Robinův kryptosystém –

$p \equiv 3 \mod 4$, p prvočísla

$x^2 \equiv a \mod p$

umíme vyřešit "lehce"

$x := \pm a^{\frac{p+1}{4}} \mod p$

- $n = pq$,

$V = n$ veřejný prvočísla

$S = (p, q)$

$p \equiv 3 \mod 4$
$q \equiv 3 \mod 4$

- zašifrování zprávy M:

$C := M^2 \bmod n$

- dešifrování: vyřešíme rovnici $x^2 \equiv C \bmod n$

$x^2 \equiv C \bmod p$
$x^2 \equiv C \bmod q$
} umíme vyřešit

$\rightarrow$ ČZV $\rightarrow$ vyřešíme

NB: 4 řešení

5.4 (i)

- veřejný klíč $n = 437$
- zpráva $M = 321$

- zašifrování:

$C = M^2 = (321)^2 \equiv (-116)^2 = (4 \cdot 29)^2$

$$= 4^2(30-1)^2 = 4^2(900-60+1)$$

$$\equiv 4^2(26-60+1) \qquad 437\cdot 2 = 874$$

$$\equiv \dots \equiv 346 \mod \underbrace{437}_{\text{zašifrovaná zpráva}}$$

• dešifrování: $x^2 \equiv 346 \mod \underset{19\cdot 23}{\overset{}{437}}$

$$x^2 \equiv 346 \equiv -34 \equiv 4 \mod 19 \qquad 19\cdot 20 = 380$$

$$23\cdot 5 = 115$$

$$x^2 \equiv 346 = 116 \equiv 1 \mod 23$$

$$\boxed{\begin{aligned} x^2 &\equiv 4 \mod 19 \\ x^2 &\equiv 1 \mod 23 \end{aligned}} \qquad \begin{aligned} 19 &\equiv 3 \mod 4 \\ 23 &= 3 \mod 4 \end{aligned}$$

$$x \equiv \pm 4^{\frac{19+1}{4}} \equiv \pm 4^5 \equiv \pm 4\cdot 16^2$$

$$\equiv \pm 4(-3)^2 = \pm 36 = \pm 2 \mod 19$$

$$x \equiv \pm 1^{\frac{24+1}{4}} = \pm 1 \mod 23$$

$$\Rightarrow \boxed{\begin{aligned} x &\equiv \pm 2 \mod 19 \\ x &\equiv \pm 1 \mod 23 \end{aligned}}$$

$$\boxed{x = 19y \pm 2}$$

$$\Rightarrow 19y \pm 2 \equiv \pm 1 \mod 23$$

$$19y \equiv \mp 2 \pm 1 \mod 23 \quad | \cdot (-6)$$

$$(19,23) = 1 \rightsquigarrow 19\cdot(-6) + 23\cdot 5 = 1$$

$\uparrow$ Bezout

$$y \equiv -6\,(\underbrace{\mp 2 \pm 1}_{-1 \text{ a } +1}) \mod 23$$

$$y = 23\cdot r \pm 6$$

$$x = 19y \pm 2 = 19\cdot(23r \pm 6) \pm 2$$

$$= 437 \underbrace{\pm 114 \pm 2}_{\pm 116,\ \pm 112}$$

Závěr: poslána zpráva

tedy ± 116 nebo $\pm 117 \mod 437$

$$\underbrace{\pm 116}_{\parallel} = \pm 321$$

Trochu jinak: $x \equiv \pm 2 \mod 19$

$x \equiv \pm 1 \mod 23$

$$19 \cdot (-6) + 23 \cdot 5 = 1$$

Položme $x := \underbrace{19 \cdot (-6)}_{\equiv 1 \mod 23} \cdot (\pm 1) + \underbrace{23 \cdot 5}_{\equiv 1 \mod 19} \cdot (\pm 2)$

ElGamal kryptosystém

- Veřejná informace: prvočíslo p s primitivním kořenem g
- ~~Alice zveřejní náhodné $a \in \mathbb{Z}$ bez~~
- Bob

- Alice tajně zvolí $a \in \mathbb{Z}$ a pošle $g^a \bmod p$ Bobovi
- Bob tajně zvolí $b \in \mathbb{Z}$ a pošle $g^b \bmod p$ Alici
- Bob chce poslat zprávu M Alici ⇝ pošle $(g^b, M \cdot h^b) = (C_1, C_2)$ — šifrovaná zpráva

  kde $h = g^a$

  $h^b = (g^a)^b = g^{ab} = (g^b)^a$ — $= g^{ab}$
- Alice dešifruje: $\dfrac{C_2}{(C_1)^a} \bmod p$

