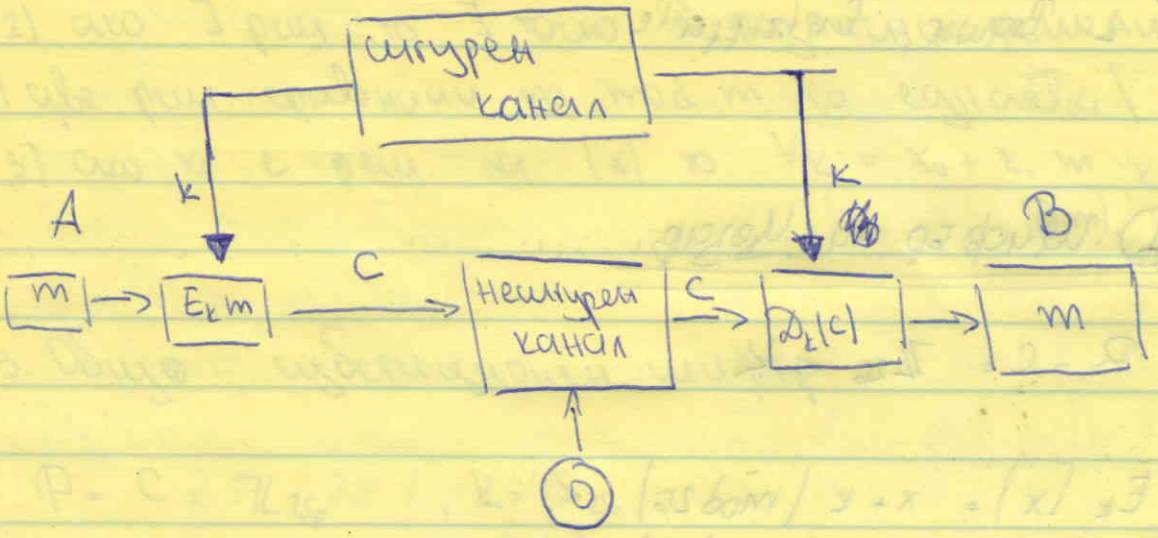
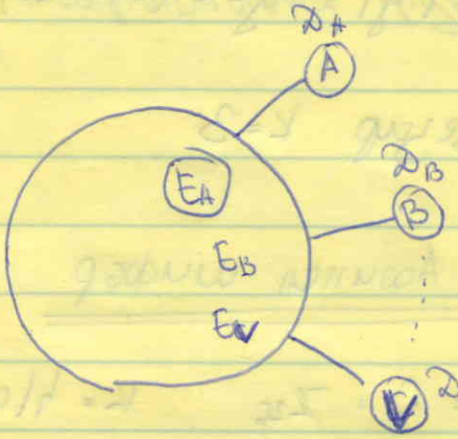
26.02.2014г. Криптография



$D_k(E_k(m)) = m$

система, в
която участват
потребители



Криптосистема: (P, C, K, E, D)

D.R. Stinson, Contemporary Cryptography

- P - множество открити текстове
- C - мн. от криптотекстове
- K - множество от ключове
- E - мн. от шифриращи трансформации $E_k: P \to C$
- D - мн. от дешифриращи трансф. $D_k: C \to P$

$\forall$ съобщения и $\forall$ ключ от

$\forall m \in P, \forall k \in K: D_k(E_k(m)) = m$

D. Kahn, The Codebreakers – история на криптографията '68г.
F. L Bauer, Entzifferte

(1) Шифър на Цезар

$R - C = \mathbb{Z}_{26} = K$

$E_k(x) = x + k \pmod{26}$
$D_k(y) = y - k \pmod{26}$

Цезар $k = 3$

(2.) Афинен шифър

$P = C = \mathbb{Z}_{26}$, $K = \{(a,b) \mid b \in \mathbb{Z}_{26}, a \in \mathbb{Z}_{26}^*\}$
$|K| = \varphi(26) \cdot 26 = 312$

$E_k(x) = ax + b \pmod{26}$
$D_k(y) = \frac{1}{a} y - \frac{b}{a} \pmod{26}$

$\frac{1}{9} = 3$ защото $3 \cdot 9 = 1$

$k = (7,3)$
$E_k(x) = 7x + 3 \pmod{26}$
$D_k(y) = 15y + 7 \pmod{26}$

$\overline{ax \equiv b \pmod{m}}$ *

1) реш. $\exists \Leftrightarrow (a, m) \mid b$

2) ако $\exists$ реш. то $\exists$ точно d различни решения;
(две реш. сравними по mod m са еднакви)

3) ако x_0 е реш. на (*) то $\forall k = x_0 + k \cdot \frac{m}{(a,m)}$, $k = 0, \ldots, d-1$

3. Общ субституционен шифър.

