Criptografie şi Securitate (ROL) - Seminar 1

Sisteme de criptare clasice

1. Sistemul cavalerilor de Malta.

$A:$	$B:$	$C:$
$D:$	$E:$	$F:$
$G:$	$H:$	$I:$

$J.$	$K.$	$L.$
$M.$	$N.$	$O.$
$P.$	$Q.$	$R.$

S	T	U
V	W	X
Y	Z	

   (a) Criptaţi mesajul SUBTITUTIE SIMPLA.

   (b) Decriptaţi mesajul $\underline{\quad .} \quad \boxed{\quad :} \quad \underline{\quad} \quad \underline{\quad :} \quad \underline{\quad .}$

   (c) Câte chei posibile există ?

2. Sistemul Polybius cu cheie (I=J).

   (a) Criptaţi mesajul SUBSTITITIE folosind cheia de criptare POL.

   (b) Decriptaţi mesajul 21 32 24 42 45.

   (c) Câte chei posibile există ?

3. Sistemul Cezar cu cheie.

   (a) Criptaţi mesajul CRIPTOGRAFIE folosind cheia de criptare $k = 4$.

   (b) Decriptaţi mesajul ECFDEPO ALCEJ, criptat folosind cheia $k = 11$.

   (c) Câte chei posibile există ?

4. Sistemul afin ($k = (k_1, k_2)$; $Enk_k(m) = k_1 m + k_2 \pmod{26}$).

   (a) Criptaţi mesajul TEXT folosind cheia de criptare $k = (3, 5)$.

   (b) Decriptaţi mesajul PRHFG, criptat folosind cheia $k = (3, 5)$.

   (c) Câte chei posibile există ?

5. Sisteme de substituţie simplă.

   (a) Criptaţi mesajul WEB DESIGN folosind cuvântul cheie BROWSER.

   (b) Decriptaţi mesajul KQSFCYDEX folosind cuvântul cheie ASYMMETRIC.

   (c) Câte chei posibile există ?

6. Sisteme de transpoziţie.

(a) Criptaţi mesajul STANDARDUL DE CRIPTARE cu ajutorul permutării $\sigma = (2, 3, 1)$.

(b) Decriptaţi mesajul SFCME TAEAE NLR, cifrat cu ajutorul permutării $\sigma = (1, 2, 3)$.

7. Sisteme mixte.

(a) Criptaţi mesajul SISTEM MIXT cu ajutorul sistemului Cezar şi al permutării $\sigma = (2, 3, 1)$.

(b) Decriptaţi mesajul CPKQCG ZGTVTK GOERIH, cifrat cu ajutorul sistemului Cezar $k = 2$ şi al permutării $\sigma = (3, 2, 1)$.

8. Sistemul Playfair (I=J).

(a) Criptaţi mesajul THE CIRCLE cu ajutorul parolei $ALBUM$.

(b) Decriptaţi mesajul PIGOY CLETY AEYLQ VSFWN, parola utilizată fiind CRYPTOOL.

9. Sistemul Hill ($C = MK$).

(a) Criptaţi mesajul RONALD folosind cheia

$$\begin{pmatrix} \text{B} & \text{E} \\ \text{V} & \text{H} \end{pmatrix}$$

(b) Decriptaţi mesajul NYNAF JUWBL, cifrat cu ajutorul cheii

$$\begin{pmatrix} \text{J} & \text{S} \\ \text{W} & \text{V} \end{pmatrix}$$