Algorytmy kryptograficzne

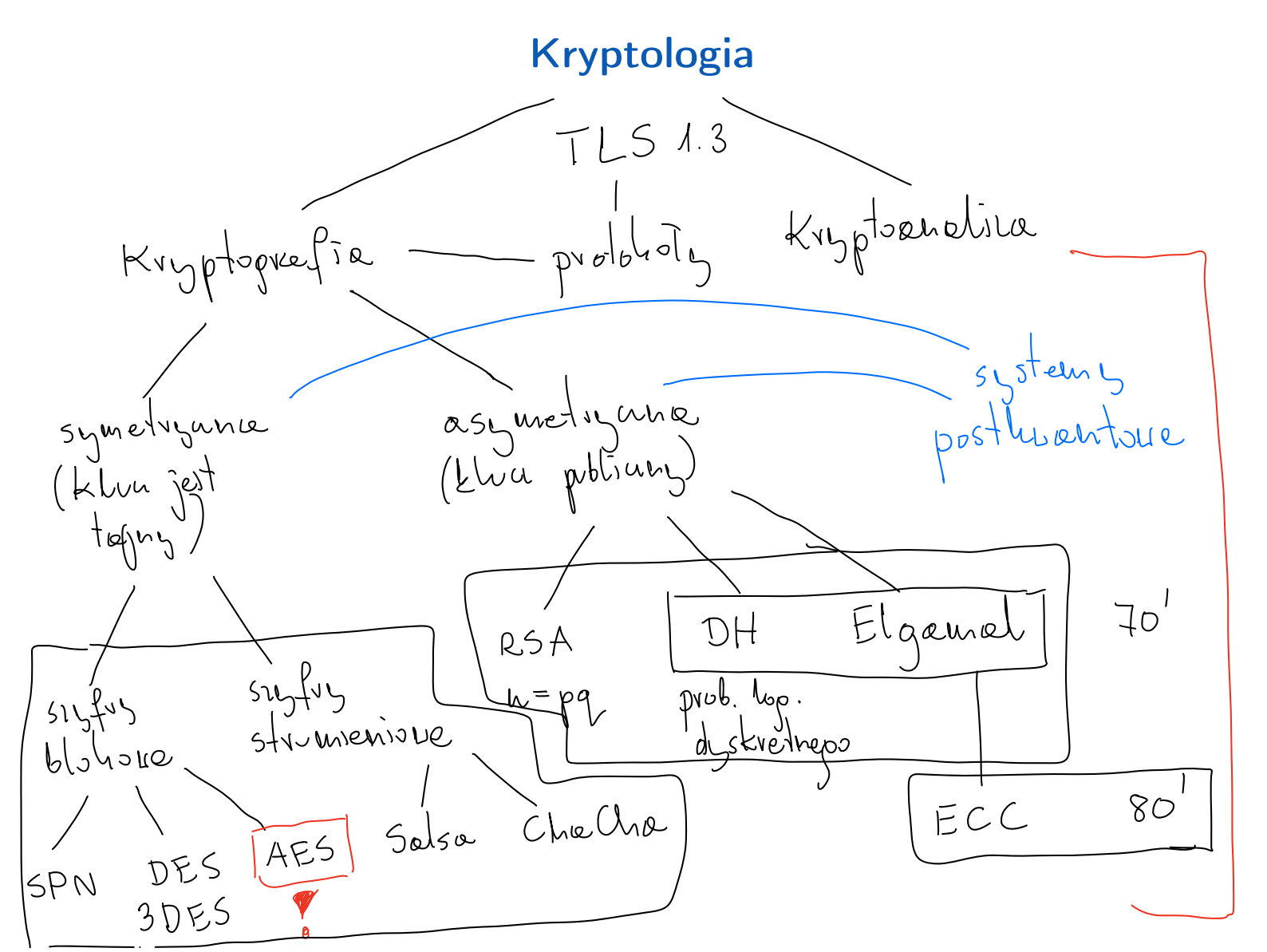
Adam Gregosiewicz

gregosiewicz.github.io/teaching/

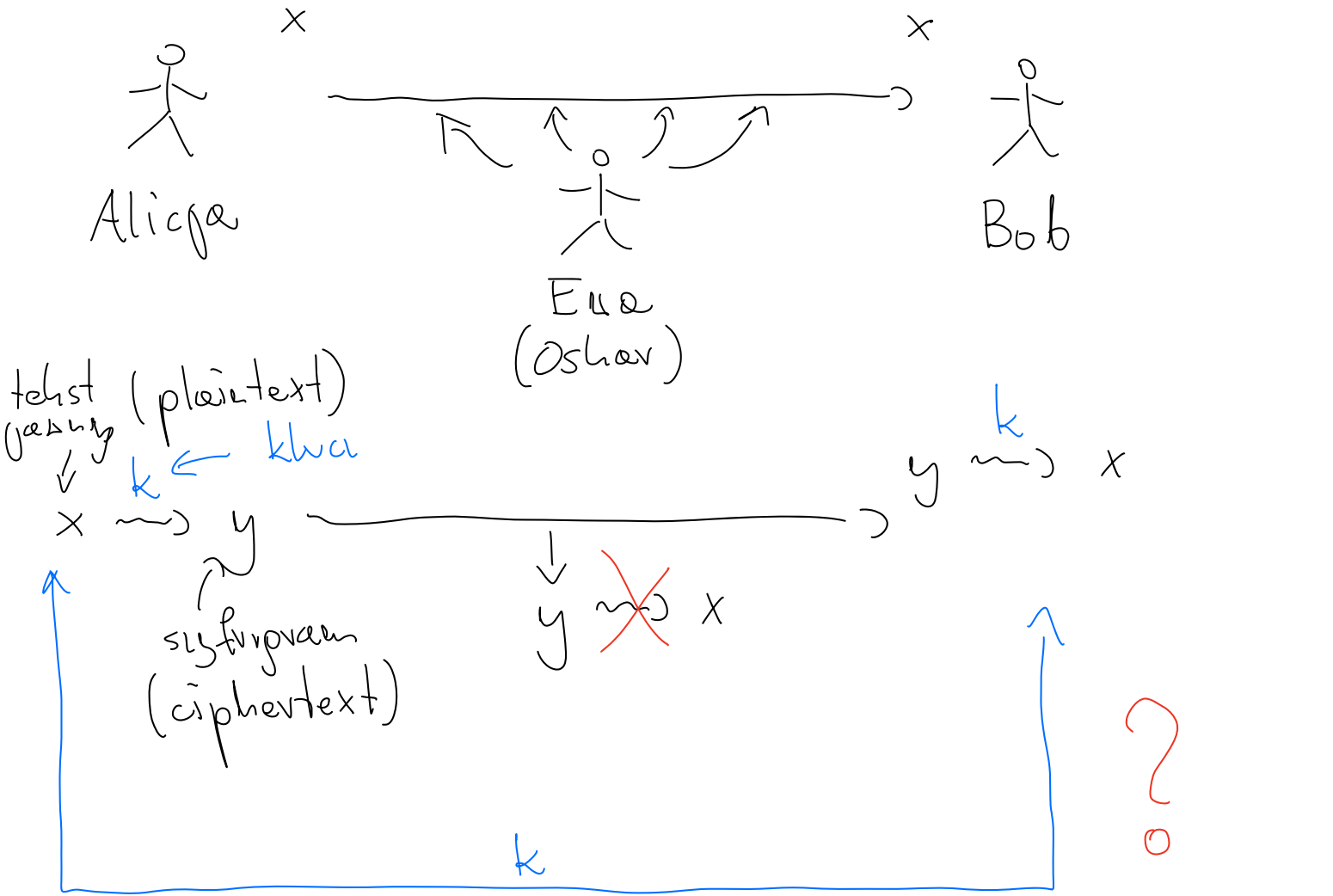
18 kwietnia 2026

Kryptografia w teorii i praktyce
D. Stinson, M. Paterson

Kryptologia



Model ogólny



Kryptosystem

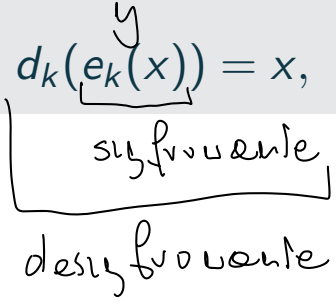
Kryptosystem

Kryptosystemem nazywamy piątkę (P, C, K, E, D), gdzie

- P jest zbiorem tekstów jawnych,
- C jest zbiorem szyfrogramów,
- K jest zbiorem kluczy,
- E jest zbiorem funkcji $P \to C$,
- D jest zbiorem funkcji $C \to P$,

przy czym dla każdego $k \in K$ istnieją funkcje $e_k \in E$ oraz $d_k \in D$ spełniające warunek

$$d_k(e_k(x)) = x, \qquad x \in P.$$



Szyfr przesuwający (Cezara)

a → D

b → E

⋮

a	b	c	...	z
0	1	2		25

Szyfr przesuwający (Cezara) (monoalfabetyczny)

