Rabin – veřejný klíč: $n = p \cdot q$; $p, q \equiv 3 \pmod 4$

soukromý klíč: p, q

šifrování

$$M \pmod n \rightsquigarrow_D C \equiv M^2 \pmod n$$

$$M \equiv \sqrt{C} \pmod n \dashleftarrow C \pmod n$$

L 4 možnosti

řešíme $M^2 \equiv C \pmod{p \cdot q}$

$$\Downarrow$$

$$M^2 \equiv C \pmod p$$

$$M^2 \equiv C \pmod q$$

$$M^2 \equiv C \cdot C^{\frac{p-1}{2}} \equiv C^{\frac{p+1}{2}} \pmod p$$

$$\uparrow \quad \left(\frac{C}{p}\right) \quad \searrow$$

$$M^2 \equiv \left(C^{\frac{p+1}{4}}\right)^2$$

$$\Rightarrow M \equiv \pm C^{\frac{p+1}{4}} \pmod p$$

$M \equiv 327 \pmod{713}$

$\downarrow$

$C \equiv M^2 \equiv 5^2 \equiv 2 \pmod{23}$

$C \equiv M^2 \equiv (-14)^2 \equiv 10 \pmod{31}$

$31C \equiv 2 \cdot 31 \pmod{713}$

$23C \equiv 10 \cdot 23$

$8C \equiv 2 \cdot 31 - 10 \cdot 23$

$7C \equiv -4 \cdot 31 - 1 \cdot 23$

$C \equiv 6 \cdot 31 - 9 \cdot 23 \equiv -21 \equiv 692 \pmod{713}$

$M \equiv \sqrt{C} \equiv \pm C^6 \equiv \pm 2^6 \equiv \pm 5 \pmod{23}$

$M \equiv \sqrt{C} \equiv \pm C^8 \equiv \pm 10^8 \equiv \pm 14 \pmod{31}$

$10^8 \equiv 1 \cdot (10^2)^4 \equiv 1 \cdot (-7)^4 \equiv 1 \cdot ((-7)^2)^2$

$\equiv 1 \cdot (-13)^2 \equiv 169 \equiv 14$

$M \equiv -5 \quad (23)$
$M \equiv -14 \quad (31)$

$31M \equiv -5 \cdot 31$
$23M \equiv \quad -14 \cdot 23$
$8M \equiv -5 \cdot 31 + 14 \cdot 23$
$7M \equiv +10 \cdot 31 + 11 \cdot 23$
$M \equiv -15 \cdot 31 + 25 \cdot 23 \equiv +110 \quad (713)$

$5, 14 \rightsquigarrow -110$
$-5, -14 \rightsquigarrow 110$

4 odmocniny jsou
$\pm 15 \cdot 31 \pm 25 \cdot 23$

$M \equiv 5$
$M \equiv -14$
$\downarrow$
$M \equiv 15 \cdot 31 + 25 \cdot 23 \equiv 327$

$5, -14 \rightsquigarrow 327$
$-5, 14 \rightsquigarrow -327$

$M \rightsquigarrow C = M^2 \rightsquigarrow M' = M, -M, \underline{N, -N}$

$M \equiv C^{\frac{p+1}{4}} \quad (p)$ $\qquad N \equiv C^{\frac{p+1}{4}} \quad (p)$

$M \equiv C^{\frac{q+1}{4}} \quad (q)$ $\qquad N \equiv -C^{\frac{q+1}{4}} \quad (q)$

$M - N \equiv 0 \quad (p)$ $\qquad p \mid M-N$

$M - N \equiv 2C^{\frac{q+1}{4}} \not\equiv 0 \quad (q)$ $\qquad q \nmid M-N$

$\Rightarrow (p \cdot q, M-N)$

$= p$

$M \rightsquigarrow H_M \rightsquigarrow H_M^d$

M + podpis $\quad H_M^d$

$\downarrow \qquad\qquad \downarrow$

$H_M \quad \equiv \quad (H_M^d)^e$?

