Algoritmus RSA

Jáchym Tomášek
info@tomasek.work
www.tomasek.work/RSA.pdf

Komunikace pomocí RSA

Před začátkem komunikace pomocí RSA

- Zvolí se dvě velká prvočísla p a q
- Spočítá se jejich součin n: $n = pq$
- Spočítá se hodnota Eulerovy funkce $\phi(n) = (p - 1)(q - 1)$
- Zvolí se číslo e: $e < \phi(n)$ a e je nesoudělné s $\phi(n)$
- Zjistí se číslo d: $de = 1 \pmod{\phi(n)}$

Komunikace RSA

- Veřejný klíč – *e* a *n*
  - *e* je šifrovací exponent
  - *n* je modul
- Soukromý klíč – *d* a *n*
  - *d* je dešifrovací exponent
  - *n* je modul

Zašifrování komunikace RSA

- Zpráva se převede na číslo j: $j < n$
- Zpráva se zašifruje na číslo k: $k = j^e \ mod \ n$
- Číslo k je zašifrovaná zpráva, která se odešle příjemci

Dešifrování komunikace RSA

- Příjemce dostane zašifrovanou zprávu *k*
- Původní zprávu *j* získá pomocí: $j = k^d \bmod n$

Digitální podpisy

Certifikát

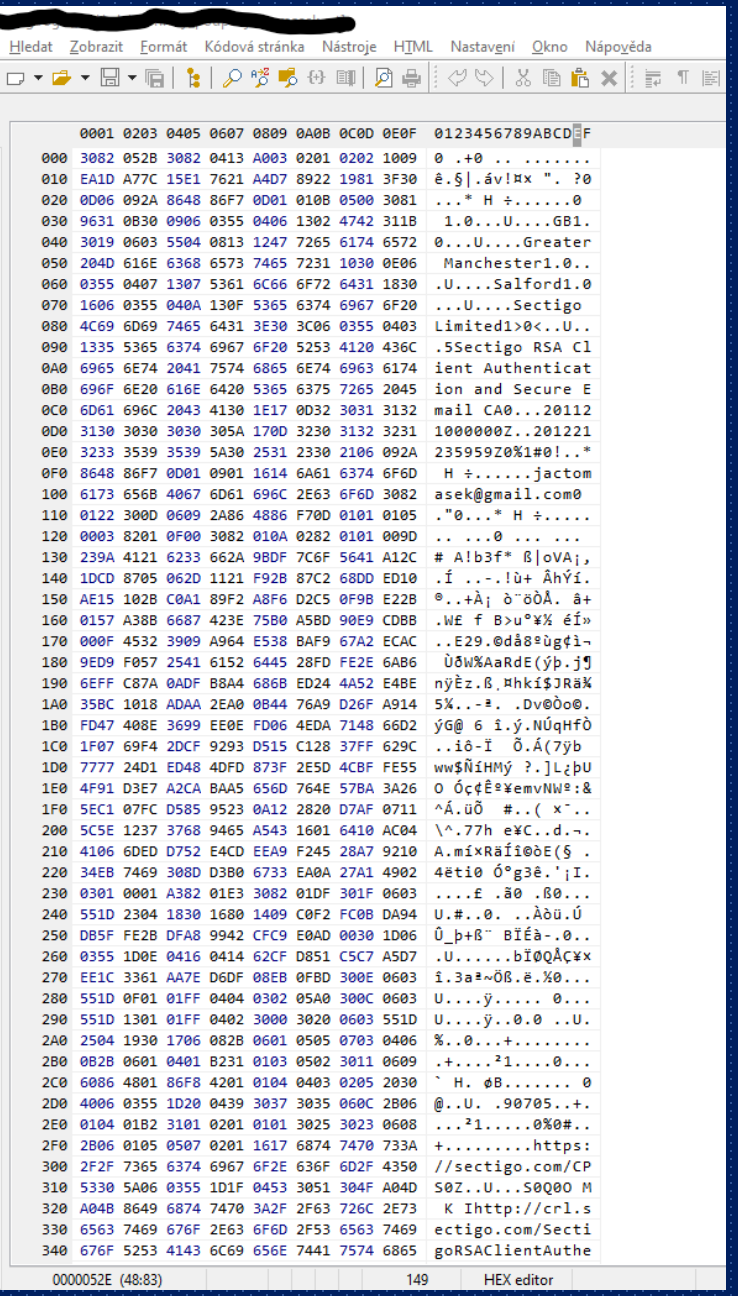
- Certifikační autorita vytvoří soukromý a veřejný klíč

