Teorija kodiranja in kriptografija - definicije, trditve in izreki

Oskar Vavtar
po predavanjih profesorice Arjane Žitnik

2021/22

Kazalo

1 Klasične šifre

Definicija 1.1. *Kriptosistem* je peterka $(\mathscr{B}, \mathscr{C}, \mathscr{K}, \mathscr{E}, \mathscr{D})$, kjer so

- $\mathscr{B}$ končna množica besedil,
- $\mathscr{C}$ končna množica kriptogramov,
- $\mathscr{K}$ končna množica ključev,
- $\mathscr{E} = \{E_k : \mathscr{B} \to \mathscr{C} \mid k \in \mathscr{K}\}$ družina kodirnih funkcij,
- $\mathscr{D} = \{D_k : \mathscr{C} \to \mathscr{B} \mid k \in \mathscr{K}\}$ družina dekodirnih funkcij,

tako, da velja

$$\forall e \in \mathscr{K}, \exists d \in \mathscr{K} : \; D_d(E_e(x)) \;=\; x, \quad \forall x \in \mathscr{B}.$$

Trditev 1.1. Vsaka kodirna funkcija $E_k \in \mathscr{E}$ je injektivna.

Šifra 1 (Cezarjeva/s pomikom)**.** a, b, c,. . . , ž označimo z 0, 1, 2,. . . , 24.

- $\mathscr{B} = \mathscr{C} = \mathscr{K} = \{0, 1, 2, \ldots, 24\} = \mathbb{Z}_{25}$
- kodiranje: $E_k(x) \equiv x + k \pmod{25}$
- dekodiranja: $D_k(y) \equiv y - k \pmod{25}$

Računamo torej v grupi $(\mathbb{Z}_{25}, +)$.

Algoritem 1 (Izčrpno iskanje ključev)**.**

- Podatki: $x \in \mathscr{B}, y \in \mathscr{C}$ za kriptosistem $(\mathscr{B}, \mathscr{C}, \mathscr{K}, \mathscr{E}, \mathscr{D})$
- Iščemo: $k \in \mathscr{K}$, za katerega je $E_k(x) = y$

for $k \in \mathscr{K}$ **do**
  if $E_k(x) = y$ **then return** k
  end if
end for

Deluje za majhne $|\mathscr{K}|$. Kriptosistem je *razbit*, če lahko ključ najdemo "dosti hitreje" kot s preverjanjem vseh ključev.

Razširjen evklidov algoritem

Izrek 1.1 (Osnovni izrek o deljenju)**.** Naj bosta $a \in \mathbb{Z}$ in $b \in \mathbb{N}$. Potem obstajata enolično določeni $q, r \in \mathbb{Z}$, $0 \leq r \leq b$, da velja

$$a = q \cdot b + r.$$

Algoritem 2 (Evklidov algoritem)**.**

- Vhod: $a, b \in \mathbb{N}$
- Izhod: $\texttt{gcd}(a, b)$

$r_0 = a$
$r_1 = b$
while $r_{n+1} \neq 0$ **do**
  $q_i = r_{i-1}/r_i$ ▷ "grdo" deljenje brez ostanka
  $r_{i+1} = r_{i-1} - q_i \cdot r_i$
end while
return r_n

Algoritem 3 (Razširjeni Evklidov algoritem)**.**

- Vhod: $a, b \in \mathbb{N}$
- Izhod: (r, s, t); $r = \texttt{gcd}(a, b)$, $s \cdot a + t \cdot b = \texttt{gcd}(a, b)$

$r_0 = a$, $s_0 = 1$, $t_0 = 0$
$r_1 = b$, $s_1 = 0$, $t_1 = 1$
while $r_{n+1} \neq 0$ **do**
  $q_i = r_{i-1}/r_i$ ▷ "grdo" deljenje brez ostanka
  $r_{i+1} = r_{i-1} - q_i \cdot r_i$
  $s_{i+1} = s_{i-1} - q_i \cdot s_i$
  $t_{i+1} = t_{i-1} - q_i \cdot t_i$
end while
return (r_n, s_n, t_n)

Trditev 1.2.

$$s_n \cdot a + t_n \cdot b \;=\; \mathtt{gcd}(a, b)$$

Definicija 1.2.

$$\begin{aligned} \mathbb{Z}_n^* &= \{i \in \{1, \ldots, n-1\} \mid i \perp n\} \;=\; \{i \in \{1, \ldots, n-1\} \mid \mathtt{gcd}(i, n) = 1\} \\ |Z_n^*| &= \varphi(n) \end{aligned}$$

Za $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ je

$$\varphi(n) \;=\; (p_1 - 1)p_1^{\alpha_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{\alpha_k - 1}.$$

Šifra 2 (Afina)**.**

- $\mathscr{B} = \mathscr{C} = \mathbb{Z}_{25}$, $\mathscr{K} = \mathbb{Z}_{25}^* \times \mathbb{Z}_{25}$
- ključ: $(a, b) \in \mathscr{K}$
- kodiranje: $E_{(a,b)}(x) = ax + b \pmod{25}$
- dekodiranje: $D_{(a,b)}(y) = a^{-1}(y - b) \pmod{25}$

$$D_{(a,b)}(E_{(a,b)}(x)) \;=\; a^{-1}\left((ax + b) - b\right) \;=\; x$$

Šifra 3 (Hillova)**.**

- $\mathscr{B} = \mathscr{C} = \mathbb{Z}_{25}^n$, $\mathscr{K} = \{\mathbf{A} \in \mathbb{Z}_{25}^{n \times n} \mid \det(\mathbf{A}) \in \mathbb{Z}_{25}^*\}$
- ključ: $\mathbf{A} \in \mathscr{K}$
- kodiranje: $E_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\mathbf{x} \pmod{25}$
- dekodiranje: $D_{\mathbf{A}}(\mathbf{y}) = \mathbf{A}^{-1}\mathbf{y} \pmod{25}$

$$D_{\mathbf{A}}(E_{\mathbf{A}}(\mathbf{x})) \;=\; \mathbf{A}^{-1}\mathbf{A}\mathbf{x} \;=\; \mathbf{x}$$