V: p prvočíslo; g prim. kořen

$43 \equiv g^a (p)$

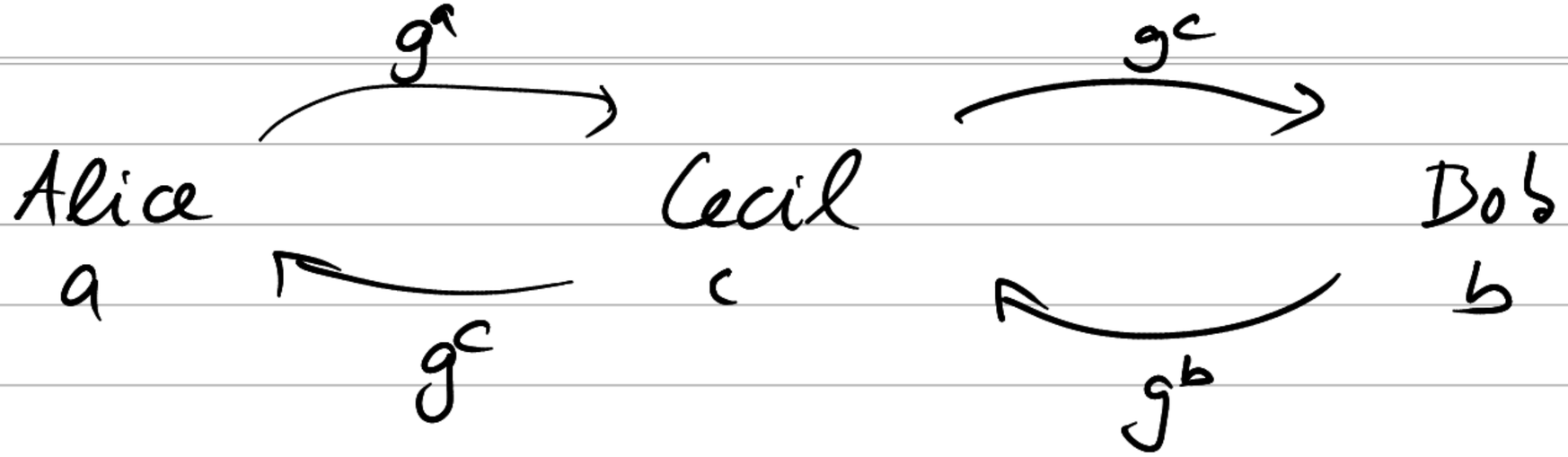
Alice (a) ⇄ Bob (b)

