Criptografie și Securitate

Tema 2

Exc 1 a) Mesaj de criptat: MESAJ CRIPTAT

Cheia: KEY

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

Text Criptat: 33 12 44 14 31 21 43 31 4 145 14 45

b) Mesaj de decriptat: 43 23 21 11 23 44

Cheia: RON

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

Text Decriptat: SECRET

Exc 2 a) Mesaj de criptat: MESAJ

Cheia: $k=(7,2) \Rightarrow k_1 = 7$

$k_2 = 2$

$Enc_k(M) = (7 \cdot 12 + 2) \% 26 = 86 \% 26 = 8 = I$

$Enc_k(E) = (7 \cdot 4 + 2) \% 26 = 30 \% 26 = 4 = E$

$Enc_k(S) = (7 \cdot 18 + 2) \% 26 = 128 \% 26 = 24 = Y$

$Enc_k(A) = (7 \cdot 0 + 2) \% 26 = 2 \% 26 = 2 = C$

$Enc_k(J) = (7 \cdot 9 + 2) \% 26 = 65 \% 26 = 13 = N$

Text Criptat: IEYCN

b) Mesaj de decriptat: QJA

Cheia: $k=(17,5) \Rightarrow k_1 = 17$

$k_2 = 5$

$Dec_k(Q) = 17^{-1}(16-5) \bmod 26$

$= (17^{-1} \cdot 11) \bmod 26$

$26 = 17 \cdot 1 + 9 \quad \Leftrightarrow \quad 26 + 17 \cdot (-1) = 9$

$17 = 9 \cdot 1 + 8 \quad \Leftrightarrow \quad 17 + 9(-1) = 8$

$9 = 8 \cdot 1 + 1 \quad \Leftrightarrow \quad 9 + 8(-1) = 1$

$8 = 8 \cdot 1$

$\Rightarrow 9 + [17 + 9(-1)] \cdot (-1) = 1$

$9 + 17(-1) + 9 = 1$

$2 \cdot 9 + 17(-1) = 1$

$2 \cdot [26 + 17(-1)] + 17 \cdot (-1) = 1$

$2 \cdot 26 + 17(-2) + 17 \cdot (-1) = 1$

$\underbrace{2 \cdot 26}_{0} + 17(-3) = 1 \pmod{26}$

$17(-3) = 1$

$\mathbb{Z}_{26} \Rightarrow (-3) = 23$

$\Rightarrow 17 \cdot 23 = 1$

$17 \cdot 17^{-1} = 1$

$\Rightarrow 17^{-1} = 23 \pmod{26}$

$Dec_k(Q) = (23 \cdot 11) \bmod 26 = 19 = T$

$Dec_k(J) = 23 \cdot (9-5) \bmod 26 = 14 = O$

$Dec_k(A) = 23 \cdot (-5) \bmod 26 = 15 = P$

Text Decriptat : TOP

Exc 3 a) Mesaj de criptat : CERCETARI OPERATIONALE

Permutare : $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Lungime cheie : 3

2 1 3
C E R
C E T
A R I
O P E
R A T
I O N
A L E

Text Criptat : EERPAOL CCAORIA RTIETNE

b) Mesaj de decriptat : PTASC OANER RORAE ILEH

Permutare : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

Lungime cheie : 4

19 caractere

19 / 4 = 4 rest 3 => coloanele 2, 1, 4 (adică primele 3) vor avea 5 caractere

2	1	4	3
O	P	E	R
A	T	I	O
N	A	L	R
E	S	E	A
R	C	H	

Text Decriptat: OPERATIONAL RESEARCH

Exc 4 a) Mesaj de criptat: MESAJ CLAR

Cheia: CHEIE

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

ME SA JC LA RQ

NH UE AH PC SR

Text Criptat: NH UE AH PC SR

b) Mesaj de decriptat: TAAK SUCP

Cheia: ATAC

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

TA AK SU CP

AD VE RS AR

Text Decriptat: AD VE RS AR