Przyjmujemy $P = C = K = \mathbb{Z}_{26}$ oraz $\{0, 1, 2, \ldots, 25\}$

$$e_k(x) = x + k \pmod{26}, \qquad d_k(y) = y - k \pmod{26}.$$

$k \in K = \{0, 1, \ldots, 25\}$

Szyfr przesuwający (Cezara)

Przyjmujemy $P = C = K = \mathbb{Z}_{26}$ oraz

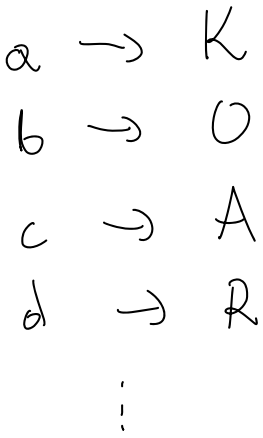
$$e_k(x) = x + k \pmod{26}, \qquad d_k(y) = y - k \pmod{26}.$$

$\rightsquigarrow$ Dla $k = 3$ otrzymujemy klasyczny szyfr Cezara:

$$\mathrm{a} \mapsto \mathrm{D}, \qquad \mathrm{b} \mapsto \mathrm{E}, \qquad \ldots \qquad \mathrm{z} \mapsto \mathrm{C}.$$

$\#K = 26$

Szyfr podstawieniowy



Szyfr podstawieniowy

Przyjmujemy

$\rightsquigarrow$ $P = C = \mathbb{Z}_{26}$,

$\rightsquigarrow$ K jest zbiorem wszystkich permutacji zbioru $\mathbb{Z}_{26}$.

$\mathbb{Z}_{26} \to \mathbb{Z}_{26}$

Dla $k = \pi \in K$ definiujemy

$$e_\pi(x) = \pi(x), \qquad d_\pi(y) = \pi^{-1}(y).$$