- Veřejný klíč je dostupný všem (i příjemci)
- Soukromý klíč je uložený na počítači majitele nebo na nějakém externím zařízení

- Pomocí certifikátu se ukládá soukromý klíč na počítač

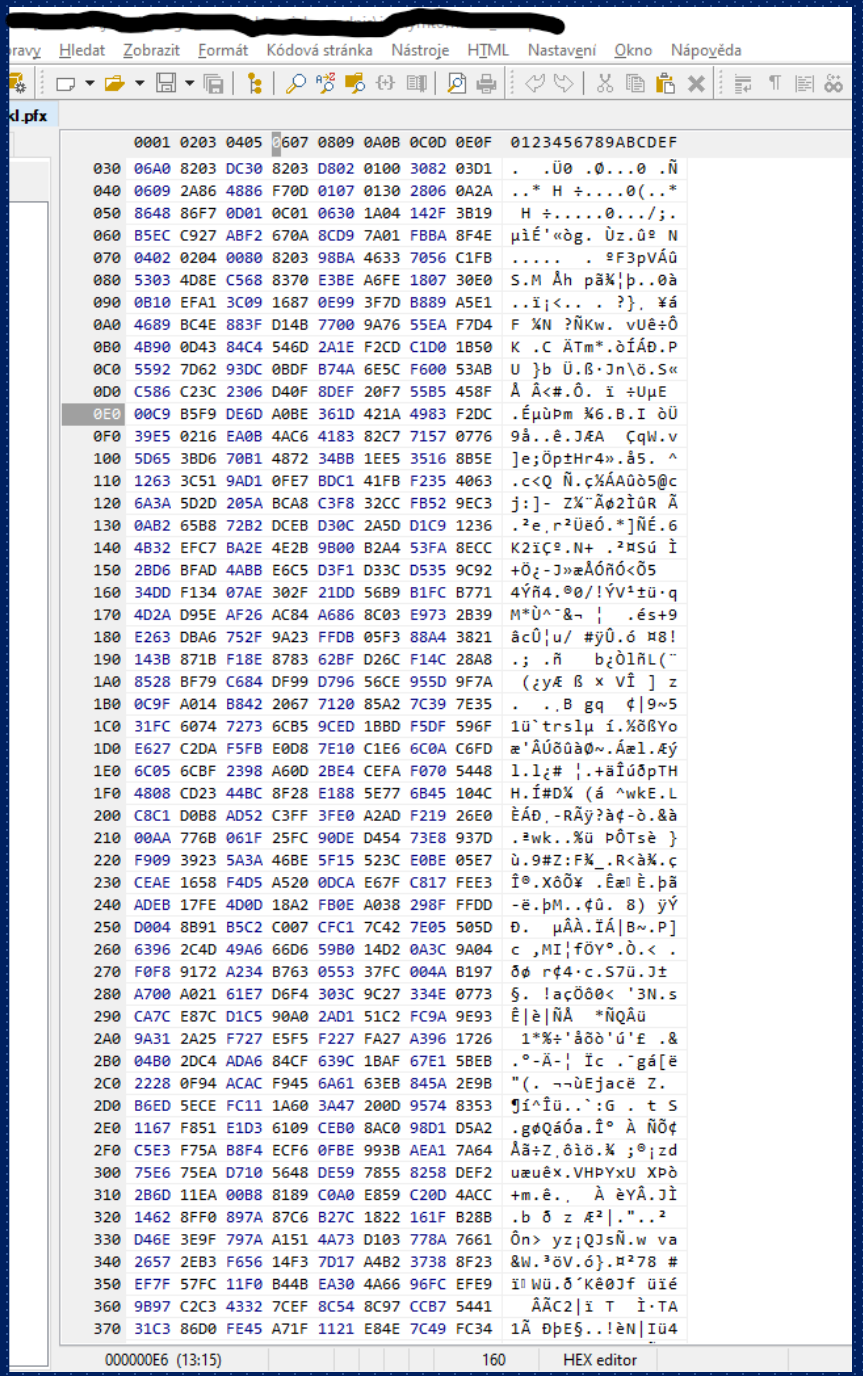
Certifikát

- Soubor s příponou CRT



Soukromý klíč

- Soubor s příponou PFX
