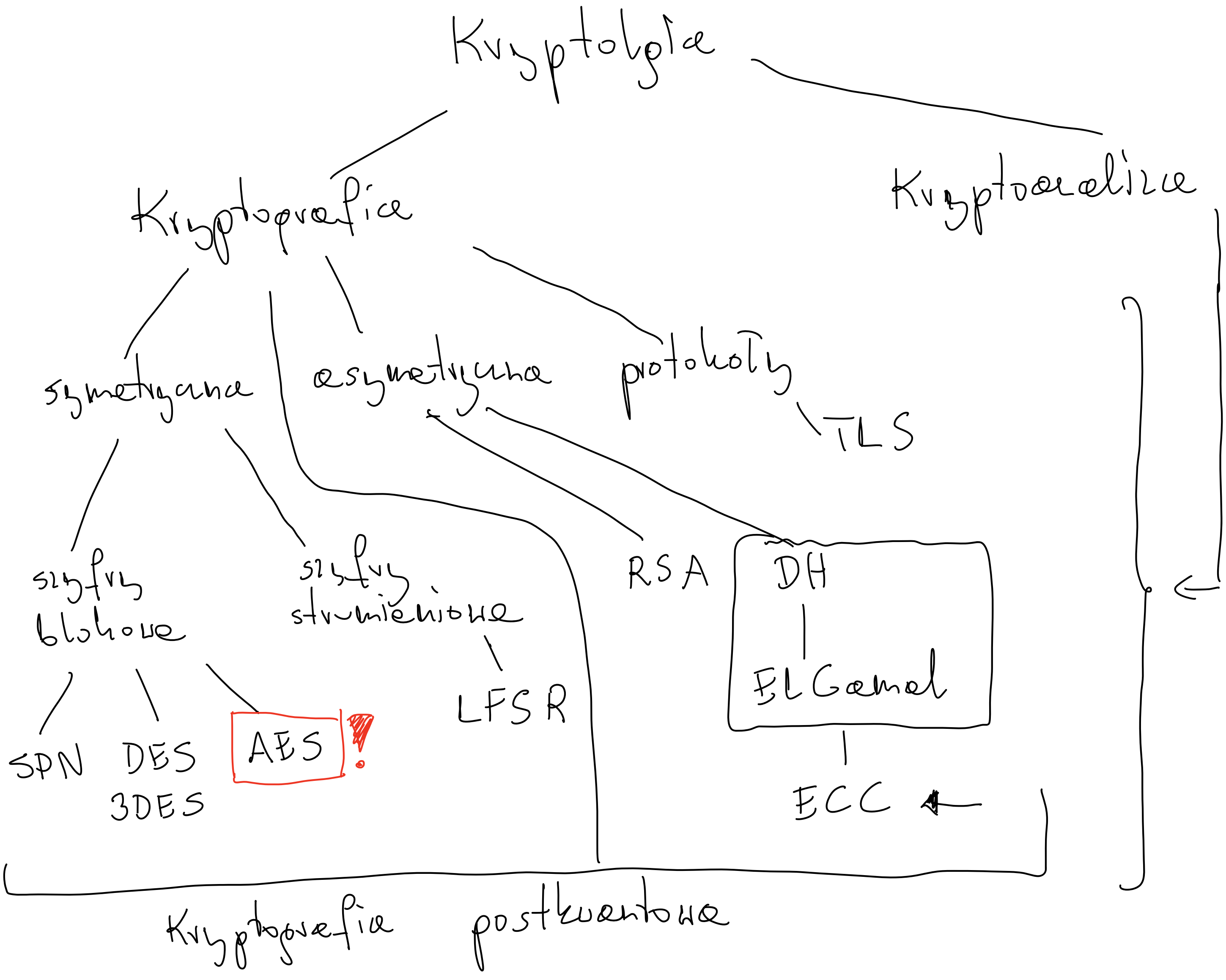
gregosiewicz.github.io / teaching /

Kryptografia w teorii i praktyce

D. Stinson, M. Paterson



Ewa — Oskar

Alicja x ⟶ Bob (Bogumił)

tekst jawny / plaintext — szyfrogram / ciphertext — Ewa

Alicja $x \rightsquigarrow y$ ⟶ $y \rightsquigarrow x$ Bob

szyfrowanie / encryption — K — ? — K — deszyfrowanie / decryption

kanał bezpieczny

klucz / key

Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

- $\mathcal{P}$ — zb. tekstów jawnych
- $\mathcal{C}$ — zb. szyfrogramów
- $\mathcal{K}$ — zb. kluczy
- $\mathcal{E}$ — zb. funkcji szyfrujących
- $\mathcal{D}$ — zb. f. deszyfr.

