Pavel Vondruska

Digitálně podepsal Pavel Vondruska
DN: CN = Pavel Vondruska, C = cz, O = O2, OU = ZAM
Důvod: Jsem autor tohoto dokumentu
Datum: 2008.04.22 18:23:08 +02'00'

MFF UK
Praha, 22. duben 2008

Elektronický podpis / CA / PKI – část 1.

http://crypto-world.info/mff/mff_01.pdf

P.Vondruška

Telefónica

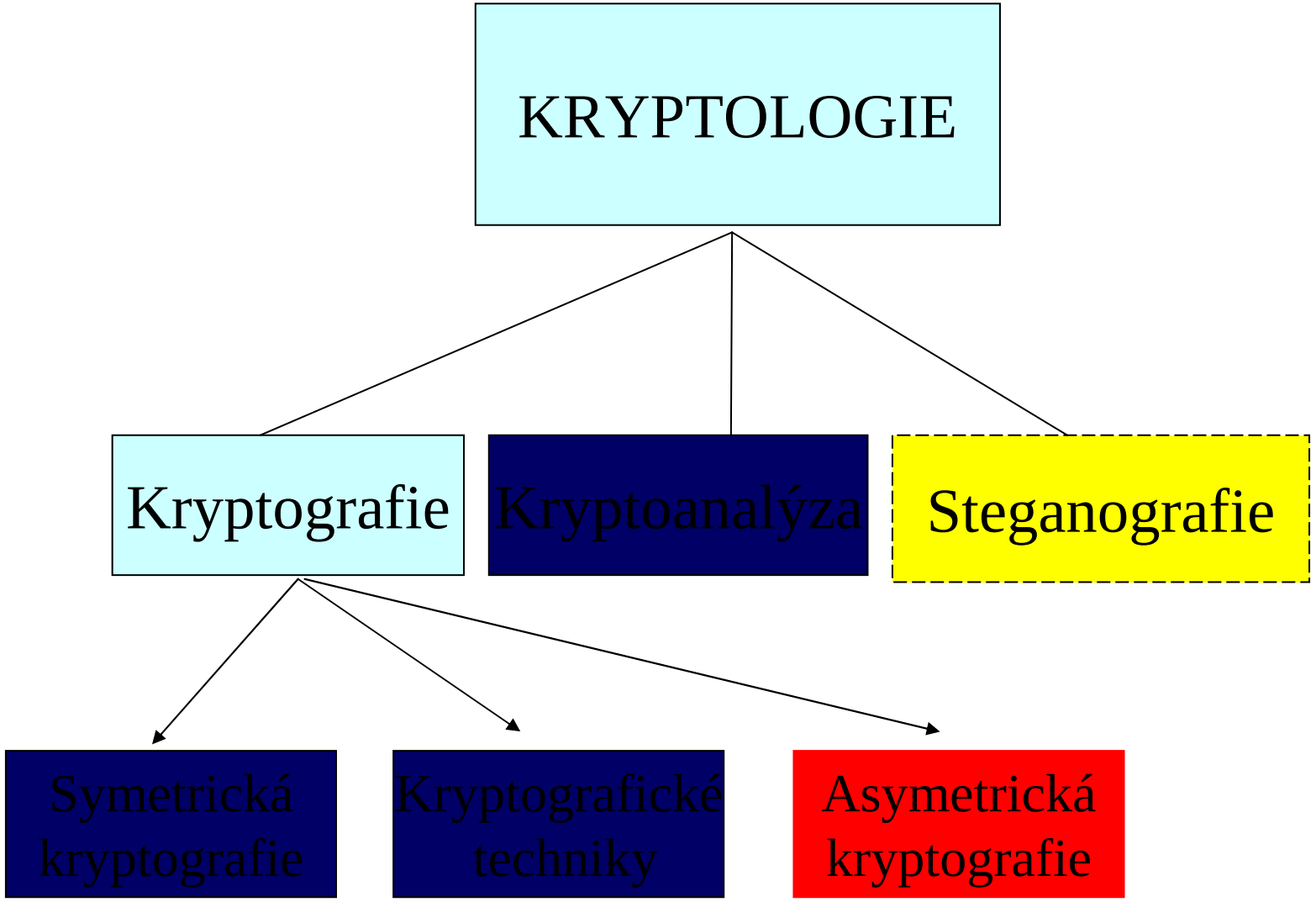
O2

Přednáška pro ty, kteří chtějí vědět **PROČ** kliknout ANO/NE a co zatím všechno „vězí“.

1. **ÚVOD**
2. Základní pojmy asymetrické kryptografie (filozofie, algoritmy, podpisové schéma)
3. Ukázka ….
4. Zákon o elektronickém podpisu č.227/2000 Sb. (pojmy : typy podpisů, poskytovatelů, certifikátů ..)