$$\pi: \begin{pmatrix} 0 & 1 & 2 & \dots & 25 \\ 3 & 18 & 13 & \dots & 2 \end{pmatrix}$$

$$e_\pi(c) = e_\pi(2) = \pi(2) = 13 = N$$

$$\#K = 26 \cdot 25 \cdot 24 \cdot \dots \cdot 2 \cdot 1 = 26!$$

Szyfr afiniczny

Przyjmujemy

$\rightsquigarrow \quad P = C = \mathbb{Z}_{26},$

$\rightsquigarrow \quad K = \mathbb{Z}_{26} \times \mathbb{Z}_{26}.$

Dla $k = (a, b) \in K$ definiujemy

$$e_k(x) = ax + b \pmod{26}, \qquad d_k(y) = a^{-1}(y - b) \pmod{26}.$$

$a = 3$ $\quad a^{-1}$ = element odwrotny do 3

? $\quad \square \cdot 3 = 1 \pmod{26}$

$$d_k(e_k(x)) = d_k(ax + b) = a^{-1}\big((ax + b) - b\big) =$$
$$= a^{-1}(ax + b - b) = a^{-1}ax = x.$$

a^{-1} istnieje $\iff$ NWD$(a, 26) = 1$

$$\#K = 26 \cdot 26 = \varphi(26) \cdot 26 = \varphi(2)\varphi(13) \cdot 26 = 12 \cdot 26 =$$
$$1 \quad 12$$
$$= 312$$

