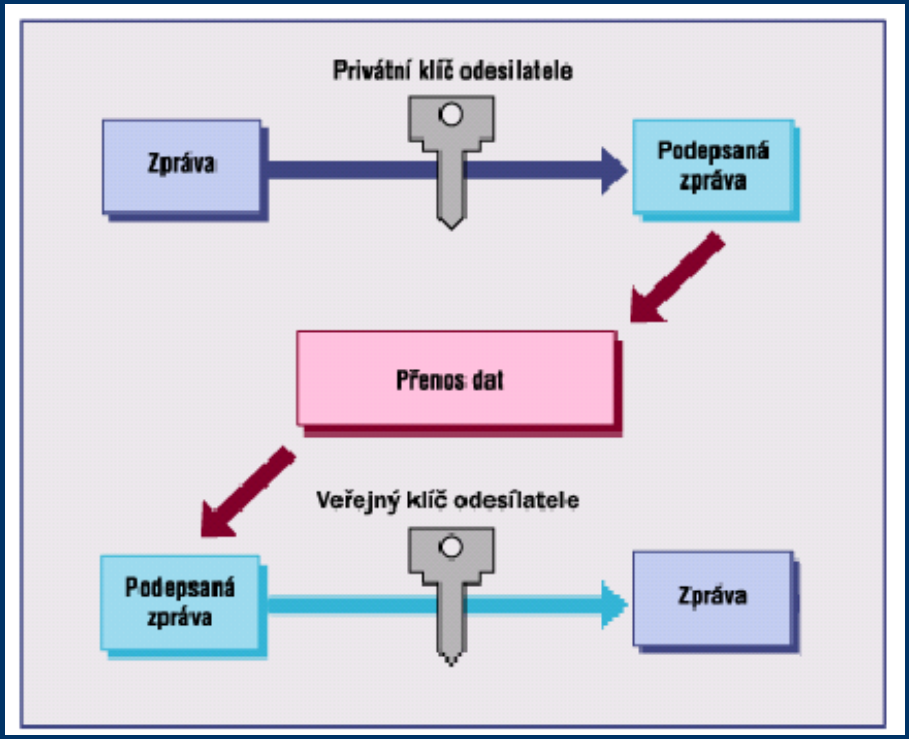


Princip digitálního podpisu

- srovnání s šifrováním



Princip digitálního podpisu



- Jak poznat komu patří daný klíč?

