Lucrarea de laborator 2

Tema: Cifruri de substituție polialfabetică.

Sistemul de criptare Playfair:

Sistemul a fost inventat 1854 de Sir Charles Wheatstone. Cel care îl promovează și îl susține pentru a fi adoptat ca cifru oficial al Marii Britanii este baronul Lyon Palyfayr de St. Andrews. Guvernul preferă altă variantă, dar acest sistem de criptare capătă numele baronului. Ideea de bază este următoarea: Din cele 26 litere ale alfabetului se elimină una de frecvență minimă; să spunem Q. Restul literelor se aranjează arbitrar sub forma unui pătrat 5×5. Să exemplificăm sistemul pentru tabloul.

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

Acest tabel va forma atît cheia de criptare cît și cea de decriptare. Regulile de criptare/de-criptare sunt:

1. Textul clar este separat în blocuri de cîte două caractere (ignorînd spațiile). Condiția este ca nici un bloc să nu conțină aceiași literă, iar textul să fie de lungime pară. Aceste deziderate se realizează ușor modificînd puțin textul clar (se introduce o literă de frecvență mică între cele două litere egale, respectiv ca ultim caracter).
2. Fiecare bloc se criptează astfel: dacă cele două litere nu sunt plasate în tabel pe aceiași linie sau coloană (de exemplu A și E), se cercetează colțurile dreptunghiului determinat de cele două litere (în cazul nostru A, F, O, E). Perechea AE este criptată în F O. Ordinea este determinată de ordinea liniilor pe care se află literele din textul clar. Astfel, EA se criptează în OF, SF în ZB etc. Dacă cele două litere se găsesc pe aceași linie (coloană), se merge ciclic cu o poziție la dreapta (respectiv jos). Deci CA se criptează în AX, W X în UG, CA în AX etc.

De exemplu, textul clar AFARA PLOUA se criptează în XHHPPDPEPX. Se observă că cele patru apariții ale caracterului A au fost criptate cu X, H, P și din nou X. O permutare ciclică a liniilor și coloanelor tabloului nu modifică criptarea.

De exemplu, pătratul obținut prin deplasarea cu două poziții spre stînga și o poziție în sus, este echivalent cu cel inițial (ambele asigură aceeăsi cheie de criptare). Regulile de bază pot fi modificate sau completate după necesități. Astfel, se poate adăuga din loc în loc cîte o literă falsă (cu frecvență foarte redusă, cum ar fi X, Y) care să modifice textul criptat.

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

Sarcina 1: Să se scrie un program pentru implementarea criptosistemu lui **Playfair**.

Cifrul Vigenere. La fel ca cifrul Cezar, cifrul Vigenere deplasează literele, dar, spre deosebire de acesta nu se poate sparge uşor in 26 combinaţii. Cifrul Vigenere foloseşte o deplasare multiplă. Cheia nu este constituită de o singură deplasare, ci de mai multe. Cheia este constituită din câţiva întregi, k_i unde $0 \leq k_i \leq 25$.

Criptarea se face in felul următor:

$$c_i = m_i + k_i \pmod{26}.$$

Cheia poate fi, de exemplu, k = (21, 4, 2 19, 14, 17) şi ar provoca deplasarea primei litere cu 21, c1 = m1 + 21 (mod 26), a celei de a doua cu 4, c2 = m2 + 4 (mod 26), ş.a.m.d. pană la sfarşitul cheii şi apoi de la inceput, din nou. Cheia este de obicei un cuvant, pentru a fi mai uşor de memorat – cheia de mai sus corespunde cuvantului „vector". Metoda cu deplasare multiplă oferă protecţie suplimentară din două motive:

1. primul motiv este că ceilalţi nu cunosc lungimea cheii.
2. cel de al doilea motiv este că numărul de soluţii posibile creşte;

De exemplu, pentru lungimea cheiia egală cu 5, numărul de combinaţii care ar fi necesare la căutarea exhaustivă ar fi 26^5 = 11 881 376.

Decriptarea pentru cifrul Vigenere este asemănătoare criptării. Diferenţa constă in faptul că se scade cheia din textul cifrat

$$m_i = c_i + k_i \pmod{26}.$$

Pentru simplificarea procesului de cifrare se poate utiliza următorul tabel, numit Tabula Recta). Aici toate cele 26 cifruri sunt situate pe orizontală şi fiecărui cifru ii corespunde o anumită literă din cheie, reprezentată in colana din stanga abelului. Alfabetul corespunzător literelor textului clar se află in prima linie de sus a tabelului. Procesul de cifrare este simplu – este necesar ca avand litera x din cheie şi litera y din textul clar să găsim litera textului cifrat care se află la intersecţia liniei x şi coloanei y.

	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	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
b	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
c	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	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	**V**	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Sarcina 1: De cifrat, utilizând cifrul Vigenere, mesajul „Per aspera ad astra” folosind cheia K=SUPER. Pentru a cifra sau descifra mai întâi facem corespondenţa următoare:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Sarcina 2: De descifrat textul primit la sarcina precedentă, utilizând cifrul Vigenere, folosind cheia K=SUPER.

Sarcina 3: Să se scrie un program pentru implementarea criptosistemu lui Vigenere.