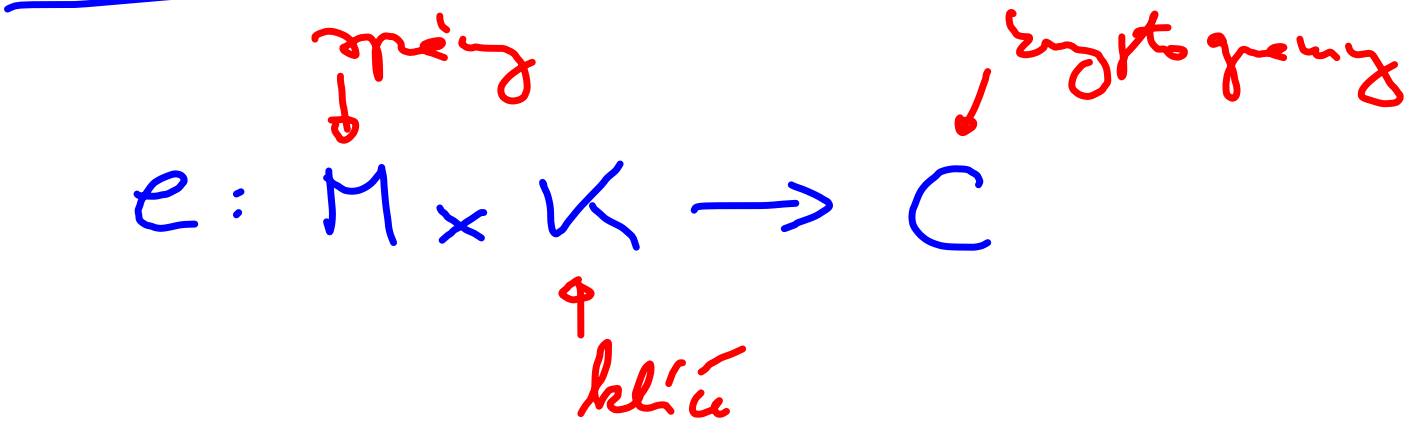
Šifrování: Claud E. Shannon



$$d : C \times K \to M$$

$$\forall k \in K \quad f_k(m) = e(m, k)$$

$$f_k^{-1}(f_k(m)) = m$$

Cyklické grupy $\mathbb{Z}_n$

$\gcd(m,n) = (m,n)$

Lemma: $(m,n)=1$ pak $\mathbb{Z}_{mn} = \mathbb{Z}_m \times \mathbb{Z}_n$.

Důk. $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$

$\mathbb{Z}_{mn}$ — $\mathbb{Z}_m$ — $\mathbb{Z}_n$

generátory: a — b — c

$f(a^r) = (b^r, c^r)$ (pokud $a^r = a^{r'}$, $r - r' = 0 \bmod mn$)

$\Rightarrow r - r' = 0 \bmod m$, $r - r' = 0 \bmod n$

$\Rightarrow$ dobře definováno

$f(a^r \cdot a^s) = f(a^{r+s}) = (b^{r+s}, c^{r+s}) =$
$= (b^r, c^r) \cdot (b^s, c^s) = f(a^r) \cdot f(a^s)$

f

$(a,b) + (c,d) =$

$(a+c, b+d)$

$a^r \in \ker f \Rightarrow a^r \xmapsto{f} (b^r, c^r) = (e, e)$

$\downarrow \mathbb{Z}_m \qquad \downarrow \mathbb{Z}_n$

$\Rightarrow r$ dělitelné m i n a

protože $(m,n) = 1$, je dělitelné i $m \cdot n$.

$\Rightarrow f$ injektivní. Z prvních pět pro $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n|$

$\Rightarrow f$ iso. □

Th. $\mathbb{Z}_{mn} = \mathbb{Z}_m \times \mathbb{Z}_n \iff (m,n) = 1$.

Př. V $\mathbb{Z}_m \times \mathbb{Z}_n$ není řád prvku větší než $\operatorname{lcm}(m,n)$.

$(a,b)^{\operatorname{lcm}(m,n)} = (e,e)$

Okruhy $\mathbb{Z}_{mn}$:

Th. $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ jako okruhy $\Leftrightarrow (m,n) = 1$.

Důk. $f([x]_{mn}) = ([x]_m, [x]_n)$

$f([x].[y]) = ([xy]_m, [xy]_n) = ([x]_m \cdot [x]_n) \cdot ([y]_m, [y]_n)$

$f([x]) \cdot f([y])$ =

Důsledek: $m = m_1 \cdot \ldots \cdot m_r$, $(m_i, m_j) = 1$

$\forall i \neq j$. Pak $\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$.

Čínská věta o zbytcích

($ax \equiv b \pmod n$) $\Leftrightarrow$ $ax + ny = b$, $x, y \in \mathbb{Z}$

Tvrzení: rovnice má řešení $x, y \in \mathbb{Z}$ $\Leftrightarrow (a,n) \mid b$.