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

S_{26} симетричната група.

$\pi \in S_{26}$

$E_\pi(x) = \pi(x)$

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

$K = 26! \approx 4 \cdot 10^{26}$

CAESBY - написана без буквата е

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	

CRYPTOGRAPHY

4. Шифър на Playfair.

I = J (където има J се присвоява на I)

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

- открит текст - четна дължина
- разбиват се на двойки различни букви

M | SS | SS | PPI

MI SZ SI SZ SI PZ PI

- Ако имаме две букви в различен ред и стълб - правило на правоъгълник.

QR → BU

- Ако имаме две букви, ⓚ са в един ред - циклично дясно изместване.
- Ако имаме две букви, ⓚ са в един стълб, правим циклично изместване надолу.

CR YP TO GR AP HY

HI DI NG TU OA SX CS

5 Шифър на Vigenere.

- като простата субституция;

m - фикс. ест. число

$P = C = K = \mathbb{Z}_{26}^m = \{(a_1, \dots, a_m) \mid a_i \in \mathbb{Z}_{26}\}$

$k = (k_1, k_2, \dots, k_m)$

$E_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, x_3 + k_3, \dots, x_m + k_m) \bmod 26$

$D_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m) \bmod 26$

пример: THIS CRYPTOSYSTEM ....

19 7 8 18 2 17 24 15 19 14 18 24 18 19 4 12

CIPHERCIPHERCIPH

(2 8 15 7 4 17)(2 8 5 7 4 17) 2 8 15 7

21 15 23 25 6 8 0 23 24 21 22 15 20 1 19 19

YPXZGIAXIVWPUBTT

първият ред е позиция 1 x mod 26

II ред е позиция 2 x mod 26

събираме редовете и получаваме нова на новата дума стойност на позиция $n-1$,

Колкото по-дълъг е ключа, толкова по-сигурна е системата.

5. Шифър на L. Hill

$P = C = \mathbb{Z}_{26}^m$

$m \in \mathbb{N}$ - фиксирано

K = обратими матрици $m \times m$ над $\mathbb{Z}_{26}$

$E_K(x) = xK \pmod{26} \quad K \in K$

$D_K(y) = yK^{-1} \pmod{26}$

пример $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \quad K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

JULY → 9 20 11 24

$(9, 20) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (3, 4) \rightarrow DE$

$(11, 24) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (11, 22) \rightarrow LW$

JULY → DELW

$(3, 4) \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (9, 20) \rightarrow JU$

6. Пермутационен шифър.

$m \in \mathbb{N}$

$P = C = \mathbb{Z}_{26}^m$

$K = S_m$

$\pi \in K$

$E_\pi(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots x_{\pi(m)})$

$D_\pi(y_1, y_2, \ldots y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)} \ldots y_{\pi^{-1}(m)})$

пример:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{pmatrix}$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 2 & 4 \end{pmatrix}$$

she sells seas/he lls b

EES LSH/SALSES/LSHBLE

Симулация случаен шифър на шифъра на L. Hill

(SHESEL) $\begin{pmatrix} 0&0&1&0&0&0 \\ 0&0&0&0&0&1 \\ 1&0&0&0&0&0 \\ 0&0&0&0&1&0 \\ 0&1&0&0&0&0 \\ 0&0&0&1&0&0 \end{pmatrix}$ = EESLSH

6x5 - grid пишем хоризонтално - четем вертикално

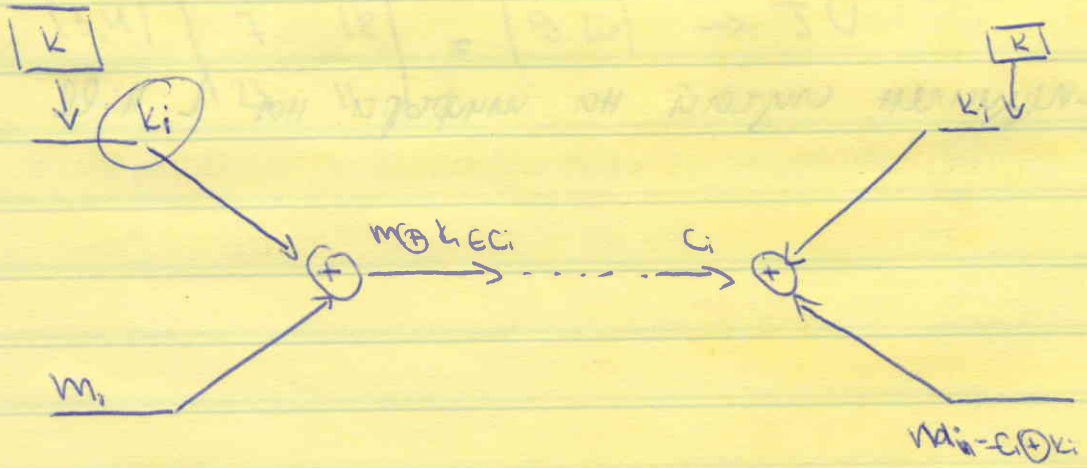
S	H	E	S	E
L	L	S	S	E
A	S	H	E	L
L	S	B	T	T
H	E	S	E	A
S	H	O	R	E

