Aplikace teorie čísel

- výpočetní aspekty
- kryptografie

Základní úlohy TČ

$(\mathrm{mod}\ n)$ – $+, -, \cdot, x^y$

– NSD, Bezout, inverze

$x \cdot x^{-1} (= x^{-1} \cdot x) = 1$

$151x \equiv 20 \pmod{315} \quad / 151^{-1}$

$151^{-1} \cdot 151 x \equiv 151 \cdot 20 \quad -\!\!\!\cdot\!\!\!-$

$151^{-1} = 151^{\varphi(315)-1}$

$2^{560} \pmod{561}$

$2^{560} = (2^2)^{280} = 4^{280} = 16^{140} = 256^{70} \equiv 460^{35}$

$= 460 \cdot 460^{34} \equiv 460 \cdot 103^{17} \equiv (460 \cdot 103) \cdot 256^{8}$

$\equiv 256 \cdot 256^4 \equiv 256 \cdot 460^2 \equiv 256 \cdot 103 \equiv 511$

$\equiv 1 \cdot 511^0 \equiv 1$

$560 = (1000110000)_2$

Kryptografie s veřejným klíčem

RSA

dva klíče - veřejný a soukromý

p, q velká prvočísla $n = p \cdot q$

$\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$

n veřejné, $\varphi(n)$ je těžké spočítat

(p zná šifrátor, může si $\varphi(n)$ spočítat)

veřejný klíč ... e $\quad (e, \varphi(n)) = 1$

soukromý klíč ... d $\quad e \cdot d \equiv 1 \pmod{\varphi(n)}$

známe-li $\varphi(n)$, určíme d jako $e^{-1} \bmod \varphi(n)$

M, zpráva $(\bmod n)$

šifrování: $C \equiv M^e \pmod n$

dešifrování: $C^d \equiv (M^e)^d = M^{e \cdot d} \equiv M^1 \pmod n$

$$M^{\varphi(n)-1} \equiv 1 \pmod n$$

Rabin

V - veřejný, S - soukromý

p, q velká prvočísla, $p, q \equiv 3 \pmod 4$

$V = n = pq$, $\quad S = (p, q) \leftarrow$ usp. dvojice

šifrování: $C \equiv M^2 \pmod n$

dešifrování: vezmeme čtyři odmocniny z C

nejprve: vše $(\bmod n)$

$r \equiv C^{p+1/4}$, $\quad s \equiv C^{q+1/4}$

$ap + bq = 1 \Rightarrow a, b$

$x \equiv aps + bqr \qquad y \equiv aps - bqr$

odmocniny jsou $\pm x, \pm y$

$x^2 \equiv C \pmod n \Leftarrow x^2 \equiv C \pmod p$ a $\pmod q$

$x^2 \equiv (xps + bqr)^2 \equiv (bq)^2 r^2 \equiv 1^2 \cdot C^{p+1/2} \pmod p$

rovnice je řešitelná pro $C^{p-1/2} \equiv 1 \pmod p$

$\rightarrow \equiv C$

Př. $p=23, q=31 \quad n=pq=713 \quad M=327$

$C \equiv 327^2 \equiv 692 \pmod{n}$

$C^6 \equiv 18 \pmod{23} \quad C^8 \equiv 14 \pmod{31}$

$-4 \cdot 23 + 3 \cdot 31 = 1$

$\pm 4 \cdot 23 \cdot 14 \pm 3 \cdot 31 \cdot 18 \pmod{713}$

Digitální podpis

$M \to H \to S(H)$ podepsání

otisk (hash) / šifrování soukromým klíčem

$\to H' \overset{?}{\equiv} V(S(H))$ kontrola (ověření)

Diffie - Hellman

p prvoč. veřejné, g primit. kořen $(\mathrm{mod}\ p)$ také veřejný

a soukromý, b soukromý

$g^a \ldots S(H) \quad \times \quad g^b \ldots S'(H)$

$g^{ab} \qquad\qquad g^{ab}$ – společný klíč

El Gamal

Alice ... p prvo., prim. k. g, soukromé a $\to (p, g, g^a) \to$ Bob

Bob ... volí b $\quad C_1 \equiv g^b \pmod{p}$

$h = g^a \quad C_2 \equiv M \cdot h^b$

dešifrování Alicí: k inverze k $C_1^a = g^{ab} = h^b$

$c_2 \cdot k \equiv M$