- Dlouhý kolem 150 řádků
- Veřejný klíč vypadá podobně

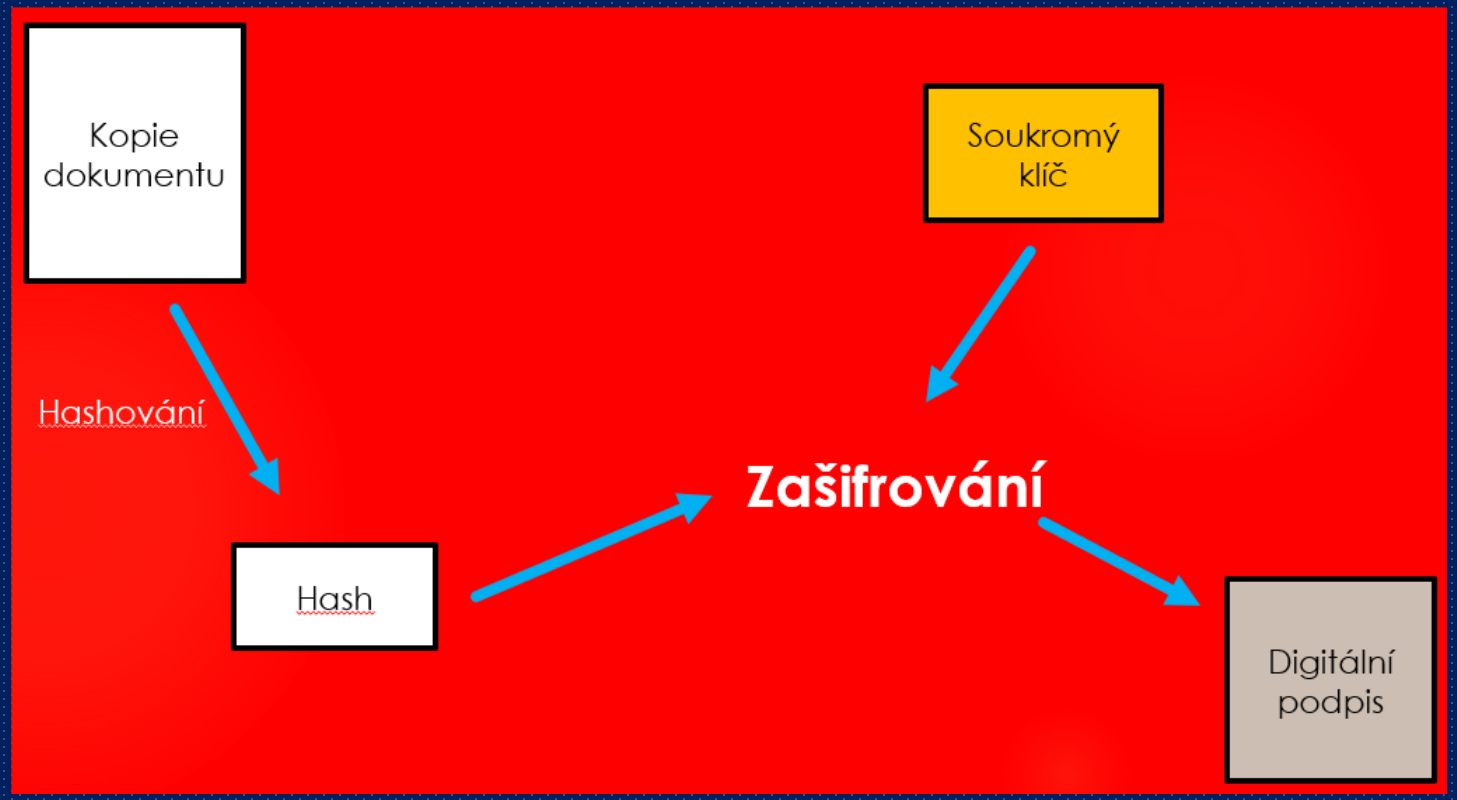


Digitální podepsání dokumentu

- Vytvoření kopie podepisovaného dokumentu
- Zahashování kopie dokumentu (SHA, MD5, …)
- Zašifrování hashe (*j*) soukromým klíčem (*d*) autora: $k = j^d \bmod n$

