Teorie kódování
Šifrování

Základní informace

Šifrování – Encryption (E)

Dešifrování – Decryption (D)

Abeceda $\mathbb{T}$, $|\mathbb{T}| = p$

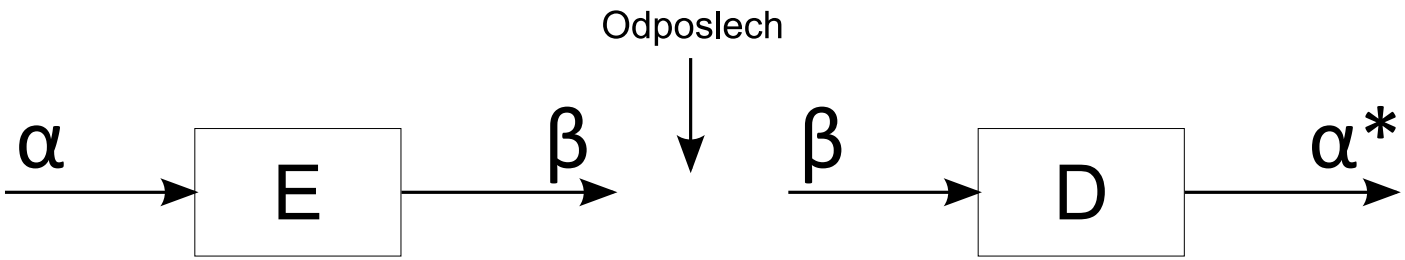
anglická abeceda	$p = 26$ ($p = 27$ . . . s mezerou)
anglická abeceda s číslicemi	$p = 36$ ($p = 37$ . . . s mezerou)

Očíslování znaků – $\mathrm{o} : \mathbb{T} \to \mathbb{Z}_p$

Šifrování: $\beta = \mathrm{E}(\alpha), \quad \mathrm{E} : \mathbb{T}^n \to \mathbb{T}^n$

Dešifrování: $\alpha^* = \mathrm{D}(\beta), \quad \mathrm{D} : \mathbb{T}^n \to \mathbb{T}^n$

$$\forall \alpha \in \mathbb{T}^n : \mathrm{D}(\mathrm{E}(\alpha)) = \alpha$$



Caèsarova metoda

segmenty délky 1

$$b = a \oplus c \quad \text{v } \mathbb{Z}_p, \quad c \ldots \text{konstanta}$$

dešifrování

$$b = a \oplus c \quad / \oplus -c$$
$$a^* = b \oplus -c$$

+ jednoduchost
– podle četnosti znaků snadno odhadneme konstantu c

Afinní šifra

segmenty délky 1

$$b = a \otimes c \quad \text{v } \mathbb{Z}_p, \quad c \ldots \text{konstanta}$$

dešifrování

$$b = a \otimes c \quad / \otimes c^{-1}$$
$$a^* = b \otimes c^{-1}$$

– snadná zranitelnost

\+ dobré výsledky v kombinaci s jinými metodami

Výpočet inverzního prvku

	p	0
	x	1
q_n	a_n	b_n

$$
\begin{aligned}
q_n &= \left\lfloor \frac{p}{x} \right\rfloor = \left\lfloor \frac{a_{n-2}}{a_{n-1}} \right\rfloor \\
a_n &= p - x \cdot q_n = a_{n-2} - a_{n-1} \cdot q_n \\
b_n &= b_{n-2} - b_{n-1} \cdot q_n
\end{aligned}
$$

Algoritmus končí $\Leftrightarrow a_n = 0$

Pokud $a_{n-1} = 1 \Rightarrow b_{n-1} = x^{-1}$

Během výpočtu vždy převedeme b_n do $\mathbb{Z}_p$

Vigenèrova šifra

segmenty délky n

$$\beta = \alpha \oplus \gamma(posun) \quad \text{v } \mathbb{Z}_p, \quad \gamma \ldots \text{kniha}$$
$$posun \ldots \text{posun v knize}$$

dešifrování

$$\beta = \alpha \oplus \gamma(posun) \quad / \oplus -\gamma(posun)$$
$$\alpha^* = \beta \oplus -\gamma(posun)$$

+ téměř nerozluštitelná šifra
– problémy s příliš krátkou knihou

Vigenèrova šifra

Řešení problému s příliš krátkou knihou

- periodické opakování krátké knihy

  $\gamma^* = \gamma\,\gamma\,\ldots\gamma$

- nesoudělné krátké knihy

$$\begin{aligned}
\gamma_1^* &= \gamma_1\,\gamma_1\,\ldots\gamma_1 & |\gamma_1| &= n_1\\
\gamma_2^* &= \gamma_2\,\gamma_2\,\ldots\gamma_2 & |\gamma_2| &= n_2\\
&\vdots & &\\
\gamma_k^* &= \gamma_k\,\gamma_k\,\ldots\gamma_k & |\gamma_k| &= n_k
\end{aligned}$$

$$\gamma^* = \gamma_1^* \oplus \gamma_2^* \oplus \cdots \oplus \gamma_k^*$$

Jsou-li délky knih $\gamma_1, \ldots, \gamma_k$ nesoudělné, je perioda knihy γ^* rovna $n_1 \cdot n_2 \cdot \ldots \cdot n_k$

Permutační šifra

segmenty délky n

$$\beta = \alpha \otimes \pi \qquad \text{v } \mathbb{Z}_p, \quad \pi \ldots \text{permutační matice}$$

dešifrování

$$\begin{aligned} \beta &= \alpha \otimes \pi \qquad / \otimes \pi^{-1} \text{ zprava} \\ \alpha^* &= \beta \otimes \pi^{-1} \end{aligned}$$

+ není nutné pracovat s konverzí do $\mathbb{Z}_p$
+ snadný numerický výpočet
+ pro velké n existuje velké množství permutačních matic ($n!$)
– pro malé n snadno napadnutelná

Stačí uchovávat permutační vektor místo matice.