<u>Př 5.4 (ii)</u> $p = 41$, $g = 11$

- Martin zvolí tajný klíč $a = 10$

⇝ Martin zveřejní $(41, 11, A)$

$A = 11^{10} \bmod 41$

• Honza mu poslal $(c_1, c_2) = (22, 6)$

Dešifrování z práce

$$M = \frac{c_2}{c_1^a} = \frac{6}{22^{10}} \mod 41$$

• $22^{10} = ((2 \cdot 11)^2)^5 = 2^{10} \cdot 121^5$

$\equiv 2^{10} \cdot (-2)^5 = -2^{15} \equiv$

$\equiv -(32)^3 \equiv -(-9)^3 \equiv$

$\equiv 9 \cdot 81 \equiv 9 \cdot (-1) \equiv -9 \mod 41$

$$M = \frac{6}{-9} \mod 41$$ $(-9) \cdot 9 \equiv 1 \mod 41$

$9 \cdot 9 = 81 \equiv -1 \mod 41$

$= 9 \cdot 6 = 54 \equiv \underline{\underline{13}} \mod 41$

(iii) RSA: $\left.\begin{array}{l} n = 33 \\ e = 3 \end{array}\right\}$ veřejný klíč

tajný klíč je $p = 3,\ q = 11$

• dešifrování zprávy $C = 7$

$$\Vert$$

$$M^e \bmod n$$

$$M = (M^e)^d \bmod n$$

kde $ed \equiv 1 \bmod \varphi(n)$

$e = 3,\ d = ?,\ \varphi(n) = \varphi(33) = 2 \cdot 10 = 20$

$\rightsquigarrow d = 7$ neboť $3 \cdot 7 \equiv 1 \bmod 20$

(obecněji použitím Bézoutovy rovnosti)

$$\to M = C^7 = 7^7 \equiv$$

$$\equiv 7 \cdot (49)^3 \equiv 7 \cdot 16^3 \equiv$$

$$\equiv 7 \cdot 2^{12} \equiv 7 \cdot 2^2 \cdot (2^5)^2 \equiv$$

$$\equiv 7 \cdot 4 \cdot (32)^2 \equiv 7 \cdot 4 \cdot (-1)^2$$

$$\equiv \underline{\underline{28}} \bmod 33$$

Booleovská alg. : $(K, \wedge, \vee, (\,)')$

splňujících mnoho vlastností

- komutativita
- asociativita
- distributivita $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$
- $\exists 1 \in K$ t. ž.

  $\forall A \in K: \; A \vee A' = 1$
- $\exists 0 \in K$ t. ž.

  $\forall A \in K: \; A \wedge A' = 0$

Př 6.1:

$$(A \wedge B \wedge C) \vee (A' \wedge B) \vee (A \wedge B \wedge C')$$

$$= (A \wedge B) \wedge \underbrace{(C \vee C')}_{1} \vee (A' \wedge B)$$

$$= (A \wedge B) \vee (A' \wedge B)$$

$$= B \wedge \underbrace{(A \vee A')}_{= 1} = B$$

(ii) Úplná disjunktní forma výroku

$$(B' \Rightarrow C) \wedge (A \vee C)$$

$B' \Rightarrow C$ totéž jako $B \vee C$

A	B	C	$B' \Rightarrow C$	$A \vee C$	
0	0	0	0	0	0
0	1	0	1	0	0
0	0	1	1	1	1
0	1	1	1	1	1
1	0	0	0	0	0
1	1	0	1	1	1
1	0	1	1	1	1
1	1	1	1	1	1

