Tutorial 4 SK

06 October 2021 18:01

Historické šifrovanie a dokonalá tajnosť (perfect secrecy)

Formálna definícia šifrovacieho systému

P - množina správ (plaintext)

C - množina šifrovaných správ (cipher text)

K - množina kľúčov $\quad P \to C$

$e: (P \times K) \to C \qquad e_k : e(\_, k = k)$

$d: (C \times K) \to P \qquad d_k : d(\_, k = k)$

$\forall p, k \quad d_k(e_k(p)) = p \qquad e_k$ je injektívna.

CÉZAROV KRYPTOSYSTÉM

0 1 2 ... 25

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

C D E F G . . . . . A B

$P = \{A, \dots, Z\} = \{0, \dots, 25\}$

$C = \{A, \dots, Z\} = \{0, \dots, 25\}$

$K = \{A, \dots, Z\} = \{0, \dots, 25\}$

$e_k(i) = i + k \mod 26$

$d_k(j) = j - k \mod 26$

$H + C = 7 + 2 = 9 = J$

b b

0

.

.

.

25

$\{0, \dots, 25\} \to \{1, \dots, 25\}$

26!

POLYBIOUS CRYPTOSYSTEM

	A	B	C	D	E
F	A	B	C	D	E
G	F	G	H	I/J	K
H	L	M	N	O	P
I	Q	R	S	T	U
J	V	W	X	Y	Z

$= K$

$|k| = 25!$

$P = \{A, B, \dots, Z\}$

$C \subseteq \{A, B, \dots, Z\}^2$

Správa: 'CRYPTOLOGY'

C → FC P → L Y → JD

R → IB T → O

Y → JD O → G

MONOALFABETICKÁ ŠIFRA

EVERY Y YOU Y E E E E E

WIWGC RYC CXA VYC VYMW LGXUGWOO. WIWGC OSWL VYC QW BGAHSBAN.

E THERE E E E E E E E E

CWS SEWGW DHNN OSGWSPE XAS QWBXGW CXA YZ WIWG–NWZUSEWZHZU,

E E E E E E

WIWG–YOPWZRHZU, WIWG–HVLGXIHZU LYSE. CXA MZXD CXA DHNN ZWIWG

ET TO THE E THE D E

CWS SEWGW DHNN OSGWSPE XAS QWBXGW CXA YZ WIWG–NWZUSEWZHZU,
WIWG–YOPWZRHZU, WIWG–HVLGXIHZU LYSE. CXA MZXD CXA DHNN ZWIWG
UWS SX SEW WZR XB SEW FXAGZWC. QAS SEHO, OX BYG BGXV
RHOPXAGYUHZU, XZNC YRRO SX SEW FXC YZR UNXGC XB SEW PNHVQ.

W→E
E→H
S→T
X→O
G→R
I→V
C→Y
A→V

HILL CRYPTOSYSTEM

$P = \{A, \ldots Z\}^2$ (víceobecné n-tice)

$C = P$

K = množina všetkých 2×2 $(n \times n)$ matíc M_i invertibilných mod 26.

$$e_{M_i}(a\,b) = M_i \begin{pmatrix} a \\ b \end{pmatrix} \bmod 26 \qquad \det(M) = d$$

$$d_{M_i}(i\,j) = M_i^{-1} \begin{pmatrix} i \\ j \end{pmatrix} \bmod 26 \qquad \det(M^{-1}) = 1/d$$

$\det(M)$ musí byť invertibilný mod 26 $\gcd(\det(M), 26) = 1$

a je invertibilné mod n
$\Leftrightarrow \gcd(a, n) = 1$

$\det(M) \neq \{$párne čísla, 13$\}$

$$M = \begin{pmatrix} 1 & 3 \\ 3 & 4 \end{pmatrix} \qquad \det(M) = 4 \cdot 1 - 3 \cdot 3 = -5 = 21 \bmod 26$$

$M^{-1} \cdot M = \begin{pmatrix} 1 & 0 \end{pmatrix}$

$$M^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad M^{-1} \cdot M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\left.\begin{aligned} a.1 + b.3 &= 1 \\ a.3 + b.4 &= 0 \\ 1.c + 3d &= 0 \\ 3c + 4d &= 1 \end{aligned}\right| \Rightarrow \begin{aligned} a &= 20 \\ b &= 11 \\ c &= 11 \\ d &= 5 \end{aligned}$$

$$M^{-1} = \begin{pmatrix} 20 & 11 \\ 11 & 5 \end{pmatrix}$$

AC → 02

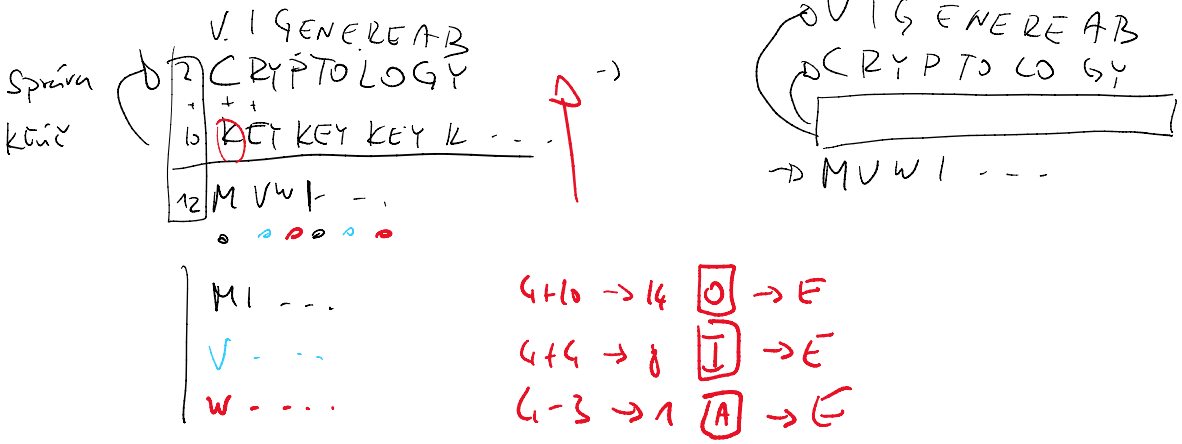
$$M\begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 \\ 2 \end{pmatrix} = (6\ 8) \qquad AC \to GI$$