Důk. $d = (a,n)$. Řeš. existují $\Rightarrow$ $d \mid b$. Naopak $b = \xi \cdot d$. Bezout $\Rightarrow$ ex. s, t

$as + nt = d$. $a\underbrace{s\xi}_{x} + n\underbrace{t\xi}_{y} = d \cdot \xi = b$ ☐

Th. $ax \equiv b \pmod n$ má řešení $\iff$

$d = (a,n) \mid b$. Navíc pak existuje právě

d nekongruentních řešení modulo n.

$[a][x] = [b]$ má d různých řešení

Th (Čínská věta) $m = m_1 \cdot m_2 \cdots m_r$,

$(m_i, m_j) = 1 \ \forall\, i \neq j$. Pak kongruence

$x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r}$

má vždy řešení v $\mathbb{Z}$. Navíc, je-li b řešení,

všechna řešení jsou tvaru $x \equiv b \pmod m$.

Věta. Pro $m = m_1 \cdot \ldots \cdot m_r$ je $\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$.

x je řešením $\Leftrightarrow f([x]_m) = ([a_1]_{m_1}, \ldots, [a_r]_{m_r})$

$[x]_m = f^{-1}(\cdot, \ldots, \cdot)$ □

Pozn. $y_i \cdot \frac{m}{m_i} \equiv 1 \pmod{m_i}$

$b = \sum_{i=1}^{n} a_i y_i \frac{m}{m_i}$

Eulerova funkce

$\varphi(n)$ = počet kladných $p \in \mathbb{Z}$, $p \leq n$, $(p,n)=1$.

Th. $\forall a \in \mathbb{Z}$, $a^{\varphi(n)} \equiv 1 \pmod n$, $(a,n)=1$.

Dk. $G \subset \mathbb{Z}_n$ multiplikativní podgrupa $\Rightarrow |G| = \varphi(n)$.

Fermatova malá věta $a^{|G|} = 1$. ∎

Vlastnosti $\varphi(n)$:

$\varphi(1) = 1$, p prvočíslo $\Rightarrow \varphi(p) = p-1$

$\varphi(p^\xi) = (p-1)\, p^{\xi-1}$.

Lemma $\varphi(mn) = \varphi(m)\varphi(n)$ pro $(m,n) = 1$.

Důk. $n < m = m_1 \cdot m_2$

$n \equiv n_1 \pmod{m_1}$ $\quad (n_1, m_1) = 1$

$n \equiv n_2 \pmod{m_2}$ $\quad (n_2, m_2) = 1$

m_1, m_2 dělitelná $\Rightarrow$ (Čínská věta) $\exists!\, n$ splňující ~~vlastnosti~~ a $(n,m) = 1$. □

$$n = p_1^{k_1} \cdot \dots \cdot p_r^{k_r}$$

$$\varphi(n) = (p_1 - 1) p_1^{k_1 - 1} \cdot \dots \cdot (p_r - 1) p_r^{k_r - 1}$$

$$= \prod_{i=1}^{r} \left(p_i^{k_i} - p_i^{k_i - 1} \right) \left(= n \cdot \prod_{p \mid n} \left(1 - \frac{1}{p} \right) \right)$$

Ex. $n = p \cdot q$ $\quad p, q$ prvočísla, $p \neq q$

$$\boxed{\varphi(n) = (p-1)(q-1)}$$

.

RSA : R. Rivest, A. Shamir, L. Adleman

- p, q "velká" prvočísla
- $n = p \cdot q$, $\varphi(n) = (p-1)(q-1) = \varphi$

veřejné

- vybere se e, $1 < e < \varphi$, $(e, \varphi) = 1$.
- spočte se jediné d, $1 < d < \varphi$, $e \cdot d \equiv 1 \pmod{\varphi}$

$(e, \phi) = 1 \Rightarrow \underbrace{a e}_{e \cdot d} + b\phi = 1$

veřejný klíč: n, e

neveřejný klíč: d

šifrování:

$m \in \mathbb{Z}$ -- zpráva v $[0, n-1]$

$c = m^e \pmod n$

---

dešifrování: — " —

$m = c^d \pmod n$

Proč to platí:

$n = p \cdot q$

$m \mapsto m^e \pmod n \mapsto (m^e)^d \pmod n$

$= m^{e \cdot d} \pmod n$

$e \cdot d = 1 + k\varphi$

$\gcd(m,p) = \begin{cases} 1 \\ p \end{cases} \Rightarrow m^{p-1} \equiv 1 \bmod p$ (Fermat)

mocníme na $\xi(q-1)$

mocníme na m

$m^{(p-1)(q-1)\cdot\xi + 1} \equiv m \pmod p$ platí

$\Rightarrow \left.\begin{aligned} m^{e\cdot d} &\equiv m \pmod p \\ m^{e\cdot d} &\equiv m \pmod q \end{aligned}\right\} \Rightarrow m^{e\cdot d} \equiv m \pmod{p\cdot q}$

✓

Rabin : $n = p \cdot q$

$m \mapsto c = m^2$

$c \mapsto m_1, \ldots, m_4$