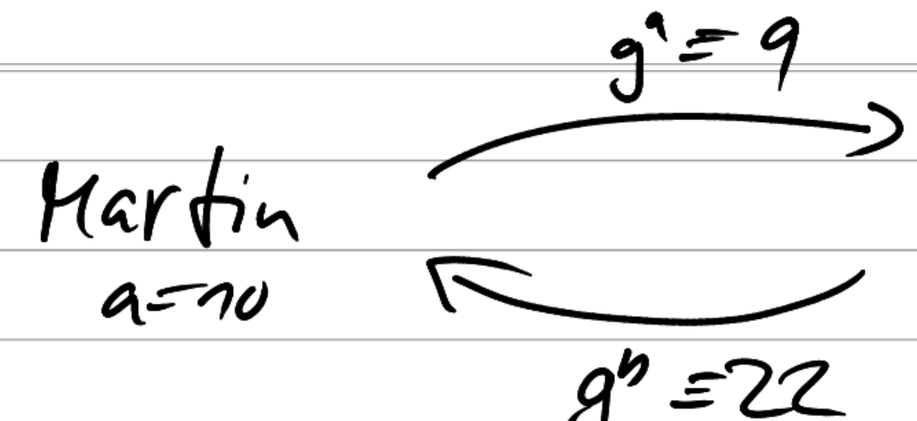
$31 \equiv g^b (p)$

$(g^b)^a \equiv g^{ab} \equiv (g^a)^b \qquad (p)$

$M \rightsquigarrow C \equiv g^{ab} \cdot M$

$C \rightsquigarrow M \equiv g^{ab\,-1} \cdot C$ tj. vyřeší se


g^a
g^c
Alice
a
Cecil
c
Bob
b
g^c
g^b



Monza
$b = ?$

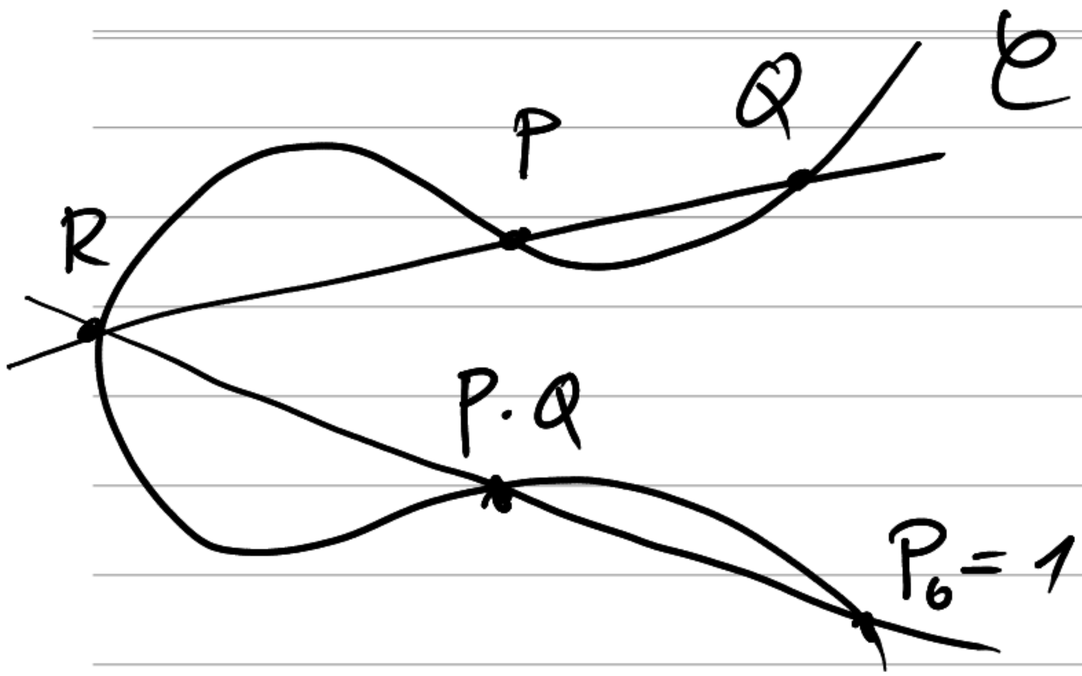
$p = 41$
$g = 11$

$g^{ab} \equiv 22^{10} \ (41)$
$\equiv 32$

$g^{ab} = ? = 32$

$6 \equiv C \equiv 32 \cdot M$ ⟵ M

$41M \equiv 0$
$32M \equiv 6 \quad (41)$
$9M \equiv -6$
$5M \equiv 24$
$4M \equiv 11$
$M \equiv 13$



