Laborator 2

Algoritmul de criptare Playfair

1.Breviar teoretic

Deși poartă numele baronului Lyon Playfair, algoritmul a fost inventat de prietenul acestuia, Charles Wheatstone şi descris pentru prima dată într-un document la 26 martie 1854. Ideea de bază este următoarea: din cele 26 litere ale alfabetului se elimină una de frecvență minimă (de exemplu J). Restul literelor se aranjează arbitrar sub forma unui pătrat 5×5, de exemplu:

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

Textul este pregătit prin transformarea în majuscule și separarea în blocuri de câte două caractere (ignorând spațiile și semnele de punctuație). Condiția este ca niciun bloc să nu conțină aceeași literă, iar textul să fie de lungime pară. Dacă textul nu îndeplinește aceste condiții, se introduce o literă de frecvență mică între cele două litere egale, respectiv ca ultim caracter.

Fiecare bloc se criptează astfel:

- dacă cele două litere nu sunt plasate în tabel pe aceeași linie sau coloană (de exemplu A și E), fiecare literă va fi înlocuită de litera aflată pe aceeaşi linie dar pe coloana celeilalte litere din cuplul curent. Astfel, AE este criptată în FO, iar EA se criptează în OF.
- dacă cele două litere se găsesc pe aceași linie (coloană), se merge ciclic cu o pozitție la dreapta (respectiv jos). Deci CA se criptează în AX, WX în UG, etc.

În varianta algoritmului Playfair cu parolă, se alege un cuvânt care va reprezenta parola iar matricea se obține trecând literele din parolă o singură dată în careul de 5x5 iar apoi celelalte litere ale alfabetului în ordine lexicografică. De exemplu, dacă parola este CRIPTOGRAFIE, se obține matricea:

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

2.Exemple

1. Să se cifreze mesajul:

Freedom is defined as the quality or state of being free.

Rezolvare:
Textul este transformat în majuscule și separat în blocuri de câte două caractere (ignorând spațiile și semnele de punctuație). Acesta devine:

FR EE DO MI SD EF IN ED AS TH EQ UA LI TY OR ST AT EO FB EI NG FR EE

Pasul următor în pregătirea textului pentru criptare este inserarea unei litere ‘X’ sau ‘Z’ între fiecare cuplu dublură de litere. De exemplu, cuvântul “FREEDOM” va deveni ”FREXEDOM”.

FR EX ED OM IS DE FI NE DA ST HE QU AL IT YO RS TA TE OF BE IN GF RE EX

Respectând regulile de cifrare Playfair, cu parola CRIPTOGRAFIE, mesajul cifrat devine:

GPAZGLBVPQLGAPUGHGUPLASMEHPCVFPNIEELGELORQAETGAZ

2.Să se decripteze mesajul obținut la exemplul1.
GPAZGLBVPQLGAPUGHGUPLASMEHPCVFPNIEELGELORQEOTGZA

Rezolvare:
Se procedează ca la criptare: textul este împărțit în grupuri de câte două caractere.
GP AZ GL BV PQ LG AP UG HG UP LA SM EH PC VF PN IE EL GE LO RQ EO TG AZ
Matricea este aceeași:

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

Perechile de litere se transformă folosind regulile inverse decât cele folosite la criptare:

FR EX ED OM IS DE FI NE DA ST HE QU AL IT YO RS TA TE OF BE IN GF RE XE

Mesajul poate fi acum citit dacă scoatem spaţiile dintre cuplurile de litere şi adăugăm spaţii noi, în funcţie de limba folosită şi de logica mesajului

FREXEDOM IS DEFINED AS THE QUALITY OR STATE OF BEING FREXE
FREEDOM IS DEFINED AS THE QUALITY OR STATE OF BEING FREE

3 Exerciții propuse

1. Să se cifreze mesajul:
   AUTONOMOUS ATTACK AGENTS
   utilizând cifrul lui Playfair cu parola MALICIOUS.

2. Să se cifreze mesajul:
   THE ART OF PROGRAMMING
   utilizând algoritmul lui Playfair și parola SECRET KEY.

3. Să se decripteze mesajul:
   RFRBD ONU
   utilizând algoritmul lui Playfair și parola PASSWORD.

4. Să se decripteze mesajul:
   RFGPRTPXCQIEKHGRCDRCTCYCESCYXS
   algoritmul lui Playfair și parola SECRET KEY.

5. Scrieți o aplicație care să implementeze următoarele funcții:
   - criptarea unui text cu ajutorul algoritmului lui Playfair
   - decriptarea unui text cifrat cu algoritmul lui Playfair