5. Certifikační autority (přehledy poskytovatelů, jak pracují a co jej jejich úkolem)
6. Důvěra v elektronické podpisy (vystavitel, nastavení a vše co s tím souvisí)

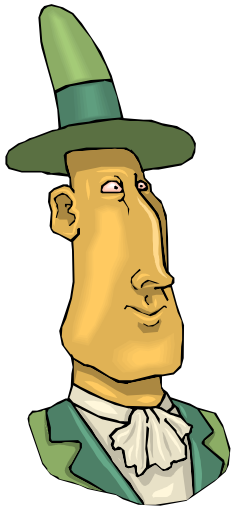
Při zavádění EL.PODPISU (PKI) je třeba řešit celou řadu velmi odlišných problémů:

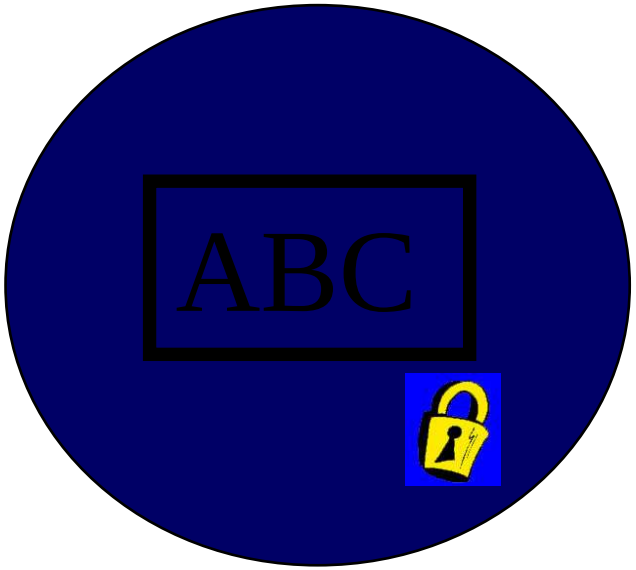
- Legislativně-právní (bude uznáno jako důkaz?) (právo)
- Volba vhodných algoritmů (kryptografie)
- Bezpečnostní (standardy, úložiště, SW, …) (informační bezpečnost)
- Administrativně – procesní („pořizování“ certifikátů, nová agenda, noví zaměstnanci)
- Kladeny nároky na SW (mimo bezpečnosti je to především kompatibilita)
- Kladeny nároky na uživatele (školení !!!)