Hillova šifra

segmenty délky n

$$\beta = \alpha \otimes \mathbf{H} \quad \text{v } \mathbb{Z}_p, \quad \mathbf{H} \ldots \text{plná matice}$$

předpoklady:

$\alpha \in \mathbb{Z}_p^n,\ n > 1,\ p \in \mathbb{P}$

$\mathbf{H} \in \mathbb{Z}_p^{n \times n}$

$|\mathbf{H}| \neq 0 \Rightarrow \exists \mathbf{H}^{-1}$

dešifrování

$$\beta = \alpha \otimes \mathbf{H} \quad / \otimes \mathbf{H}^{-1} \text{ zprava}$$
$$\alpha^* = \beta \otimes \mathbf{H}^{-1}$$

+ pro velké n je obtížně dešifrovatelná – mění znaky abecedy, jejich pořadí, ale i jejich četnosti
+ pro velké n je obtížné i při znalosti $\mathbf{H}$ vypočítat $\mathbf{H}^{-1}$

Hillova šifra + kniha

segmenty délky n z $(\alpha \oplus \gamma)$

$$\beta = (\alpha \oplus \gamma) \otimes \mathbf{H} \quad \text{v } \mathbb{Z}_p,$$

$\gamma \ldots$ dostatečně dlouhá kniha
$\mathbf{H} \ldots$ matice Hillovy šifry

dešifrování

$$\begin{aligned} \beta &= (\alpha \oplus \gamma) \otimes \mathbf{H} && / \otimes \mathbf{H}^{-1} \text{ zprava} \\ \beta \otimes \mathbf{H}^{-1} &= \alpha \oplus \gamma && / \oplus -\gamma \\ \alpha^* &= \beta \otimes \mathbf{H}^{-1} \oplus -\gamma \end{aligned}$$

Šifry s veřejným klíčem – RSA

Princip metody

- Máme zprávu vyjádřenou v $\mathbb{Z}_p$
- Bloky délky n převedeme na celá čísla
- Takto vzniklá čísla umocníme na vhodnou mocninu existující v $\mathbb{Z}_N$
  N je velké celé číslo, $N \geq p^n$, $N = a \cdot b, \quad a, b \in \mathbb{P}$
- Provedeme to s každým blokem.
- Pošleme zprávu elektronicky.
- Po přijetí zprávy odmocněním v $\mathbb{Z}_N$ získáme původní velké celé číslo.
- Vyjádříme ho v $\mathbb{Z}_p$ a získáme tak původní zprávu.

Šifry s veřejným klíčem – RSA

Pravidla pro volbu $a, b \in \mathbb{P}$: nesmějí to být

- malá prvočísla
- blízká prvočísla
- prvočísla důvěrně známá z literatury

RSA je nerozluštitelné, protože

- je velmi těžké rozložit velké číslo na prvočinitele
- roste-li výkonnost výpočetní techniky, stačí zvyšovat N

Odmocňování v tělese $\mathbb{Z}_p$

Věta: Buďte $p \in \mathbb{P}$, $\mathbb{Z}_p$ těleso. Je-li $\mathrm{nsd}(x, p-1) = 1$, pak $\forall x$ existuje $\sqrt[n]{x}$ v $\mathbb{Z}_p$ a počítá se

$$\sqrt[n]{x} \bmod p = x^m \bmod p,$$

kde $m \cdot n \bmod (p-1) = 1$.

(m je inverzní prvek k n v $\mathbb{Z}_{p-1}$: $m = n^{-1} \bmod (p-1)$)

Eulerova funkce

Eulerova funkce $\varphi(n)$

$\varphi(n)$ je počet přirozených čísel $x < n$, $\mathrm{nsd}(x, n) = 1$.

Platí: $p \in \mathbb{P} \Leftrightarrow \varphi(p) = p - 1$

Platí: $p, q \in \mathbb{P} \Rightarrow \varphi(p \cdot q) = (p - 1) \cdot (q - 1) = \varphi(p) \cdot \varphi(q)$

Věta: Pokud $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$, $n_i \in \mathbb{N}$, $p_i \in \mathbb{P}$, potom
$\varphi(n) = (p_1 - 1)p_1^{n_1 - 1} \cdot (p_2 - 2)p_2^{n_2 - 2} \cdot \ldots \cdot (p_k - 1)p_k^{n_k - 1}$.

Odmocňování v okruhu $\mathbb{Z}_p$

Věta: Buďte $p \notin \mathbb{P}$, $\mathbb{Z}_p$ okruh. Je-li $\mathrm{nsd}(x, \varphi(p)) = 1$, pak $\forall x$ existuje $\sqrt[n]{x}$ v $\mathbb{Z}_p$ a počítá se

$$\sqrt[n]{x} \bmod p = x^m \bmod p,$$

kde $m \cdot n \bmod \varphi(p) = 1$.

(m je inverzní prvek k n v $\mathbb{Z}_{\varphi(p)} : m = n^{-1} \bmod \varphi(p)$)

Zajímavá tvrzení o prvočíslech

Gauss, Fermatt : $2^a + 1 \in \mathbb{P} \Rightarrow a = 2^n$

Mersene : $2^a - 1 \in \mathbb{P} \Rightarrow a \in \mathbb{P}$

Věty umožňují hledat velká prvočísla.

Pokud platí závěr, musím ještě ověřit, že je to opravdu prvočíslo.