

Kriptosistem

$\mathcal{B}$  ... besedila  
 $\mathcal{C}$  ... kriptogrami  
 $\mathcal{K}$  ... ključi  
 $\mathcal{E} = \{E_k : \mathcal{B} \rightarrow \mathcal{C}; k \in \mathcal{K}\}$  ... kodirne f.  
 $\mathcal{D} = \{D_k : \mathcal{C} \rightarrow \mathcal{B}; k \in \mathcal{K}\}$  ... dekodirne f.

Za vsak  $e \in \mathcal{K}$  obstaja  $d \in \mathcal{K}$

$$D_d(E_e(x)) = x \quad \forall x \in \mathcal{B}$$

Vsaka kodirna funkcija  $E_k \in \mathcal{E}$  je injektivna.

Klasični kriptosistem

Cezarjeva šifra

$$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{25}$$
$$E_k(x) \equiv x + k \pmod{25}$$
$$D_k(y) \equiv y - k \pmod{25}$$

Substitucijska šifra

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}, \quad \mathcal{K} = S(\mathbb{Z}_{25})$$

Ključ je permutacija  $\pi \in \mathcal{K}$

$$E_k(x) = \pi(x)$$
$$D_k(y) = \pi^{-1}(y)$$

Afina šifra

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}, \quad \mathcal{K} = \mathbb{Z}_{25}^* \times \mathbb{Z}_{25}$$

Ključ  $(a, b) \in \mathcal{K}$

$$K_{(a,b)}(x) = ax + b \pmod{25}$$
$$D_{(a,b)}(y) = a^{-1}(y - b) \pmod{25}$$

Vigenerjeva šifra

$$\mathcal{B} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{25}^n$$

Ključ  $\underline{k} \in \mathcal{K}$

$$K_{\underline{k}}(\underline{x}) = \underline{x} + \underline{k} \pmod{25}$$
$$D_{\underline{k}}(\underline{y}) = \underline{y} - \underline{k} \pmod{25}$$

Permutacijska šifra

*Simbolov ne nadomeščamo, ampak jih premešamo*

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}^n, \quad \mathcal{K} = S_n$$
$$K_{\pi}(\underline{x}) = \underline{x}_{\pi(1)} + \cdots + \underline{x}_{\pi(n)}$$
$$D_{\pi}(\underline{x}) = \underline{x}_{\pi^{-1}(1)} + \cdots + \underline{x}_{\pi^{-1}(n)}$$

Hillova šifra

$$\mathcal{B} = \mathcal{C} = \mathbb{Z}_{25}^n, \quad \mathcal{K} = \{A \in \mathbb{Z}_{25}^{n \times n} \mid \det(A) \in \mathbb{Z}_{25}^*\}$$

Ključ je matrika  $A \in \mathcal{K}$

$$K_A(\underline{x}) = A\underline{x} \pmod{25}$$
$$D_A(\underline{y}) = A^{-1}\underline{y} \pmod{25}$$

Bločne šifre

Kripotsistem  $(\mathcal{B}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$  je bločna šifra dolžine  $n$ , če je  $\mathcal{B} = \mathcal{C} = \Sigma^n$ , kjer je  $\Sigma$  končna abeceda.

Vsaka kodirna funkcija je ekvivalentna neki permutaciji  $\Sigma^n$ , njena dekodirna funkcija pa inverzu te permutacije.

Afina bločna šifra

$$\Sigma = \mathbb{Z}_m$$
$$\mathcal{K} = \{(A, \underline{b}); \ A \in \mathbb{Z}_m^{n \times n}, \det(A) \in \mathbb{Z}_m^*, \underline{b} \in \mathbb{Z}_m^n\}$$

$$E_{(A,\underline{b})}(\underline{x}) \equiv A\underline{x} + \underline{b} \pmod{m}$$
$$D_{(A,\underline{b})}(\underline{x}) \equiv A^{-1}\underline{x} - \underline{b} \pmod{m}$$

Teorija števil

Eulerjeva funkcija

Eulerjeva funkcija nam pove koliko je obrnlivih elementov v  $\mathbb{Z}_m$ .

$$|\mathbb{Z}_m^*| = \varphi(m)$$

Za  $n \in \mathbb{N}$  s paraštevskim razcepom  $n = p_1^{\alpha_1} \cdot \dots \cdot p_m^{\alpha_m}$  velja:

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \dots \cdot \varphi(p_m^{\alpha_m}) = n \prod_{p_k \in \mathbb{P}} \left(1 - \frac{1}{p_k}\right)$$

Euljerjev izrek:

$$\gcd(a, m) = 1 \Leftrightarrow a^{\varphi(m)} \equiv_m 1; a \in \mathbb{Z}_m^*$$

$$a, m \in \mathbb{N} \wedge \gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv_m 1$$

$$a^{\varphi(m)} = 1 \text{ v } \mathbb{Z}_m^*$$

**Mali Fermatov izrek:** če je  $m \in \mathbb{P}$  ( $\varphi(m) = m - 1$ ) in  $\gcd(a, m) = 1$ , potem:

$$a^{m-1} \equiv_m 1$$

Razširjen evklidov algoritem

*vhod:*  $(a, b)$   
 $(r_0, x_0, y_0) = (a, 1, 0)$   
 $(r_1, x_1, y_1) = (b, 0, 1)$   
 $i = 1$

*dokler*  $r_i \neq 0$ :  
 $i = i + 1$   
 $k_i = r_{i-2} / r_{i-1}$   
 $(r_i, x_i, y_i) = (r_{i-2}, x_{i-2}, y_{i-2}) - k_i(r_{i-1}, x_{i-1}, y_{i-1})$

*konec* zanke  
*vrni:*  $(r_{i-1}, x_{i-1}, y_{i-1})$

Naj bosta  $a, b \in \mathbb{Z}$ . Tedaj trojica  $(d, x, y)$ , ki jo vrne razširjen evklidov algoritem z vhodnim podatkomk  $(a, b)$ , zadošča:

$$ax + by = d \text{ in } d = \gcd(a, b)$$