Lucrare de laborator nr. 3. Cifruri polialfabetice

Cifruri de substituție polialfabetică (*polyalphabetic ciphers*). Slăbiciunea cifrurilor monoalfabetice este definită de faptul că distribuția lor de frecvență reflectă distribuția alfabetului folosit. Un cifru este mai sigur din punct de vedere criptografic dacă prezintă o distribuție cât mai regulată, care să nu ofere informații criptanalistului.

O cale de a aplatiza distribuția este combinarea distribuțiilor ridicate cu cele scăzute. Daca litera *T* este criptată câteodată ca *a* și altă dată ca *b*, și dacă litera *X* este de asemenea câteodată criptată ca *a* și altă dată ca *b*, frecvența ridicată a lui *T* se combină cu frecvența scăzută a lui *X* producând o distribuție mai moderata pentru *a* și pentru *b*. Două distribuții se pot combina prin folosirea a doua alfabete separate de criptare, primul pentru caracterele aflate pe poziții pare în textul clar, al doilea pentru caracterele aflate pe poziții impare, rezultând necesitatea de a folosi alternativ doua tabele de translatare, de exemplu permutările

$$p_1(a)=(3\cdot a) \bmod 26 \text{ și } p_2(a)=(7\cdot a +13) \bmod 26.$$

Diferența dintre cifrurile polialfabetice și cele monoalfabetice constă în faptul că substituția unui caracter variază în text, în funcție de diverși parametri (poziție, context etc.). Aceasta conduce bineînțeles la un număr mult mai mare de chei posibile. Se consideră că primul sistem de criptare polialfabetic a fost creat de Leon Battista în 1568. Unele aplicații actuale folosesc încă pentru anumite secțiuni astfel de sisteme de criptare.

3.1. Cifrul Vigenère

Metoda de criptare cunoscută sub numele de „cifrul Vigenère" a fost atribuită greșit lui *Blaise de Vigenère* în secolul al XIX-lea și, de fapt, a fost descrisă pentru prima dată de *Giovan Battista Bellaso* în cartea sa din 1553 *La cifra del. Sig*. Vigenère a creat un cifru asemănător, dar totuși diferit și mai puternic în 1586.

Pe da altă parte, cifrul Vigenere folosește aceleași operații ca și cifrul Cezar. Cifrul Vigenere și fel deplasează literele, dar, spre deosebire de Cezar, nu se poate sparge ușor în 26 combinații. Cifrul Vigenere folosește o deplasare multiplă. Cheia nu este constituită de o singură deplasare, ci de mai multe, fiind generate de câțiva întregi k_i, unde $0 \le k_i \le 25$, dacă luăm ca reper alfabetul latin cu 26 de litere. Criptarea se face în felul următor:

$$c_i = (m_i + k_i) \bmod 26.$$

Cheia poate fi, de exemplu, k = (5, 20, 17, 10, 20, 13) și ar provoca deplasarea primei litere cu 5, $c_1=m_1 + 5$ (mod 26), a celei de a doua cu 20, $c_2 = m_2 + 20$ (mod 26), ș.a.m.d. până la sfârșitul cheii și apoi de la început, din nou. Cheia este de obicei un cuvânt, pentru a fi mai ușor de memorat – cheia de mai sus corespunde cuvântului „*furtun*". Metoda cu deplasare multiplă oferă protecție suplimentară din două motive:

- primul motiv este că ceilalți nu cunosc lungimea cheii;
- cel de al doilea motiv este că numărul de soluții posibile crește odată cu mărimea cheii; de exemplu, pentru lungimea cheii egală cu 5, numărul de combinații care ar fi necesare la căutarea exhaustivă ar fi 26^5 = 11 881 376.

