

Criptografie și Securitate

Tema 3

Ex1

a) Mesaj de criptat: SPRING IS HERE

Cheia 1: CIPHER

Cheia 2: KEY

1	2	3	4	5		
1	C	i	j	P	H	E
2	R	A	B	D	F	
3	G	K	L	N	N	
4	O	Q	S	T	U	
5	V	W	X	Y	Z	

Text Clar:	S	P	R	I	N	G	I	S	H	E	R	E
	43	13	21	12	35	31	12	43	14	15	21	15
	32	15	54	32	15	54	32	15	54	32	15	54

Cheie 2: K E Y K E Y K E Y K E Y

Text Criptat: 75 28 75 44 50 85 44 58 68 47 36 69

Pentru a crita acest mesaj am urmat pasii:

1. Am construit patratul lui Polybius pe baza primei chei, "CIPHER".
2. Am ignorat spatiiile din textul clar și am luat fiecare literă din acesta și am codificat-o pe baza liniei și coloanei pe care se află, (S=43, linia 4, coloana 3)
3. Am aplicat aceeași metodă și pentru cheia "KEY", și scriem sub literele din textul clar, literele din cheie, |

S
43
32
K

 |
4. Adunăm valorile literelor și obținem textul criptat
 $(43 + 32 = 75)$

b) Mesaj de criptat: 35 65 33 67 35 69 28 44 64 63

Cheia 1: DECRYPT

Cheia 2: CIPHER

	1	2	3	4	5
1	A	E	C	R	V
2	P	T	A	B	F
3	G	H	I/J	K	L
4	M	N	O	Q/S	
5	U	V	W/X	Z	

Text criptat: 35 65 33 67 35 69 28 44 64 63

Cheia 2: 13 33 21 32 12 14 13 33 21 32

Text Clar: 22 32 12 35 23 55 15 11 43 31

Pentru a decripta mesajul am mers în sens invers:

1. Am construit pătratul lui Polybius pe baza primei chei, „DECRYPT”.

2. Am codificat literele din cheia 2, „CIPHER”, pe baza linilor și coloanelor din tabel și le-am sortis sub mesajul criptat. ($\begin{matrix} 35 \\ 13 \\ c \end{matrix}$)

3. Am scăzut valorile literelor cheii din mesajul criptat și am obținut valorile literelor din textul clar. ($35 - 13 = 22$)

4. Traducem aceste valori pe baza pătratului și obținem textul clar. ($22 = T$)

Ex2 Pentru criptanaliza cifrului Nihilist, vom începe cu determinarea lungimii cheii, lucru posibil prin descoperirea unui tirar de valori numerice mici sau mari. Astfel, împărțim textul în blocuri de dimensiunea egală cu lungimea cheii pe care o bănuim și după câteva încercări va apărea un model. De asemenea, numerele din textul cifrat se pot obține doar din câteva combinații, care se pot afla prin brute force. În plus, numerele mici sau mari au un număr limitat de opțiuni,

În numerele 22 și 110 sunt speciale, deoarece arată că litera din cheie este aceeași cu cea din alfabet, în locațiile respective. Totodată, putem restrânge opțiunile pentru o valoare, prin găsirea valorilor minime și maxime care o compun ($76 = \underbrace{2} + \underbrace{55}$). Ne mai putem aiza și de la min max.

Numeră care ar cauza a două cifre 2/0 pentru că oferă varianțe limitate ($2 = 1+1; 10 = 5+5$).

O altă slabiciune este că se realizează un adăos normal, ci nu modular, ceea ce înseamnă că valori mari (> 100) se obțin din litere de pe ultima linie din pătrat, adică a cincea.