dowolne zbiory

$$\bigwedge_{K\in\mathcal{K}} \; \bigvee_{e_K\in\mathcal{E}} \; \bigvee_{d_K\in\mathcal{D}} \; \bigwedge_{x\in\mathcal{P}} d_K(e_K(x)) = x .$$

$$e_K : \mathcal{P} \to \mathcal{C}$$

$$d_K : \mathcal{C} \to \mathcal{P}$$

1. Szyfr przesunięciowy (szyfr Cezara)

$$\begin{matrix} A & B & C & \boxed{D} & \ldots & X & Y & Z \\ \downarrow & \downarrow & \downarrow & \downarrow & & & & \\ D & E & F & G & \ldots & A & B & C \end{matrix}$$

$\mathcal{P} = \{A, B, \ldots, Z\} = \{0, 1, \ldots, 25\} = \mathbb{Z}_{26} \leftarrow$ reszty mod 26

$\mathcal{C} = \mathbb{Z}_{26}$ $\qquad \boxed{\# \mathcal{K} = 26}$

$\mathcal{K} = \mathbb{Z}_{26}$

$x \in \mathcal{P}$ $\qquad e_K(x) = (x + K) \bmod 26$

$d_K(y) = (y - K) \bmod 26$

%

$-2 \% 26 = 24$

$-2 \% 26 = -2$

2. Szyfr podstawieniowy $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$

$\mathcal{K} =$ zbiór permutacji $\mathbb{Z}_{26}$

$\pi = K = (5, 7, 1, 3, 0, 19, 8, \ldots)$

$e_\pi(x) = \pi(x)$ $\qquad e_\pi(f) = e_\pi(5) = \pi(5) = 19 = T$

$d_\pi(y) = \pi^{-1}(y)$

$\# \mathcal{K} = 26! \sim 2^{88}$

2a) Szyfr afiniczny

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$

$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \text{NWD}(a, 26) = 1\}$

ISTNIEJE $\iff$ NWD$(a, 26) = 1$

$e_K(x) = e_{(a,b)}(x) = (ax + b) \bmod 26$

$d_K(y) = d_{(a,b)}(y) = a^{-1}(y - b) \bmod 26$

$\boxed{\text{el. odwrotny do } a \text{ w } \mathbb{Z}_{26} \quad a \cdot a^{-1} \equiv 1 \pmod{26}}$

rozszerzony alg. Euklidesa

$$\#\mathcal{K} = \underbrace{\varphi(26)}_{a} \cdot \underbrace{26}_{b} = 12 \cdot 26$$

f. Eulera

$$\varphi(26) = \varphi(2 \cdot 13) = \varphi(2)\varphi(13) = 1 \cdot 12 = \boxed{12}$$

3. Szyfr Vigenère'a XVI w.

$m \in \mathbb{N}$ $\quad \mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$

$K \in \mathcal{K}$ $\quad K = (k_1, k_2, \dots, k_m)$ $\quad \#K = (26)^m$

$$e_K(x_1, x_2, \dots, x_m) = (x_1 + k_1,\ x_2 + k_2,\ \dots,\ x_m + k_m) \mod 26$$

$$d_K(y_1, y_2, \dots, y_m) = (y_1 - k_1,\ y_2 - k_2,\ \dots,\ y_m - k_m) \mod 26$$

K = CIPHER $= (2, 8, 15, 7, 4, 17)$

4. Szyfr Hill'a XX w.

$m \in \mathbb{N}$ $\quad \mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ $\quad \mathcal{K}$ – zb. macierzy odwracalnych $m \times m$

$\boxed{\det K \neq 0 \mod 26}$

$$e_K(x) = e_K(x_1, x_2, \dots, x_m) = xK = [x_1\ x_2\ \cdots\ x_m]\,K$$

$$d_K(y) = d_K(y_1, y_2, \dots, y_m) = yK^{-1}$$

$$d_K(\overset{y}{e_K(x)}) = d_K(xK) = (xK)K^{-1} = x(KK^{-1}) = xI = x.$$