$$P \cdot Q \cdot R = 1 \cdot \underline{(P \cdot Q)} \cdot R$$

$b_0 b_1 \dots b_{k-1}$

$(b_0, b_1, \dots, b_{k-1}) \in \mathbb{Z}_2^k$

$\mathbb{Z}_2 = \{0, 1\}$
$= \{0(2), 1(2)\}$

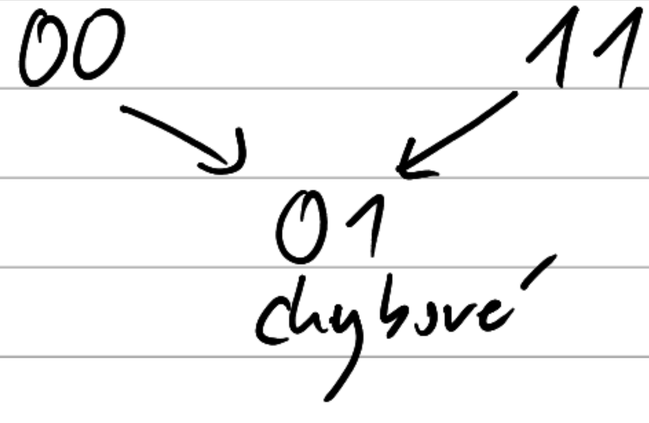
$b_0 + b_1 x + \dots + b_{k-1} x^{k-1}$

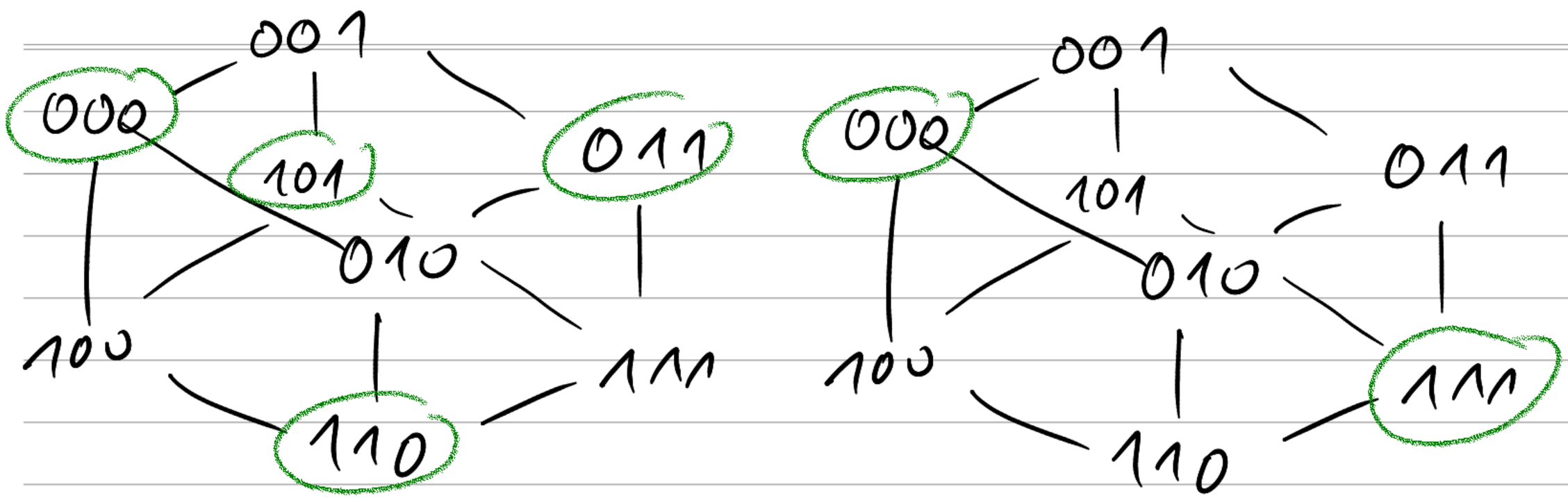
$b_0 b_1 \dots b_{k-1}$ ~~kódování~~ $\rightsquigarrow$ $\underbrace{c_0 \dots c_{n-k-1}}_{\text{kontrolní bity}} \underbrace{b_0 \dots b_{k-1}}_{\text{informační bity}}$

$\mathbb{Z}_2^k \xrightarrow{(n,k)\text{-kód}} \mathbb{Z}_2^n$

$\underline{c} b_0 \dots b_{k-1}$ kódové $\Leftrightarrow$ $c + b_0 + \dots + b_{k-1} \equiv 0$ (2)

$c \equiv b_0 + \dots + b_{k-1}$





$1+x^2$ je dělitelné $1+x$

$(x^2+1) : (x+1) = x-1$

x^2+x

$-x+1$

$-x-1$

2

$b_0 b_1 \dots b_{k-1} \longrightarrow c_0 \dots c_{n-k-1} b_0 b_1 \dots b_{k-1}$

$\underbrace{b_0 + b_1 x + \dots + b_{k-1} x^{k-1}}_{m(x)} \rightsquigarrow \underbrace{c_0 + \dots + c_{n-k-1} x^{n-k-1}}_{r(x)} + \underbrace{b_0 x^{n-k} + b_1 x^{n-k-1} + \dots + b_{k-1} x^{n-1}}_{x^{n-k} \cdot m(x)}$

$p(x) \mid r(x) + x^{n-k} \cdot m(x)$

$r(x) + x^{n-k} \cdot m(x) \equiv 0 \pmod{p(x)}$

$r(x) \equiv x^{n-k} \cdot m(x)$

$(k+1, k)$ – kód gen. $1+x$

kódová slova $1+x \mid v(x)$

$0 \rightsquigarrow 0 + 0x + 0 \cdot x^2$

$1 \rightsquigarrow 1 + 1x + 1 \cdot x^2$