- Podpis *k* je přiložen k podepsanému dokumentu

Digitální podepsání dokumentu

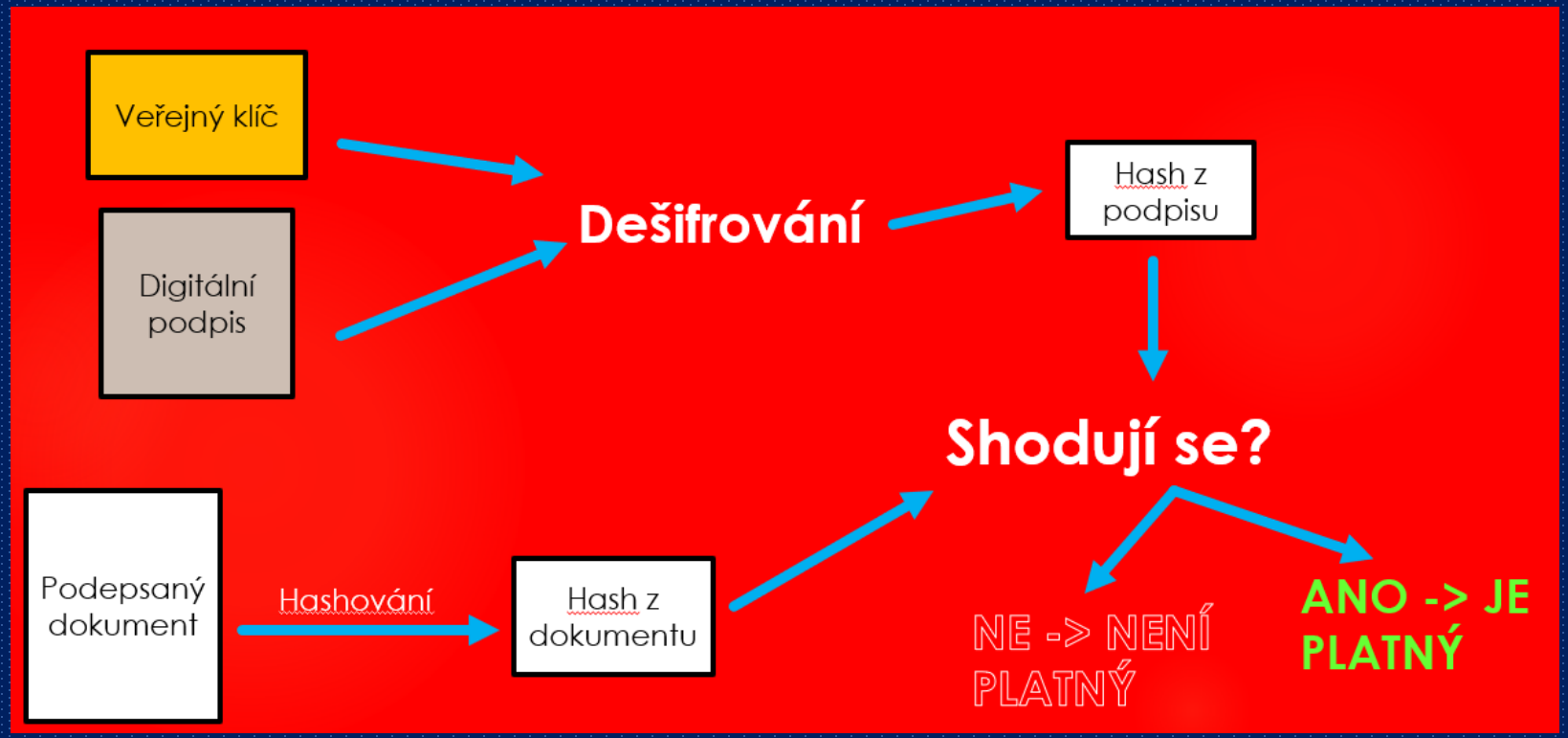


Ověření podepsaného dokumentu

- Podpis je zahashován stejnou funkcí jako při podepisování
  - Výsledek je hash přijatého dokumentu *m*
- Dešifrování podpisu (*k*) veřejným klíčem (*e*) autora: $j = k^e \bmod n$
  - *j* je hash kopie původního dokumentu

- Pokud se *j* a *m* shodují, s dokumentem se od podepsání nic nestalo.
- Pokud se *j* a *m* neshodují, dokument byl změněn a není důvěryhodný.

Ověření podepsaného dokumentu



Odkazy

- https://is.muni.cz/th/tk3wj/thesis.pdf
- https://is.ambis.cz/th/wpg59/DP_nastroje_pro_generovani_klicu.pdf
- https://knihy.nic.cz/files/edice/bajecny_svet_elektronickeho_podpisu_cznic.pdf