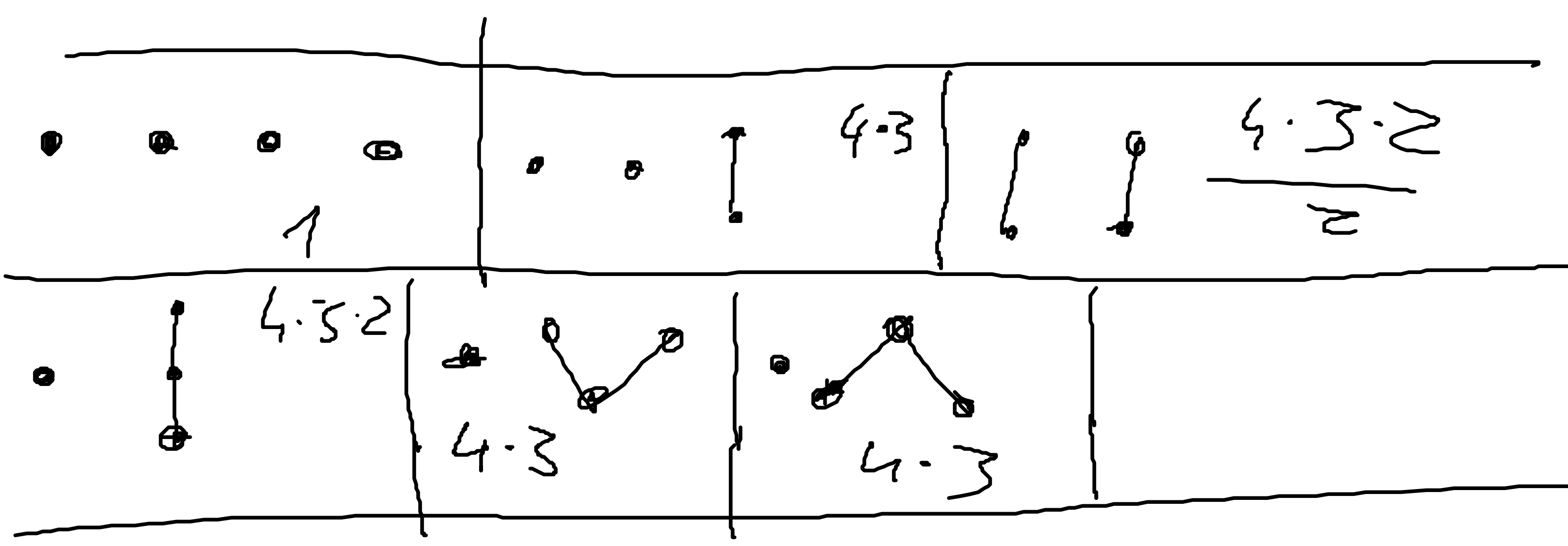
UDF: $(A' \wedge B' \wedge C) \vee (A' \wedge B \wedge C) \vee$
$\vee (A \wedge B \wedge C') \vee (A \wedge B' \wedge C) \vee$
$\vee (A' \wedge B' \wedge C')$

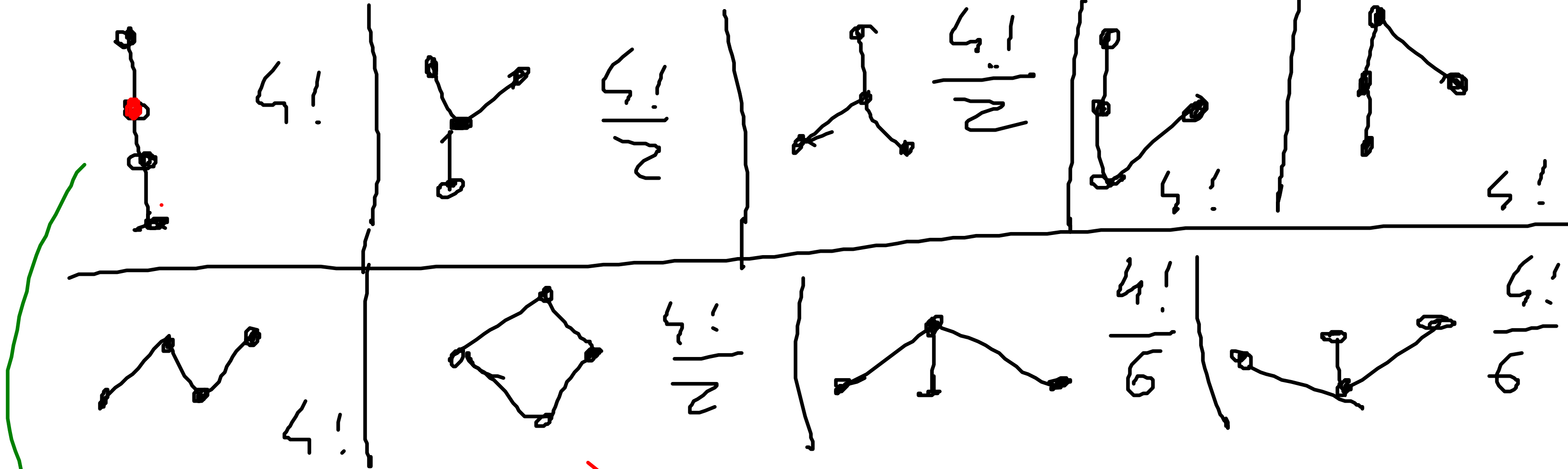
Teorie:

- Relace uspořádání je R, AS, T
  → horní/dolní závora
  supremum/infimum

- Usp. množina je svaz, jestliže ∀ dvouprvkové podm. má sup a inf

Cv. 2: usp. na čtyřprvkové mn. $M = \{a, b, c, d\}$





šňůry

Booleovská algebra $P(\{1,2\})$