Ex3 a) Mesaj de criptat - ENCRYPTION

	1	2	3	4	5	ENCRYPTION									
1	B	G	W	K	Z	3	2	4	5	5	2	5	3	3	2
2	Q	P	N	D	S	5	3	2	5	3	2	1	1	2	3
3	I	J	O	A	X	E									
4	F	C	L	U	M	3	2	4	5	5	2	5	3	2	5
5	T	H	Y	V	R	0	M	H	Y	0	Y	S	0	B	N

Mesaj criptat: OMHYOYSOBN

Pentru a crita mesajul am urmat pasii:

1. Am construit pătratul lui Polybius pentru bifid standard.
2. Am luat fiecare literă din textul clar și am codificat-o pe baza liniei și coloanei pe care se află și vom scrie valoarea pe o coloană. (

1	2	3	4	5
6	7	8	9	0

)
3. Am unit cele două linii cu cifre și am format grupuri de câte două și am identificat litera corespunzătoare și astfel, am obținut mesajul criptat. (

3	2
0	1

)

b) Mesaj de decriptat: r d r b d p m n s v y r g r l s

I

	1	2	3	4	5
1	B	G	W	K	Z
2	Q	P	N	A	S
3	J	O	A	X	E
4	F	C	L	U	M
5	T	H	Y	V	R

4 2 3 5 1 6 3 4 5 2 1 6 2 3 5 1 6

5 5 | 2 4 5 5 | 1 1 | 2 4 | 2 2 | 4 5 | 2 2 | 2 5 | 5 4 | 5 3 | 2 2 | 1 2 | 5 5 | 4 3 | 2 5

5	5	2	4	5	5	1	1	2	4	2	2	4	5	2	2
2	5	5	4	5	3	2	2	1	2	5	5	4	3	2	5
H	R	S	U	R	Y	G	G	Q	C	S	S	U	Y	P	S

II

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

4 2 | 1 4 | 4 2 | 1 2 | 1 4 | 3 5 | 3 2 | 3 5 | 4 3 | 5 1 | 5 4 | 3 5 | 2 2 | 4 2 | 3 1 | 4 3

4 2 | 1 4 | 4 2 | 1 2 | 1 4 | 3 5 | 3 2 | 3 5
4 3 | 5 1 | 5 4 | 3 5 | 2 2 | 4 2 | 3 1 | 4 3

THE QUICK BROWN FOX

Pentru a decripta mesajul am urmat pasii:

1. Am construit patratul lui Polyleius pentru Bifid standard, insa am obtinut un rezultat fara sens, asa ca am trecut in patrat literele in ordine alfabetica.

2. Am luat fiecare litera din textul criptat si am codificat-o pe baza liniei si coloanei pe care se afla si am seris valorile pe o singura linie. ($\begin{matrix} r & d & r \\ 55 & 24 & 55 \end{matrix}$)

3. Am impartit valorile in grupuri de doua si am impartit la jumata linia respectiva in doua linii, iar cea de-a doua linie am trecut-o sub prima. ($\begin{matrix} 4 & 2 \\ 4 & 3 \end{matrix}$)

4. Am decodificat literele pe baza valorilor de ne
coloana ei ($\frac{4}{4}$) și astfel, am obținut textul clar.

Ex 4 Cifrul Bifid reprezintă un cifru automic pentru perioada în care a apărut decarece comleină patratul lui Polybius cu transpoziția și folosește fractionarea pentru difuzie.

Pentru criptanaliză vom considera Σ ca fiind alfabetul și cheia ca fiind sub forma următoare:

	0	1	---	$n-1$
0	$\Gamma_{0,0}$	$\Gamma_{0,1}$	---	$\Gamma_{0,n-1}$
1	$\Gamma_{1,0}$	$\Gamma_{1,1}$	---	$\Gamma_{1,n-1}$
$n-1$	$\Gamma_{n-1,0}$	$\Gamma_{n-1,1}$	---	$\Gamma_{n-1,n-1}$

Astfel, în funcție de paritatea lungimii blocurilor de text criptarea se realizează după schemele:

• impar

Γ_0	Γ_1	Γ_2	---	Γ_{e-3}	Γ_{e-2}	Γ_{e-1}
x_0	x_1	x_2	---	x_{e-3}	x_{e-2}	x_{e-1}
y_0	y_1	y_2	---	y_{e-3}	y_{e-2}	y_{e-1}