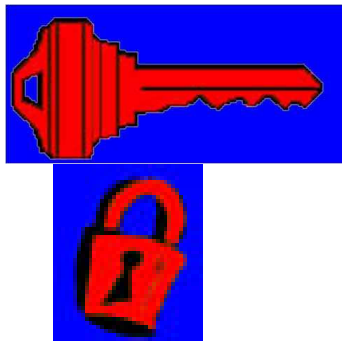

KRYPTOLOGIE
Kryptografie
Kryptoanalýza
Steganografie
Symetrická kryptografie
Kryptografické techniky
Asymetrická kryptografie

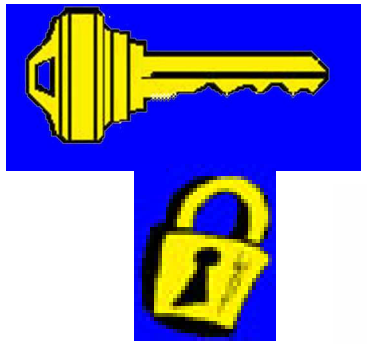
Asymetrická kryptografie

Šifrování (zjednodušeně)



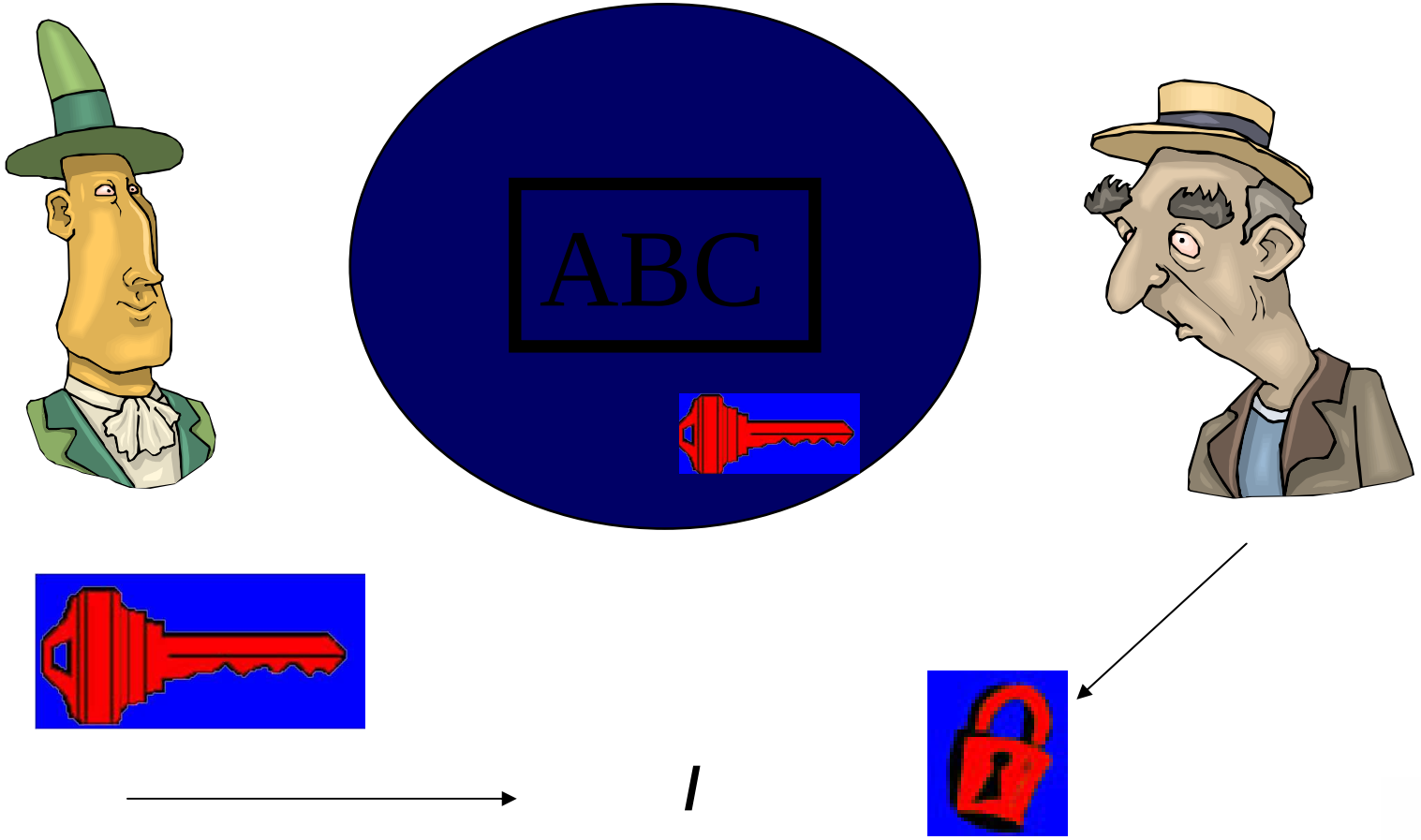






Asymetrická kryptografie

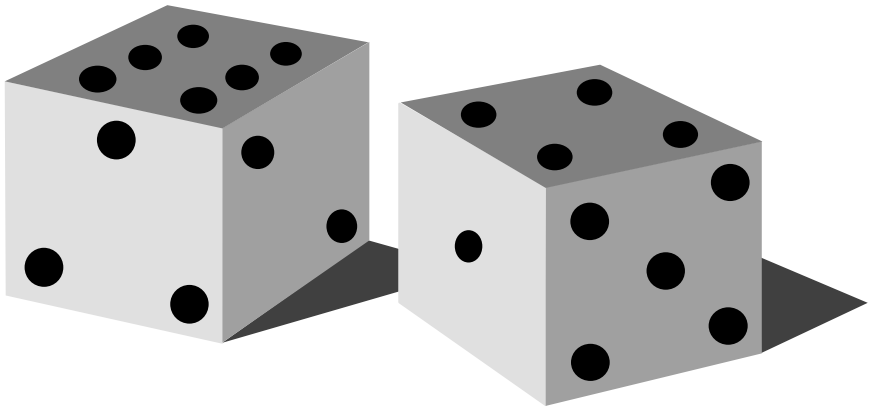
Digitální podpis (zjednodušeně)



Popis algoritmu RSA

Postup při vytváření dvojice veřejný a soukromý klíč (dat pro vytváření a ověření elektronického podpisu) pro RSA je následující:

a) nejprve náhodně (a nepredikovatelně) vygenerujeme dvě dostatečně velká prvočísla (jejich přibližná velikost tj. počet bitů je zadána) (Vondruška, P.: Fermatův test primality, Carmichelova čísla, bezčtvercová čísla. Crypto-World 6/2000)



b) Spočteme

$$N = p*q \quad a$$

$$\Phi(N) = (p-1)*(q-1)$$

Poznámka 1: $\Phi(N)$ je Eulerova funkce určující počet přirozených čísel nesoudělných s n.

Poznámka 2: stačí spočítat číslo $L = NSN(p-1, q-1)$ tj. nejmenší společný násobek čísel p-1 a q-1.

c) Zvolíme náhodné číslo e, kde

$$1 < e < \Phi(N), \quad \text{tak, že} \quad NSD(e, \Phi(N)) = 1$$

(tj. e a $\Phi(N)$ jsou nesoudělná) .

Zde NSD značí největšího společného dělitele.

d) Užitím Eukleidova algoritmu spočteme jednoznačně definované číslo d takové, že

$$1 < d < \Phi(N) \text{ a}$$
$$e*d \equiv 1 \mod \Phi(N) .$$

Existence takového čísla d je dána Bautzovou větou.

Veřejným klíčem je potom (e,N), soukromým klíčem uživatele je (d,N).

Číslo N nazýváme modul, číslo e veřejný exponent a číslo d soukromý exponent. Veřejný klíč zde tvoří čísla e, N, zadními vrátky je čtveřice čísel p, q, d, Φ (N). Přitom znalost jednoho z čísel p, q, Φ (N) vede k bezprostřednímu nalezení zbývajících tří a znalost čísla d nám dává pravděpodobnostní polynomiální algoritmus pro faktorizaci čísla N.