Szyfr afiniczny

Przyjmujemy

$\rightsquigarrow \quad P = C = \mathbb{Z}_{26},$

$\rightsquigarrow \quad K = \mathbb{Z}_{26} \times \mathbb{Z}_{26}.$

Dla $k = (a, b) \in K$ definiujemy

$$e_k(x) = ax + b \pmod{26}, \qquad d_k(y) = a^{-1}(y - b) \pmod{26}.$$

$\rightsquigarrow$ Dla $a = 1$ otrzymujemy szyfr Cezara.

Szyfr Vigenère'a

Szyfr Vigenère'a

Niech $m \in \mathbb{N}$. Przyjmujemy

$\rightsquigarrow \quad P = C = K = (\mathbb{Z}_{26})^m$.

Dla $k = (k_1, \ldots, k_m) \in K$ definiujemy

$$e_k(x) = (x_1 + k_1, \ldots, x_m + k_m) \pmod{26}, \qquad x = (x_1, \ldots, x_m)$$

i

$$d_k(y) = (y_1 - k_1, \ldots, y_m - k_m) \pmod{26}, \qquad y = (y_1, \ldots, y_m).$$

$$\#K = \underbrace{26 \cdot 26 \cdot \ldots \cdot 26}_{m} = 26^m$$

Szyfr Hilla

Niech $m \in \mathbb{N}$. Przyjmujemy

- $\rightsquigarrow$ $P = C = (\mathbb{Z}_{26})^m$,
- $\rightsquigarrow$ K jest zbiorem macierzy wymiaru $m \times m$ odwracalnych w $\mathbb{Z}_{26}$. Dla $k \in K$ definiujemy

$$e_k(x) = xk, \qquad d_k(y) = yk^{-1}.$$

$$(x_1, \dots, x_m) \begin{bmatrix} & k & \end{bmatrix}^{m \times m} = (y_1, \dots, y_m)$$

Szyfr Hilla

Niech $m \in \mathbb{N}$. Przyjmujemy

- $\rightsquigarrow$ $P = C = (\mathbb{Z}_{26})^m$,
- $\rightsquigarrow$ K jest zbiorem macierzy wymiaru $m \times m$ odwracalnych w $\mathbb{Z}_{26}$. Dla $k \in K$ definiujemy

$$e_k(x) = xk, \qquad d_k(y) = yk^{-1}.$$

- $\rightsquigarrow$ Macierz k jest odwracalna w $\mathbb{Z}_{26}$ wtedy i tylko wtedy, gdy

$$\mathrm{NWD}(\det k, 26) = 1.$$

Kryptoanaliza

Zasada Kerckhoffsa

Przeciwnik zna wszystkie szczegóły konstrukcji kryptosystemu, ale nie zna klucza. Bezpieczeństwo ma zależeć od tajności klucza, a nie od tajności algorytmu.

C. Shannon

Rodzaje ataków

- ⇝ Atak ze znanym szyfrogramem.
- ⇝ Atak ze znanym tekstem jawnym.
- ⇝ Atak z wybranym tekstem jawnym.
- ⇝ Atak z wybranym szyfrogramem.

Ewa zna y.

Ewa zna x i y.

Ewa może wybrać x i obliczyć y.

Ewa może wybrać y i obliczyć x.

Kryptoanaliza szyfru Cezara

$\rightsquigarrow$ Brute force: tylko 26 kluczy.