Decriptarea pentru cifrul Vigenere este asemănătoare criptării. Diferența constă în faptul că se scade cheia din textul cifrat,

$$m_i = (c_i - k_i) \bmod 26.$$

Pentru simplificarea procesului de cifrare se poate utiliza următorul tabel, numit *Tabula Recta* (tabelul 3.1), care se utiliza de către Vigenere. Aici toate cele 26 cifruri sunt situate pe orizontală și fiecărui cifru îi corespunde o anumită literă din cheie, reprezentată în colana din stânga tabelului. Alfabetul corespunzător literelor textului clar se află în prima linie de sus a tabelului. Procesul de cifrare este simplu – este necesar ca având litera $\boldsymbol{m_i}$ din mesaj și litera $\boldsymbol{k_i}$ din

cheie să găsim litera textului cifrat c_i, care se află la intersecția liniei m_i și coloanei k_i. În exemplul din tabelul 3.1 este prezentat cazul $m_i = M$ și $k_i = H$, iar în rezultat se obține $c_i = T$.

	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

Tabelul 3.1. *Tabula Recta pentru cifrul Vigenere*

Se poate de procedat și în conformitate cu ecuațiile ce definesc modelul matematic al cifrului:

$$c_i = m_i + k_i \pmod{26} \text{ și } m_i = c_i - k_i \pmod{26},$$

așa cum este arătat în exemplul ce urmează.

Exemplu.
De cifrat, utilizând cifrul Vigenere, mesajul „*Per aspera ad astra*” cu cheia ***K***= SUPER.
Soluție. Pentru a cifra sau descifra mai întâi facem corespondența următoare (codificăm alfabetul):

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

Apoi alcătuim și completăm tabelul:

Textul clar ***M***	P	E	R	A	S	P	E	R	A	A	D	A	S	T	R	A
Cheia ***K***	**S**	**U**	**P**	**E**	**R**	S	U	P	E	R	S	U	P	E	R	S
Textul clar ***M***	15	4	17	0	18	15	4	17	0	0	3	0	18	19	17	0
Cheia ***K***	18	20	15	4	17	18	20	15	4	17	18	20	15	4	17	18
M+***K*** (mod 26)	7	24	6	4	9	7	24	6	4	17	21	20	7	23	8	18
Textul cifrat ***C***	H	Y	G	E	J	H	Y	G	E	R	V	U	H	X	I	S

Criptograma este ***C***= *HYGEJHYGERVUHXIS*.

Pentru decriptare procedăm la fel, aplicând formula reciprocă: $m_i = c_i - k_i \pmod{26}$.

Textul cifrat C	H	Y	G	E	J	H	Y	G	E	R	V	U	H	X	I	S
Cheia K	S	U	P	E	R	S	U	P	E	R	S	U	P	E	R	S
Textul cifrat C	7	24	6	4	9	7	24	6	4	17	21	20	7	23	8	18
Cheia K	18	20	15	4	17	18	20	15	4	17	18	20	15	4	17	18
M–K (mod 26)	15	4	17	0	18	15	4	17	0	0	3	0	18	19	17	0
Textul clar M	P	E	R	A	S	P	E	R	A	A	D	A	S	T	R	A

Textul clar este ***M*** = PERASPERAADASTRA

Sarcină de laborator:
De implementat algoritmul Vigenere în unul din limbajele de programare pentru mesaje în limba română (31 de litere), acestea fiind codificate cu numerele 0, 1, ... 30. Valorile caracterelor textului sunt cuprinse între ‘A’ și ’Z’, ’a’ și ’z’ și nu sunt premise alte valori. În cazul în care utilizatorul introduce alte valori - i se va sugera diapazonul corect al caracterelor. Lungimea cheii nu trebuie să fie mai mică de 7. Criptarea și decriptarea se va realiza în conformitate cu formulele din modelul matematic prezentat mai sus. În mesaj mai întâi trebuie eliminate spațiile, apoi toate literele se vor transforma în majuscule. Utilizatorul va putea alege operația - criptare sau decriptare, va putea introduce cheia, mesajul sau criptograma și va obține criptograma sau mesajul decriptat.