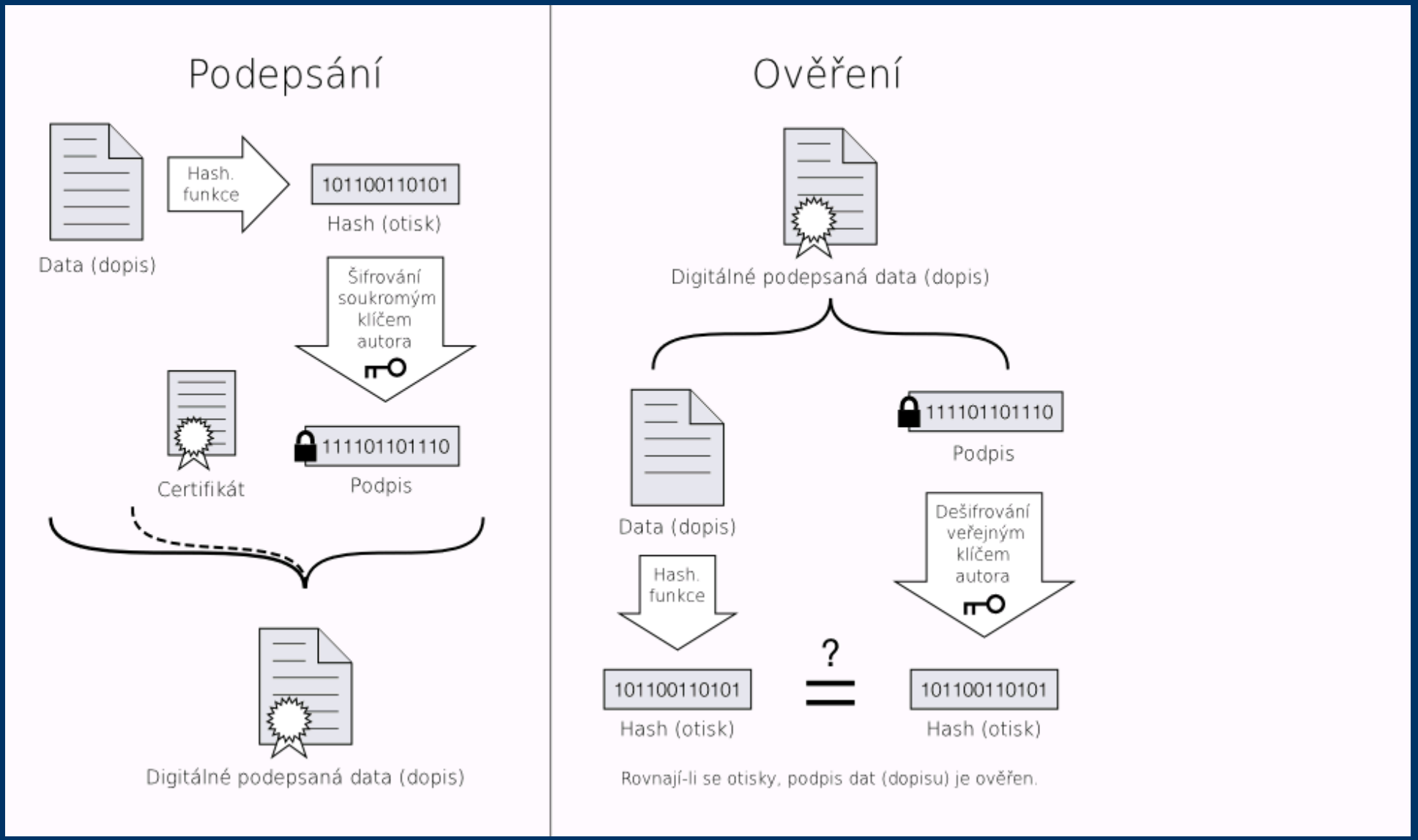
Princip digitálního podpisu

-Podpisové vzory a jejich správa

- Certifikáty = spojení podpisu (tj. veřejného klíče) a autora (tj. právnické/fyzické osoby)
  - Kvalifikované certifikáty
- Certifikační autority = správci certifikátů
  - Akreditovaný poskytovatel certifikačních služeb
  - CRL (= Certification Revocation List)