Kryptoanaliza szyfru podstawieniowego

$\#K = 26!$

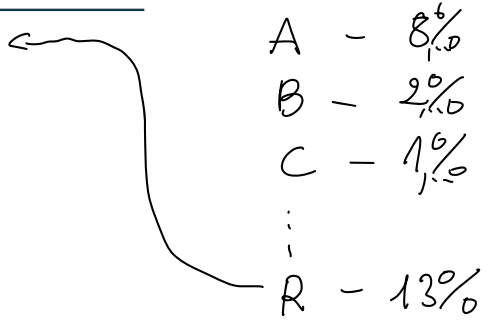
Kryptoanaliza szyfru podstawieniowego

- $\rightsquigarrow$ Brute force jest niepraktyczny: 26! kluczy.

Kryptoanaliza szyfru podstawieniowego

- ⇝ Brute force jest niepraktyczny: 26! kluczy.
- ⇝ Analiza częstości.

litera	prawdopodobieństwo
E	.127
T	.091
A	.082
O	.075
I	.070
N	.067
S	.063
H	.061
R	.060
⋮	⋮
Q	.001
Z	.001



Kryptoanaliza szyfru podstawieniowego

- ⇝ Brute force jest niepraktyczny: 26! kluczy.
- ⇝ Analiza częstości.

litera	prawdopodobieństwo
E	.127
T	.091
A	.082
O	.075
I	.070
N	.067
S	.063
H	.061
R	.060
⋮	⋮
Q	.001
Z	.001

- ⇝ Analiza digramów: TH, HE, IN.

Kryptoanaliza szyfru podstawieniowego

- ⇝ Brute force jest niepraktyczny: 26! kluczy.
- ⇝ Analiza częstości.

litera	prawdopodobieństwo
E	.127
T	.091
A	.082
O	.075
I	.070
N	.067
S	.063
H	.061
R	.060
⋮	⋮
Q	.001
Z	.001

- ⇝ Analiza digramów: TH, HE, IN.
- ⇝ Analiza trigramów: THE, ING, AND.

Kryptoanaliza szyfru afinicznego

- $\rightsquigarrow$ Brute force: tylko 312 kluczy.

Kryptoanaliza szyfru afinicznego

- $\rightsquigarrow$ Brute force: tylko 312 kluczy.
- $\rightsquigarrow$ Z analizy częstości zgadujemy obrazy dwóch częstych liter i rozwiązujemy układ równań

$$\begin{cases} ax_1 + b \equiv y_1 \pmod{26}, \\ ax_2 + b \equiv y_2 \pmod{26}. \end{cases}$$

Kryptoanaliza szyfru Vigenère'a

- $\rightsquigarrow$ Wyznaczamy długość słowa-klucza m.
- $\rightsquigarrow$ Test Kasiskiego.
- $\rightsquigarrow$ Indeks koincydencji.
- $\rightsquigarrow$ Po ustaleniu m każdą kolumnę łamiemy jak szyfr Cezara.

Test Kasiskiego

Szukamy w szyfrogramie jednakowych fragmentów długości co najmniej 3. Jeżeli ich początki są oddalone o δ, to jest duża szansa, że

$$m \mid \delta,$$

gdzie m oznacza długość słowa-klucza. Dla kilku odległości $\delta_1, \ldots, \delta_r$ badamy NWD$(\delta_1, \ldots, \delta_r)$.

Indeks koincydencji

Indeksem koincydencji tekstu x nazywamy prawdopodobieństwo, że dwa losowo wybrane znaki tekstu x są identyczne.

Indeks koincydencji

Indeksem koincydencji tekstu x nazywamy prawdopodobieństwo, że dwa losowo wybrane znaki tekstu x są identyczne.

Jeżeli litera i występuje f_i razy w tekście długości n, to

$$I_c(x) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}.$$

Indeks koincydencji

Indeksem koincydencji tekstu x nazywamy prawdopodobieństwo, że dwa losowo wybrane znaki tekstu x są identyczne.

Jeżeli litera i występuje f_i razy w tekście długości n, to

$$I_c(x) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}.$$

- $\rightsquigarrow$ Dla tekstu angielskiego zwykle $I_c \approx 0.065$.
- $\rightsquigarrow$ Dla tekstu losowego zwykle $I_c \approx 0.038$.

Przy poprawnej długości klucza kolumny szyfrogramu mają indeks bliski 0.065.