Popis vlastního šifrování a dešifrování

Popíšeme nyní jak probíhá vlastní zašifrování a odšifrování. Předpokládejme, že strana B zná autentický veřejný klíč strany A, kterým je (N,e) a šifruje zprávu M pro A.
Strana B vyjádří zprávu M jako číslo m, $0 \leq m \leq N-1$ (resp. posloupnost takových čísel).
Dále strana B spočte

$$c = m^e \mod N$$

a zašle šifrový text straně A.

Strana A nyní při odšifrování spočte pomocí tajného klíče d

$$m = c^d \mod N$$

Výsledkem je skutečně m, což lze dokázat následovně :

Jelikož $e*d \equiv 1 \bmod \Phi(N)$, existuje tedy k tak, že $ed = 1 + k\Phi(N)$.
Dále, pokud NSD (m,p) = 1, pak podle Fermatovy věty

$$m^{p-1} \equiv 1 \bmod p.$$

Umocníme obě strany této kongruence číslem k(q-1) a posléze vynásobíme obě strany rovnice číslem m.
Dostaneme

$$m^{1 + k(p-1)(q-1)} \equiv m \bmod p.$$

Pokud je NSD (m,p) = p (druhá možná situace), pak tato rovnost platí rovněž (obě strany jsou rovny nule mod p).

Vždy tedy

$$m^{ed} \equiv m \bmod p\ .$$

Obdobně se dokáže

$$m^{ed} \equiv m \bmod q\ .$$

Odtud plyne

$$m^{ed} \equiv m \bmod N,$$

a tedy

$$c^d \equiv (m^e)^d \equiv m \bmod N\ .$$

Příklad vytvoření dvojice klíčů (s malými čísly)

p=47, q=71, N= p*q = 47*71 = 3337

(p-1)*(q-1)= 46*70 = 3220

e (nesmí mít společné dělitele s 3220) , volíme 79

d …… e*d=1 mod 3220

d= e^{-1} mod 3220 = 1019 (Eukleidův algoritmus)

e …….. veřejný klíč (79, 3337) ,

d …….. soukromý klíč (1019, 3337)

Příklad přímé šifrování a dešifrování

zpráva M= 688232687152455284848789678

M rozdělíme na bloky m_1 m_2 m_3 …..

M = 688 232 687 …

šifrování :

blok m_1 = 688

$c_1 = m_1^e \mod N$

$c_1 = 688^{79} \mod 3337 = 1570$

dešifrování :

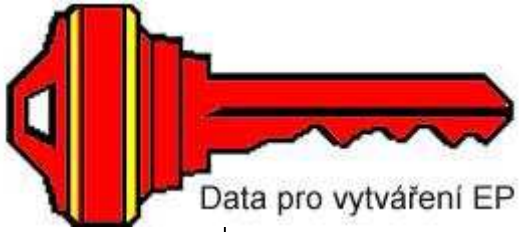
$m_1 = c_1^d \mod N$

$1570^{1019} \mod 3337 = 688$

blok m_1 = 688

Podpis datové zprávy

Datová zpráva soubor libovolného typu, například: message.doc csp.exe kocka.jpg



SHA-1
MD5

Výsledek hashovací funkce

RSA
DSA
EC

Elektronický podpis datové zprávy

Ověření podpisu datové zprávy

Datová zpráva soubor libovolného typu, například: message.doc csp.exe kocka.jpg

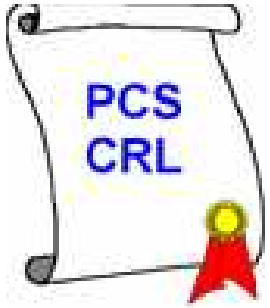
Elektronický podpis datové zprávy

RSA
DSA
EC

SHA-1
MD5

Výsledek hashovací funkce

Hash před podpisem



Identifikace
Neporušenost
Nepopiratelnost
Akceptovatelnost

Telefónica

O2

Pavel Vondruška
Crypto-World
http://crypto-world.info
mobil +420 602 560 963