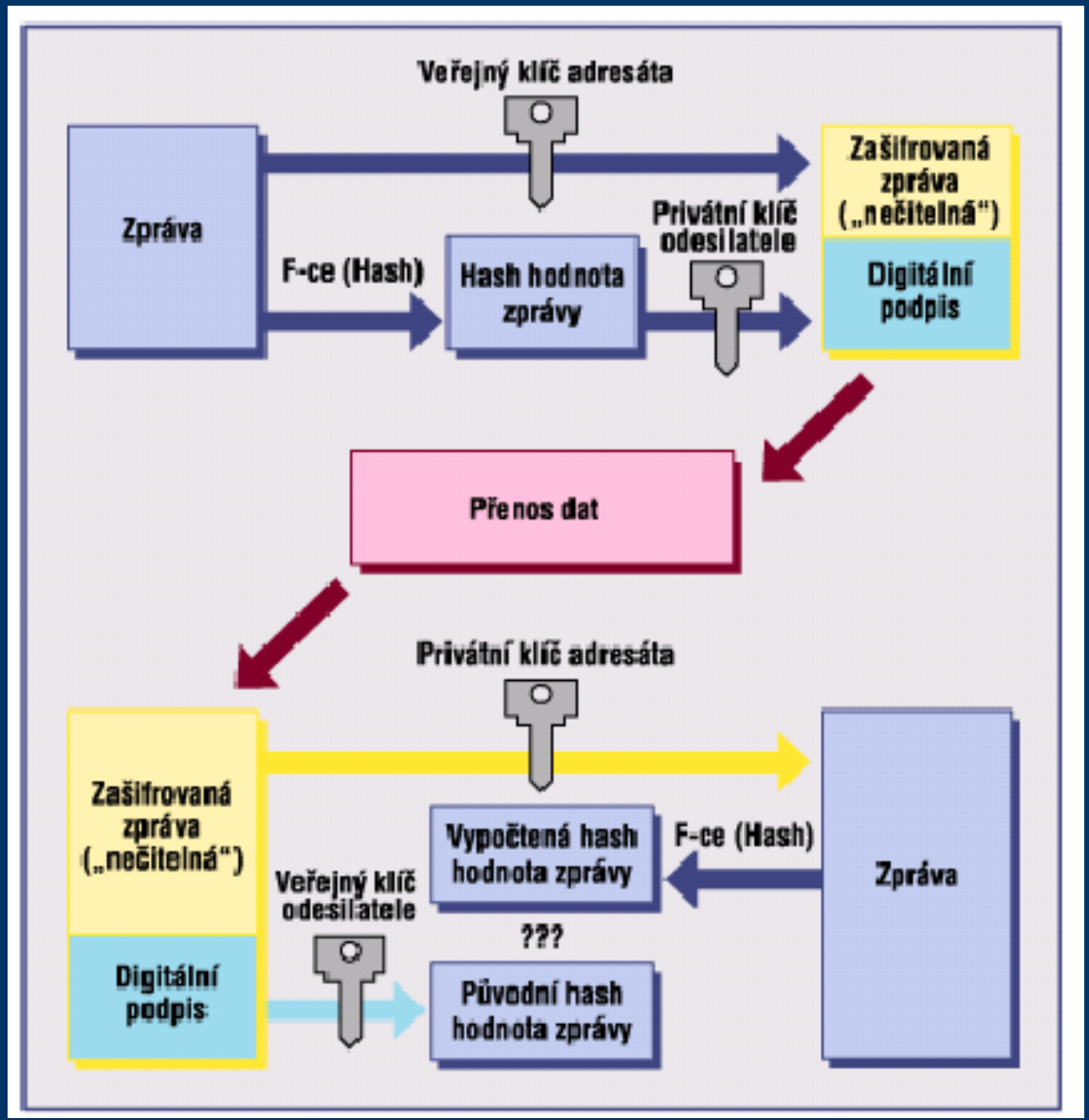
Princip digitálního podpisu

- ověření identity autora + optimalizace



Princip digitálního podpisu

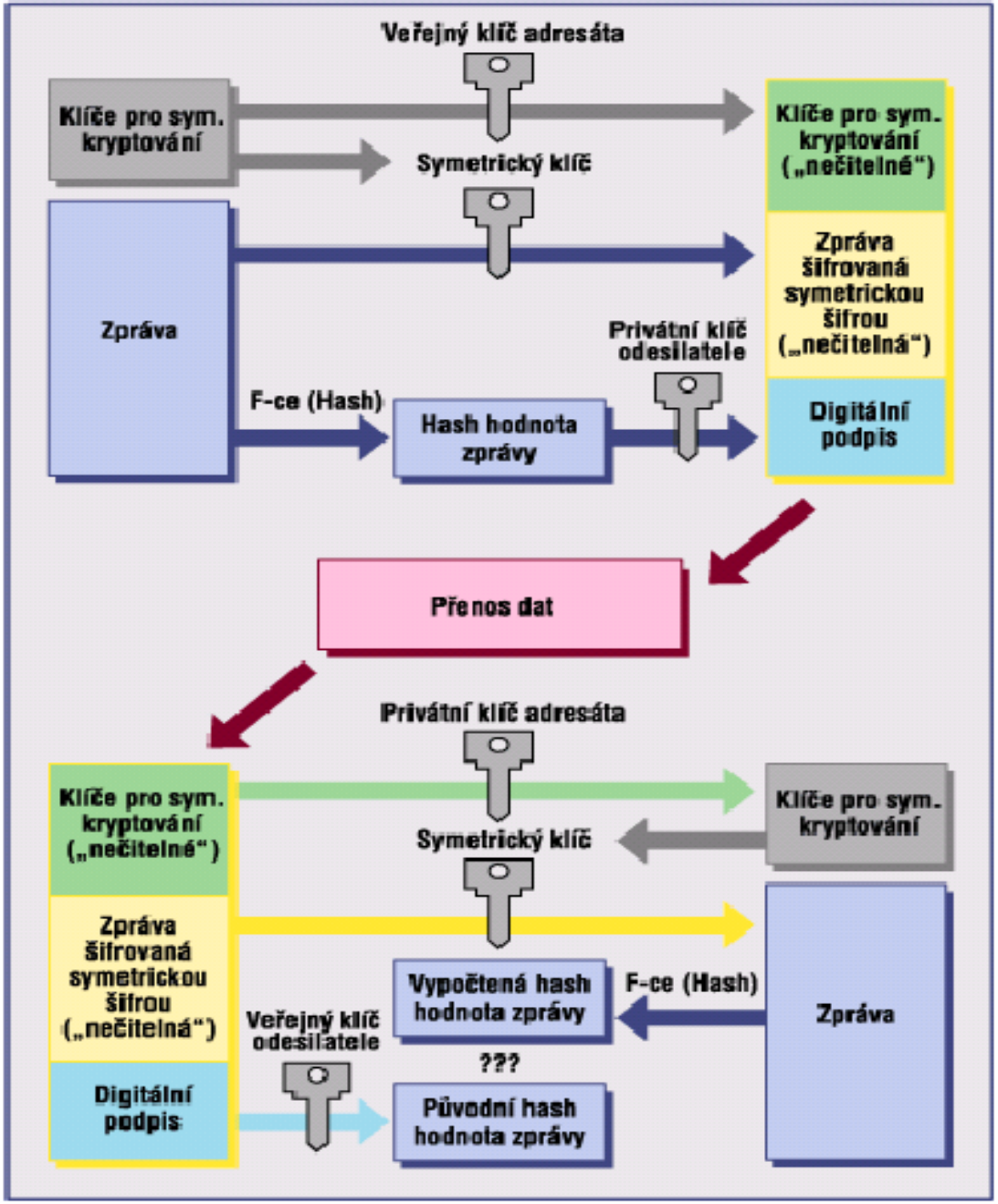
- zároveň se zašifrováním



Princip digitálního podpisu

- se zašifrováním

1. optimalizace výpočtu, podepisujeme jen hash zprávy
2. optimalizace asymetrickou kryptografií šifrujeme jen klíč, kterým je zašifrována samotná zpráva



4. Vlastnosti digitálního podpisu

Digitální podpis
- vlastnosti

- Autenticita – kdo
- Integrita – co
- Nepopiratelnost – jen on
- Časové označení - kdy

Digitální podpis
- vlastnosti

- Vztahuje se tedy k celé zprávě oproti klasickému podpisu
- Zprávou se myslí libovolná data v elektronické podobě

Digitální podpis
- kde se používá

- Jedno z prvních rozsáhlých použití: SWIFT
- V softwarovém balíku PGP
  - Kombinace RSA + IDEA
  - Digitální podpis na modelu W. Diffie & M. Hellman
- SSL – v protokolu https://
  - RSA + RC4
- S-MIME – MS Outlook
  - RSA + SHA-1

5. Algoritmus DSA

Algoritmus DSA

- Ustanoven v r. 1991 jako DSS (=Digital Security Standard) jako stadnard americké vlády

Tvorba klíčů DSA

- Výběr parametrů – veřejné, sdílené
- Vytvoření samotných klíčů

Tvorba klíčů DSA
– výběr parametrů

