Šifrování:
příklad 1 - RSA (PKC)

2 klíče: veřejný V_A, soukromý S_A

p,q prvočísla, $n = p\cdot q$ (těžké spočítat)

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

veřejný klíč je e takové, že $(e, \varphi(n)) = 1$

soukromý klíč: d takové, že $e\cdot d \equiv 1 \mod \varphi(n)$

$M \longmapsto C = V_A(M) = M^e \pmod n$

$C \longmapsto S_A(C) = C^d \pmod n = (M^e)^d = M^{e\cdot d} = M \pmod n$

3 20-15:55

10.87. RSA, veřejný klíč $(7, 33)$. Byla poslána: 29, 7, 21. Jaká byla M?

$n = 33$, $e = 7$

chceme řešit $7\cdot d \equiv 1 \pmod{\varphi(33)}$

$\varphi(33) = \varphi(3)\,\varphi(11) = 20$

"vidíme" $7\cdot 3 \equiv 1 \pmod{20} \Rightarrow d = 3$

$29 \longmapsto 29^3 = (-4)^3 = +2 \pmod{33}$

$7 \longmapsto 7^3 = 16\cdot 7 = 112 = 13 \pmod{33}$

$21 \longmapsto 21^3 = 3^3\cdot 7^3 = (-6)\cdot 13 = 21 \pmod{33}$

3 20-16:18

Útok na RSA:

$n = p\cdot q$, $|p-q|$ malé $\qquad (a\pm b)^2 = a^2 + b^2 \pm 2ab$

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

$\Rightarrow s = (p-q)/2$ malé $\quad t = (p+q)/2 \simeq \sqrt{n}$

$t = \lceil\sqrt{n}\rceil,\ t = \lceil\sqrt{n}\rceil + 1, \ldots$

$n = 23104222007$

$\sqrt{n} \approx 152000{,}731$

$t = 152001$

$\vdots$

$t = 152004 \quad \sqrt{t^2 - n} = 997 \in \mathbb{Z} \Rightarrow s = 997$

3 20-16:43

Rabinův kryptosystém:

V_A, S_A: $n = p\cdot q$, $p,q \equiv 3 \pmod 4$

$V_A = n$

$S_A = (p,q)$

zpráva $M \longmapsto C = V_A(M) \equiv M^2 \pmod n$

dešifrování:

odmocnina mod p, mod q zvlášť:

$r = C^{(p+1)/4} \pmod p \quad s = C^{(q+1)/4} \pmod q$

$\Rightarrow r^2 \equiv C \mod p$, $s^2 \equiv C \mod q$

kvadratické: $x^2 \equiv a \pmod n$

$x = \pm aps \pm bqr$, $ap + bq = 1$

3 20-16:50

10.92 A: $(p,q) = (23, 31) = S_A \quad V_A = n = 713$

B: $M = 327 \longmapsto M^2 = (327)^2 \pmod{713}$

$C = 692 \pmod{713}$

A: $\sqrt{C} = \sqrt{692} \pmod{713}$ $\qquad ap + bq = 1$; $(-4)\cdot 23 + 3\cdot 31 = 1$

$713 = 23\cdot 31$, hledáme $r^2 \equiv C \mod 23$, $s^2 \equiv C \mod 31$

$r = C^{\frac{p+1}{4}} = 692^{\frac{23+1}{4}} = 692^6 \equiv 18 \mod 23$

$s = C^{\frac{q+1}{4}} = 692^8 \equiv 14 \mod 31$

$x = \pm aps \pm bqr = \pm(-4)\cdot 23\cdot 14 \pm 3\cdot 31\cdot 18 \pmod{713}$

$\Rightarrow 386, 603, 110, 327$

3 20-17:00

Diffie-Hellman

p -- prvočíslo

g -- primitivní kořen $\pmod p$ } veřejné!

tj. $g^{p-1} \equiv 1 \mod p$

$A \longleftrightarrow B$

A: x lib. $g^x \mod p$

B: y lib. $g^y \mod p$

$\Rightarrow g^{xy}$ je "společný klíč"

ElGamal šifra:

A: $(p, g, h = g^x)$

x je soukromé

M: zvolíme y lib., $C_1 = g^y \pmod p$, $C_2 = M\cdot h^y$

zpráva (C_1, C_2)

A: dešifruje: $C_2\cdot C_1^{-x} = M\cdot g^{xy}\cdot g^{-xy} = M$

3 20-17:16

10.91.

A: $p = 41$, $g = 11$, $x = 10$

Sec Alice: $(41, 11, \boxed{9})$

$h = g^x$

Bob posílá: $(22, 6) = (c_1, c_2)$

$m = 6/22^{10} = 6 \cdot 9 = 13 \pmod{41}$

$\varphi(41) = 40$

Řády: 2, 4, 5, 8, 10, 20

$-2 \; 4 \; 3 \; 16 \; 9 \; -1$

$= p$

$11^{10} \pmod{41}$

$22^{10} = 11^{10} \cdot 2^{10} = 9 \cdot 41$

$= -9 \pmod{41}$

$(-9)^{-1} \equiv 9 \pmod{41}$

3 20-17:28

3 20-17:36