T_0	T_1	---	$T_{\frac{e-3}{2}}$	$T_{\frac{e-1}{2}}$	$T_{\frac{e+1}{2}}$	---	T_{e-1}
x_0	x_2	---	x_{e-3}	x_{e-1}	y_1	---	y_{e-2}
x_1	x_3	---	x_{e-2}	y_0	y_2	---	y_{e-1}

• par

Γ_0	Γ_1	Γ_2	---	Γ_{e-3}	Γ_{e-2}	Γ_{e-1}
x_0	x_1	x_2	---	x_{e-3}	x_{e-2}	x_{e-1}
y_0	y_1	y_2	---	y_{e-3}	y_{e-2}	y_{e-1}



T_0	T_1	---	$T_{\frac{e-2}{2}}$	$T_{\frac{e}{2}}$	$T_{\frac{e+2}{2}}$	---	T_{e-1}
x_0	x_2	---	x_{e-2}	y_0	y_2	---	y_{e-2}
x_1	x_3	---	x_{e-1}	y_1	y_3	---	y_{e-1}

Azadar, o modalitate de a detecta perioada pe care o notăm p (blocurile de lungime fixă) este prin statistică cu bigrame pe literele din textul cifrat separate prin jumătate din perioadă. Pentru perioade pare, literele din textul cifrat la o distanță de $p/2$ sunt influențate de 2 litere din textul clar, iar pentru celul impar,

literele aflate la distanță $n/2$ rotunjite prin adăugare sau prin scădere) sunt influențate de 3 litere din textul clar.

De asemenea, pentru o perioadă fixă, numărul de cifrebi bid este mai mic decât numărul de tabele chei.

O altă metodă de a determina această perioadă este prin determinarea și analizarea frecvențelor perechilor de litere egale la o distanță dată d , adică determinarea numărului de apariții ale tiparului $\Sigma^{d-1} z$ și realizarea graficului cu rezultat în fundie de d . Forma obținută ar trebui să fie aproximativ o sinusoidă cu perioadă cantică. Putem întâlni următoarele distribuții: distribuția frecvențelor digrafurilor omogene neconectate și distribuția deviației standarde pentru digrafurile neconectate.

Ceea ce am spus până acum se bazează pe cunoașterea unor rîse din textul clar, dar putem determina cheia conform probabilităților diferențe calculate pe baza liniilor și coloanelor. De asemenea, putem observa pe linii și coloane, pentru o perioadă mai mare ca 5, dacă un grup de 5 litere se repetă în textul clar într-o poziție impară relativ la perioada atunci are loc următoarea repetiție în textul cifrat ABW?XCD și ABY?ZCD, unde W și Y aparțin aceliasi linii, iar X și Z aparțin aceliasi coloane a tabelului cheii.

--	T_{2i-1}	T_{2i}	T_{2i+1}	T_{2i+2}	T_{2i+3}	--
--	X_{2i-1}	X_{2i}	X_{2i+1}	X_{2i+2}	X_{2i+3}	--
--	Y_{2i-1}	Y_{2i}	Y_{2i+1}	Y_{2i+2}	Y_{2i+3}	--



\dots	T_i	T_{i+1}	T_{i+2}	\dots	$\frac{T_{l+i-1}}{2}$	$\frac{T_{l+i-1}+i}{2}$	$\frac{T_{l+i-1}+i+1}{2}$	\dots	$\text{ende } l = \text{dimen-}$
\dots	x_{2i}	x_{2i+2}	x_{2i+4}	\dots	*	y_{2i+1}	y_{2i+3}	\dots	siunea blocului
\dots	x_{2i+1}	x_{2i+3}	*	\dots	y_{2i}	y_{2i+2}	y_{2i+4}	\dots	

Totodată se mai pot analiza perechile diagonale sau transpuse.