CA → 20

$$M\begin{pmatrix} 2 \\ 0 \end{pmatrix} = = (2\ 6) \qquad CA \to CG$$

VIGENÉRE CRYPTOSYSTEM

Kľúč → ľubovoľné slovo dĺžky L



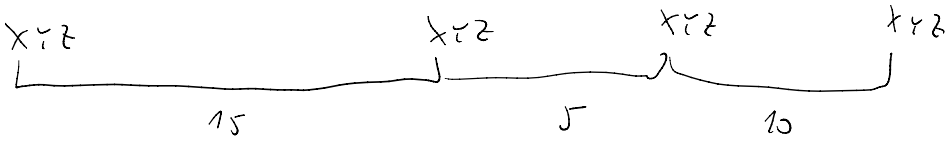
M I . . .
V . . .
W . . . .

4+10 → 14 O → E
4+4 → 8 I → E
4-3 → 1 A → E

KASISKI'S METHOD

nič sa opakuje v texte podstatne vo vzdialenosti slov

až sa opakuje v texte podstatne vo vzdialenosti, ktorá je násobkom K, tak pravdepodobná dĺžka šifra je L.



$L = 5$

FRIEDMANOVA

n - dĺžka textu

n_i - počet znakov "i" v texte

$n = \sum_{i=a\ldots z} n_i$

$$L \approx \frac{0{,}027 \cdot n}{(n-1)\cdot l - 0{,}038 \cdot n + 0{,}065} \qquad l = \sum_{i=0}^{25} \frac{n_i(n_i-1)}{n(n-1)}$$

PERFECT SECRECY – DOKONALÁ TAJNOSŤ

$P_r(P)$ – pravdepodobnosť výberu plaintextov (štatistika prirodzeného textu)

$P_r(K)$ – distribúcia tajného šifra (tipicky uniformná)

$P_r(C)$ – pravdepodobnosť ciphertextu (indukované $P_r(P)$ a $P_r(K)$)

$P_r(C=c \mid P=p)$ → pravdepodobnosť že p sa zašifruje ako c

$P_r(P=p \mid C=c)$ → pravdepodobnosť že c sa zašifruje ako p

Perfect secrecy ⇔

$$\forall p,c \quad P_r(P=p) = P_r(P=p \mid C=c)$$

$$\forall p, c \quad \boxed{Pr(P=p) = Pr(P=p \mid C=c)}$$

$P = \{x, y, z\}$

$C = \{a, b, c\}$

$K = \{1, 2, 3\}$

e_2	x	y	z
1	a	b	c
2	c	a	b
3	b	c	a

$Pr(K=1) = 1/3$ $\quad Pr(P=x) = 3/8$

$Pr(K=2) = 1/6$ $\quad Pr(P=y) = 1/8$

$Pr(K=3) = 1/2$ $\quad Pr(P=z) = 1/2$

$$Pr(C=c) = \sum_{i \in P} Pr(P=i) \sum_{k : e_2(i)=c} Pr(K=k) \quad \Downarrow$$

$$\boxed{\begin{aligned} Pr(C='a') &= Pr(P=x) \cdot Pr(K=1) + Pr(P=y) \cdot Pr(K=2) \\ &\quad + Pr(P=z) \cdot Pr(K=3) \\ &= 13/48 \end{aligned}}$$

$$Pr(C=c \mid P=p) = \sum_{k : e_2(p)=c} Pr(K=k)$$

$$\boxed{Pr(C='a' \mid P=x) = Pr(K=1) = 1/3}$$

$$\Rightarrow \exists c, p : P(P=p) \neq P(P=p)(C=c)$$

BAYESOV TEOREM

$$P(A \mid B) \cdot P(B) = P(A) \cdot P(B \mid A)$$

$P(A \mid B) = P(A, B)$ $\quad \Downarrow$ $\quad P(B \mid A) = P(A, B)$

$$P(A \mid B) = P(A) \Rightarrow P(B)\,P(B \mid A)$$

$P(K=1) = P(K=2) = P(K=3) = 1/3$ ✓

→ $P(P=x_1)\,P(P=x_2)\,P(P=x_3)$ → arbitrary

$$\forall c \quad P(C=c) = \sum_{i \in P} Pr(P=i) \cdot \sum_{k : e_k(i)=c} Pr(K=k)$$

$$= \sum_{i \in P} Pr(P=i) \cdot 1/3$$

$$= 1/3 \cdot \sum_{i \in P} Pr(P=i)$$

$$= 1/3$$

$$\forall c, p \quad P(C=c \mid P=p) = \sum_{k : e_k(p)=c} Pr(K=k)$$

$$= 1/3$$

⇓

$$\forall c, p \quad Pr(P=p) = Pr(P=p \mid C=c)$$ ✓✓