Teorija kodiranja in kriptografija

Ruslan Urazbakhtin

23. februar 2026

[verzija 23. 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;
- $\mathcal{E} = \{\mathcal{E}_k : \mathcal{B} \to \mathcal{C} \mid k \in \mathcal{K}\}$ je množica *šifrirnih* funkcij razreda $\mathcal{O}(n^p)$;
- $\mathcal{D} = \{\mathcal{D}_k : \mathcal{C} \to \mathcal{B} \mid k \in \mathcal{K}\}$ je množica *dešifrirnih* funkcij razreda $\mathcal{O}(n^p)$.

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

$$\forall m \in \mathcal{B} \,.\, \forall k \in \mathcal{K} \,.\, \exists k' \in \mathcal{K} \,.\, \mathcal{D}_{k'}(\mathcal{E}_k(m)) = m.$$