S	H	E	[illegible]	S	E
L	[illegible]	L	S	S	E
A	[illegible]	S	H	E	L
L	S	B	Y	[illegible]	T
H	E	[illegible]	S	E	A
[illegible]	S	H	O	R	E

SLALHSHLS ...

SLALH ...

7. Поточни шифри



A5/1 - име на шифър;

пример

$m = 4$

$z_{i+3} = z_{i+1} + z_i$ над $F_2 = \{0,1\}$

1	0	0	0
0	0	0	1
0	0	1	0
0	1	0	0
1	0	0	1
0	0	1	1
0	1	1	0
1	1	0	1
1	0	1	0
0	1	0	1
1	0	1	1
0	1	1	1
1	1	1	1
1	1	1	0
1	1	0	0
1	0	0	0

шифтва с една позиция надясно

- началното състояние

(1000 100 1101 0111)

15

тоз шифт регистър генерира период с дължина 15; ~~защото в 4 клетки има~~

8. Автоключ

$P = C = K = Z_{26}$

$z_1 = k$

$z_i = x_{i-1}$

z = ключова редица

$\| \quad (z_i)$

$E_z(x) = x + z \pmod{26}$

$D_z(y) = y - z \pmod{26}$

Нека $\boxed{k = 8}$

На първо място стои ключа, който е 8

R	E	N	D	E	Z	V	O	U	S
17	4	13	3	4	25	21	14	20	18
8	17	4	13	3	4	25	21	14	20
25	21	17	16	7	3	20	9	8	12
Z	V	R	Q	H	D	U	J	I	M

← събиране по mod 26

$25 - 8 = 17 \Rightarrow R$

$21 - 17 = 4 \Rightarrow E$

$17 - 4 = 13 \Rightarrow N$

9. Шифър на Vernam

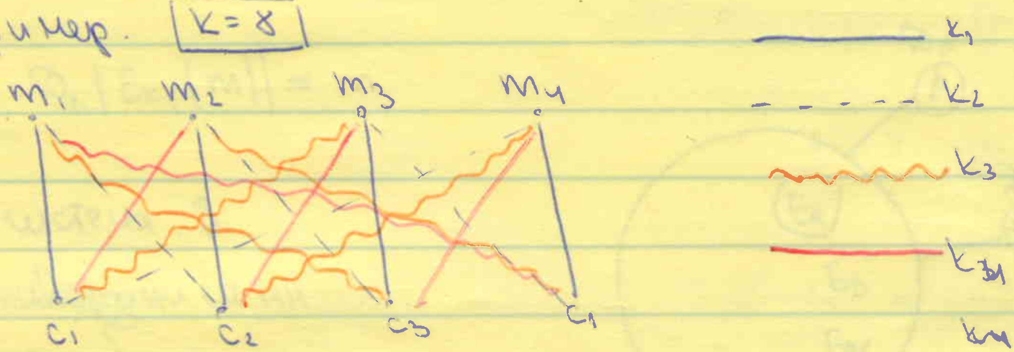
частен случай дължината на ключа е равен на дължината на открития текст

$P = C = K = \mathbb{Z}_k^n$

$E_k(x) = k \oplus x$

$D_k(y) = k \oplus y$

пример. $\boxed{K = 8}$



$p(m_1 | c_2) = \frac{1}{4}$

$p(m_1) = \frac{1}{4}$

$F_2[x] / (x^3 + x + 1)$

$0, 1, x, x+1$

$x^2, x^2+1, x^2+x, x^2+x+1$

$\boxed{x^3 = x + 1}$

$x^4 = x^2 + x$

$(x^2 + x)(x^2 + x + 1) \overset{\text{от } *}{=} x^2$

$(*)\ x^4 + \cancel{x^3} + \cancel{x^3} + \cancel{x^2} + \cancel{x^2} + x$

$x^2 + \cancel{x} + \cancel{x} = x^2$

$p(m_1 | c_2) = \frac{1}{4}$

$p(m_1) = \frac{1}{4}$