- Výběr kryptografické hašovací funkce: SHA-1, SHA-2
- Výběr L a N určující délku klíče
- N-bitové prvočíslo q, délka N >= délka H(M)
- L-bitové prvočíslo p, (p-1) je násobek q
- Spočte se $g = h^{(p-1)/q} \bmod p$, kde nejčastěji h = 2,
  - musí být g <>1 a (1 < h < p-1)
  - multiplikativní řád g mod p je q

Tvorba klíčů DSA
– vytvoření klíčů

- Náhodně se vybere x v rozsahu: $0 < x < q$
- Výpočet $y=g^x \bmod p$
- Veřejný klíč je pak: { p, q, g, y }
- Soukromý klíč je pak: { x }

Algoritmus DSA
– podepisování

- Pro danou zprávu se vybere hodnota k v rozsahu $0<k<q$
- Spočítá se $r = (g^k \bmod p) \bmod q$
- Spočítá se $s = (k^{-1}(H(z) + x*r)) \bmod q$
- Pokud r=0 nebo s=0, změníme k a počítáme znovu, jinak je podpisem (r, s)

Algoritmus DSA
– ověřování podpisu

- Pokud neplatí $0 < r < q$ a $0 < s < q$ pak se zamítá
- Výpočet: $w = (s)^{-1} \bmod q$
- Výpočet: $u1 = (H(z)*w) \bmod q$
- Výpočet: $u2 = (r*w) \bmod q$
- Konečně: $v = ((g^{u1} * y^{u2}) \bmod p) \bmod q$
- Podpis platí pokud: $v = r$

< Konec >

Použité zdroje:

- Martin Rybák 2006; Elektronický podpis v legislativě a v praxi ČR, bakalářská práce
- Simon Singh 2003; Kniha kódů a šifer, Nakladatelství Argo
- Wikipedie [cit. 6.4.2010] <http://cs.wikipedia.org/wiki/Digital_Signature_Algorithm>