Kryptoanaliza

Zasada Kerckhoffa - przeciwnik nie wszystko o systemie, ale nie zna klucza

$e_k(x) = y$
$d_k(y) = x$

Ataki

→ - ze znanym szyfrogramem (Ewa zna y)
- ze znanym tekstem jawnym (Ewa zna x i y)
- z wybranym tekstem jawnym (Ewa może wybrać x i obliczyć y)
- z - II - szyfrogramem (Ewa może wybrać y i obliczyć x)

---

1) Cezar $\#\mathcal{K} = 26$
Przeszukiwanie klucza (brute-force)

Analiza częstości

PAQXZAACP.

A - 8
B - 2
C - 5
D - 2
⋮
P - 10
⋮
Z - 1

? ?

Angielski

e -	12.7%
t -	9.1%
a -	8.2%
o -	7.5%
⋮	

DIGRAMY	TRIGRAMY
th	the
he	ing
in	and
er	her
an	⋮
⋮	

2) Szyfr afiniczny, podstawieniowy, ...

2) Szyfr Vigenère'a

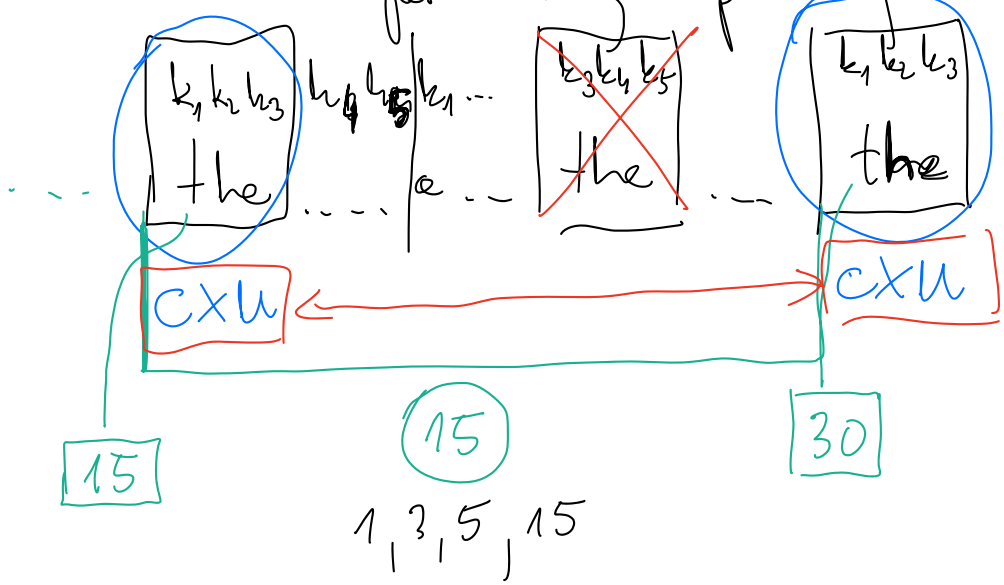
$k = (k_1, \dots, k_m)$

$k_1\ k_2\ k_3 \dots k_m\ k_1\ k_2 \dots k_m\ k_1 \dots$

$x_1\ x_2\ x_3 \dots x_m\ x_{m+1}\ x_{m+2} \dots x_{2m}\ x_{2m+1} \dots x_n$

I) Test Kasinshiego (Fryderyk Kasiński) 1863

Uwaga. Dwa bloki tekstu jawnego będą zaszyfrowane tak samo, o ile będą od siebie oddalone o δ pozycji, gdzie δ jest liczbą podzielną przez m.



$y_1 y_2 y_3 \dots y_n$

CXU 15, 20, 45, 10, ...

XAT 5, 25, 120, ...

$m \mid \delta_1, \delta_2, \dots \delta_N$

$m = NWD(\delta_1, \delta_2, \dots, \delta_N)$

→ Dwupoziom klucza m

II) Indeks koincydencji (William Friedman) 1920

X - skończony ciąg znaków $(A \dots Z)$

$I_c(X)$ - indeks koincydencji

$I_c(X) = P(\text{dwa losowe znaki w } X \text{ są równe})$

X

$x_1 x_2 x_3 \dots x_n$

A f_0 razy w X
B f_1 razy w X
C f_2
⋮
Z f_{25} …

$$I_c(X) = \frac{\binom{f_0}{2} + \binom{f_1}{2} + \dots + \binom{f_{25}}{2}}{\binom{n}{2}} = \frac{\sum_{i=0}^{25} \binom{f_i}{2}}{\binom{n}{2}} = \frac{\sum_{i=0}^{25} \frac{f_i(f_i-1)}{2}}{\frac{n(n-1)}{2}} =$$

$$= \sum_{i=0}^{25} \frac{f_i}{n} \cdot \frac{f_i - 1}{n-1}$$

n

A - $8/n$
B - $2/n$
C - $5/n$
D - $2/n$
⋮
P - $10/n$
⋮
Z - $1/n$

$\sum \frac{f_i}{n}$ = 1

$\approx P$

e - 12.7%
t - 9.1%
a - 8.2%
o - 7.5%
⋮

$\sum p_i$ = 1

prawdopodobieństwo, że losowa litera tekstu jest to i-ta litera

$$I_c(x) = \sum_{i=0}^{25} \frac{f_i}{n} \cdot \frac{f_i - 1}{n-1} \approx \sum_{j=0}^{25} p_j^2$$

(pod $\frac{f_i}{n}$ i $\frac{f_i-1}{n-1}$: ≈ p_i, ≈ p_i)

O ILE x JEST (ZASZYFROWANYM) TEKSTEM W JĘZYKU NATURALNYM

Dla języka angielskiego mamy $\sum_{i=0}^{25} p_i^2 = 0.065$

Jeżeli dla ciągu x mamy $I_c(x) \approx 0.065$, to jest duża szansa, że x jest (zaszyfrowanym) tekstem angielskim).

Dla losowego x mamy $I_c(x) \approx \sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 = 26 \cdot \frac{1}{26^2} = \frac{1}{26} \approx 0.038$

Dla $m = 1, 2, 3, 4, \ldots$ robimy szyfrowanie na części:

$m = 1$: $y_1 y_2 y_3 \ldots$ k_1 — $I_c(y) \approx 0.065$?

$m = 2$: $y_1 y_3 y_5 \ldots$ k_1 — $I_c(y_1 \ldots)$ ≈ 0.065?
$y_2 y_4 y_6 \ldots$ k_2 — $I_c(y_2 \ldots)$ ≈

$m = 3$: $y_1 y_4 y_7 \ldots$ k_1 — $I_c(y_1 \ldots)$
$y_2 y_5 y_8 \ldots$ k_2 — $I_c(y_2 \ldots)$ ≈ 0.065?
$y_3 y_6 y_9 \ldots$ k_3 — $I_c(y_3 \ldots)$

Znamy długość klucza m

n'

k_1	y_1 y_{m+1} ...
k_2	y_2 y_{m+2}
	⋮ ⋮
k_m	y_m y_{2m} ...

$\frac{f_0}{n'}, \frac{f_1}{n'}, \dots, \frac{f_{25}}{n'}$

$y_i = x_i + k_1 \pmod{26}$

$\frac{f_{0+k_1}}{n'}, \frac{f_{1+k_1}}{n'}, \dots, \frac{f_{25+k_1}}{n'}$

k_1 → jasny → zaszyfr.

$g = k_1$?

$$M_g = \sum_{i=0}^{25} \frac{f_{i+g}}{n'} \cdot p_i \approx \boxed{0.065}$$

$g = 0, 1, \dots, 25$