Laborator 3

Cifruri cu transpoziție

1.Breviar teoretic

Spre deosebire de cifrurile cu substituţie, care păstrează ordinea literelor din textul sursă dar le transformă, cifrurile cu transpoziţie (*transposition ciphers*) reordonează literele, fără a le „deghiza”.

Criptarea prin transpoziţie constă în scrierea textului iniţial - din care s-au eliminat spaţiile şi semnele de punctuaţie - într-o matrice de dimensiune $M \cdot N$ şi interschimbarea anumitor linii (sau coloane) între ele. Textul criptat se obţine prin scrierea caracterelor din noua matrice de pe fiecare coloană în parte, începând cu elementul din stânga-sus. Dacă lungimea textului iniţial este mai mică decât numărul de elemente ce pot fi scrise in matrice, atunci textul se completează cu elemente aleatoare, pană ajunge la dimensiunea $M \cdot N$.

Transpoziţie cu parolă. Pentru ca procesul de decriptare să fie mai simplu se foloseşte o versiune a criptării prin transpoziţie care se bazează pe o parolă. Literele din parolă determină ordinea în care se vor interschimba coloanele în matricea aleasă. Această ordine este stabilită astfel: se ordonează alfabetic literele din cheie şi fiecărei litere i se asociază numărul de ordine din şirul obținut prin ordonare. Lungimea parolei trebuie să fie egală cu numărul de coloane din matrice.

2.Exemple

1. Să se cripteze textul clar MISIUNEA A FOST INDEPLINITA.

Textul clar are lungimea de 24 de caractere, deci se poate alege o matrice cu 4 linii şi 6 coloane.

Pentru ca textul să fie mai greu de decodificat, acesta ar trebui să conţină şi caractere alese aleator, sau într-un mod mai inteligent, care să îngreuneze munca celui care doreşte să afle conţinutul secret din mesajul criptat.

Alegem o matrice care are 5 linii şi 6 coloane. Textului iniţial i se adaugă 6 caractere aleatoare şi se obţine textul MISIUNEA A FOST INDEPLINITA XYZTWU care se scrie în matrice astfel:

	1	**2**	**3**	**4**	**5**	**6**
1	M	I	S	I	U	N
2	E	A	A	F	O	S
3	T	I	N	D	E	P
4	L	I	N	I	T	A
5	X	Y	Z	T	W	U

Prin scrierea liniilor 1, 2, 3, 4, 5 in ordinea 5, 3, 4, 1, 2, se obţine matricea din partea dreaptă.

	1	**2**	**3**	**4**	**5**	**6**
1	M	I	S	I	U	N
2	E	A	A	F	O	S
3	T	I	N	D	E	P
4	L	I	N	I	T	A
5	X	Y	Z	T	W	U

	1	**2**	**3**	**4**	**5**	**6**
5	X	Y	Z	T	W	U
3	T	I	N	D	E	P
4	L	I	N	I	T	A
1	M	I	S	I	U	N
2	E	A	A	F	O	S

Textul criptat care se obţine este: XTLMEYIIIAZNNSATDIIFWETUOUPANS

2. Să se cripteze textul clar MISIUNEA A FOST INDEPLINITĂ utilizând parola VOINIC.

Textul este scris într-o matrice de dimensiuni 5×6 ca în exemplul anterior. Lungimea parolei este egală cu numărul de coloane din matrice.

Literele din parolă se ordonează alfabetic şi se obţine şirul: C, I, I, N, O, V.

- indicele 1 este asociat cu litera C
- indicele 2 este asociat cu prima literă I din parolă
- indicele 3 este asociat cu a doua literă I din parolă
- indicele 4 este asociat cu litera N
- indicele 5 este asociat cu litera O
- indicele 6 este asociat cu litera V

	V	**O**	**I**	**N**	**I**	**C**
	6	**5**	**2**	**4**	**3**	**1**
1	M	I	S	I	U	N
2	E	A	A	F	O	S
3	T	I	N	D	E	P
4	L	I	N	I	T	A
5	X	Y	Z	T	W	U

	1	**2**	**3**	**4**	**5**	**6**
1	N	S	U	I	I	M
2	S	A	O	F	A	E
3	P	N	E	D	I	T
4	A	N	T	I	I	L
5	U	Z	W	T	Y	X

Textul cifrat care se obţine în final este: NSPAUSANNZUOETWIFDITIAIIYMETLX

3 Exerciții propuse

1. Să se cifreze mesajul:

   THE ART OF PROGRAMMING

   utilizând cifrul cu transpoziție cu matrice 5x4 și permutarea (3,1,5,2,4).

2. Să se cifreze mesajul:

   ACESTA ESTE UN TEXT CRIPTAT

   utilizând cifrul cu transpoziție cu parola PAROLA.

3. Să se decripteze mesajul:

   ETERLRCIICAAUONRBFRNFIOIIAOPRETLRTASAAMOTITXAGOS

Criptarea s-a realizat utilizând cifrul cu transpoziție cu matrice 6x8 și permutarea (4,6,5,2,1,3).

4. Să se decripteze mesajul:

   PAMDTXTOEEEANTEDIXAITORESIOAPXRZSTCR

   Criptarea s-a realizat utilizând cifrul cu transpoziție cu parola ENIGMA.

5. Scrieți o aplicație care să implementeze următoarele funcții:
   - criptarea unui text utilizând cifrul cu transpoziție cu parolă
   - decriptarea unui text utilizând cifrul cu transpoziție cu parolă