Teorija kodiranja in kriptografija

Ruslan Urazbakhtin

24. februar 2026

[verzija 24. februar 2026]

Kazalo

1 Kriptografija

1.1 Šifriranje

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

- $\mathcal{B}$ je končna množica besedil;
- $\mathcal{C}$ je množica kriptogramov (angl. ciphertext);
- $\mathcal{K}$ je množica ključev;
- $\mathcal{E} = \{E_k : \mathcal{B} \to \mathcal{C} \mid k \in \mathcal{K}\}$ je množica *šifrirnih* funkcij razreda $\mathcal{O}(n^p)$;
- $\mathcal{D} = \{D_k : \mathcal{C} \to \mathcal{B} \mid k \in \mathcal{K}\}$ je množica *dešifrirnih* funkcij razreda $\mathcal{O}(n^p)$.

Pri tem za kriptosistem mora veljati *pravilnost*, tj.

$$\forall m \in \mathcal{B} \,.\, \forall k \in \mathcal{K} \,.\, \exists k' \in \mathcal{K} \,.\, D_{k'}(E_k(m)) = m.$$

Opomba 1.2. Za vse $k \in \mathcal{K}$ je funkcija E_k injektivna (zakaj?), sledi da $|\mathcal{B}| \leq |C|$.

1.1.1 Varnost

Kerckhoffovo načelo. Kriptosistem naj bo varen, če tudi napadalec pozna sistem, ne pa skrivnega ključa.

1.2 Popolna tajnost

Označimo z

- $X_{\mathcal{B}}$ slučajno spremenljivko izbire besedila;
- $X_{\mathcal{C}}$ slučajno spremenljivko izbire kriptograma.

Predpostavimo, da je $\forall c \in \mathcal{C} \,.\, P(X_{\mathcal{C}} = c) > 0$.

Definicija 1.3. Kriptosistem *ima lastnost popolne tajnosti (LPT)*, če

$$\forall m \in \mathcal{B} \,.\, \forall c \in \mathcal{C} \,.\, P(X_{\mathcal{B}} = m \mid X_{\mathcal{C}} = c) = P(X_{\mathcal{B}} = m).$$

Lema 1.4. *Kriptosistem ima LPT* $\Leftrightarrow P(X_{\mathcal{C}} = c \mid X_{\mathcal{B}} = m) = P(X_{\mathcal{C}} = c)$

Dokaz. TODO □

Opomba 1.5. Če kriptosistem ima LPT, potem

$$\forall m_1, m_2 \in \mathcal{B} \,.\, \forall c \in \mathcal{C} \,.\, P_{k \leftarrow K}(E_k(m_1) = c) = P_{k \leftarrow K}(E_k(m_2) = c)$$

1.2.1 Vernamova šifra (OTP: one-time pad)

Naj bodo $\mathcal{B} = \mathcal{C} = \mathcal{K} = \{0, 1\}^\lambda$, $\lambda > 0$. Ključi izbiramo enakomerno naključno. Definiramo

- $E_k(m) = m \oplus k$;
- $D_k(c) = c \oplus k$.

Trditev 1.6. *Vernamova šifra je pravilna in ima LPT.*

Dokaz. TODO □

Vernamova šifra ima LPT, ampak tudi slabosti:

- Ključ lahko uporabimo samo enkrat:

$$E_k(m_1) = m_1 \oplus k,\ E_k(m_2) = m_2 \oplus k \Rightarrow m_1 \oplus m_2 \oplus (k \oplus k) = m_1 \oplus m_2.$$

  Iz $m_1 \oplus m_2$ ponavadi se da dobiti neko informacijo.
- Ključi so enako dolgi kot besedilo, kar povzroči $2x$ porabo prostora.

Izkaže se, da vsak kriptosistem, ki ima LPT, ima dolge ključe, saj

Trditev 1.7. *Če ima kriptosistem LPT, potem*

$$|\mathcal{B}| \leq |\mathcal{C}| \leq |\mathcal{K}|.$$

Dokaz. TODO □

Opomba 1.8. Recimo, da $\mathcal{B} = \{0,1\}^\lambda$ ter $\mathcal{K} = \{0,1\}^t$. Tedaj $|\mathcal{B}| = 2^\lambda$ in $|\mathcal{K}| = 2^t$. Če ima kriptosistem LPT, potem $|\mathcal{B}| \leq |\mathcal{K}| \Rightarrow \lambda \leq t$. Torej vsak ključ je dolg vsaj λ.

1.3 Tokovne šifre