Lucrarea de laborator 1

Tema: Cifruri de substituție monoalfabetică. Criptarea textelor cu ajutorul algoritmului Caesar, Affine și Polibius.

Cifruri de substituţie monoalfabetică (*monoalphabetic ciphers*) sunt cifrurile în care fiecare caracter al textului în clar ***m*** este înlocuit cu un caracter corespunzător în textul cifrat ***c***. Mai jos sunt prezentate câteva dintre cele mai cunoscute cifruri de substituţie monoalfabetică:

Cifrul lui *Cesar* (sau *Cezar*). In acest cifru fiecare literă a textului clar este inlocuită cu o nouă literă obţinută printr-o deplasare alfabetică. Cheia secretă k, care este aceeaşi la criptare cat şi la decriptare, constă in numărul care indică deplasarea alfabetică, adică k∈{1, 2, 3,…, n–1}, unde **n** este lungimea alfabetului. Criptarea şi decriptarea mesajului pentru cifrul Cezar poate fi definită de formulele:

Criptarea:

$$e_k(\mathrm{x}) = \mathrm{x} + \mathrm{k} (\mathrm{mod}\ \mathrm{n})$$

Decriptarea:

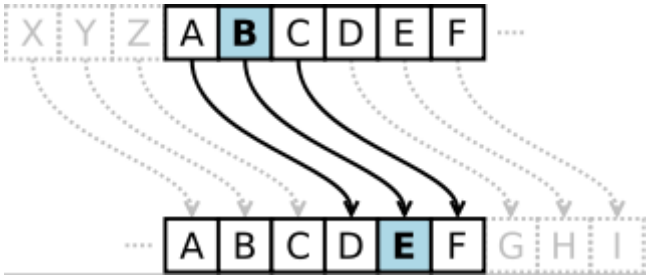
$$d_k(\mathrm{y}) = \mathrm{y} - \mathrm{k} (\mathrm{mod}\ \mathrm{n})$$

Transformarea poate fi prezentată aliniind 2 alfabete :

Dacă cheia va fi 3 atunci alfabetul va fi rotat la stânga cu 3 pozitii

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC



Sarcina 1: a) Criptați următorul text, folosind criptosistemul lui Cezar cu cheia K = 5 pe un alfabet cu 26 de caractere (A - Z):

INTRODUCERE IN CRIPTOGRAFIE

b) Criptați următorul text, folosind criptosistemul lui Cezar cu cheia K = KEY pe un alfabet cu 26 de caractere (A - Z):

AZI ESTE PRIMUL CURS

Sarcina 2: Decriptați următorul text cifrat obținut folosind criptosistemul lui Cezar utilizând cheia de decriptare K= 3:

HAHPSOLILFDUH FHCDU

Sarcina 3: Să se scrie un program pentru implementarea criptosistemului Cezar (Limbajul de programare la decizia dumneavoastră).

Cifrul *Alffin* este o generalizare a cifrului Cezar.

Cheia $\boldsymbol{k} = \{(a, b) \mid a, b \in Z_{26} = \{0, 1, 2, \ldots, 25\}, \mathrm{cmmdc}(a, 26) = 1\}$, iar funcţiile de criptare şi decriptare (pentru o cheie $\boldsymbol{k} = (a, b)$) sunt:

Criptarea:

$$e_k(\boldsymbol{x}) = a\boldsymbol{x} + b \ (\mathrm{mod}\ 26)$$

Decriptarea:

$$d_k(\mathrm{y}) = a^{-1}\mathrm{y} + a^{-1}(26 - b) \ (\mathrm{mod}\ 26)$$

Condiţia ca a să fie prim cu 26 asigură existenţa lui a^{-1} în Z_{26}.

Pentru literele de la A la Z, ele vor avea urmatoarele valori:

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

Vom cripta textul „Affine” vom lua a = 5 și b = 8, și m = 26, *26 de litere*

Pentru **A** vom avea: (5*0 + 8) mod 26 = 8

Pentru **F** vom avea: (5*5 + 8) mod 26 = 10

Decriptarea:

Pentru **A** vom avea 5^{-1} mod 26 = 21

Pentru **I** vom avea: 21(8-8) mod 26 = 0

Text clar	A	F	F	I	N	E
(5x +8) mod 26	8	7	7	22	21	2
Text criptat	I	H	H	W	V	C
21(y-8) mod 26	0	5	5	8	13	4
Text decriptat	A	F	F	I	N	E

Sarcina 1: Criptați următorul text, folosind criptosistemul lui Alffin cu cheia (3,2) pe un alfabet cu 26 de caractere (A - Z):

CRIPTOGRAFIE

Sarcina 2: Să se scrie un program pentru implementarea criptosistemului Alffin.

In *cifrul Polibios* pentru fiecare alfabet se construieşte un careu aparte de cifrare, de cele mai dese ori cu numărul de coloane şi linii sunt egale (însă nu e o condiţie necesară). Dimensiunile careului depind de lungimea *n* a alfabetului. Pentru a crea careul se iau două numere întregi, produsul cărora e cel mai aproape de *n*. Liniile şi coloanele se numerotează. După aceasta literele alfabetului se înscriu în acest careu în ordinea apariţiei.

Dacă nu sunt suficiente celule pentru literele alfabetului se pot înscrie întro celulă 2 litere (de frecvenţa cat mai redusă) sau este omisă litera care are o frecvenţă redusă ca de exemplu:

	a	b	c	d	e
a	A	B	C	D	E
b	F	G	H	I/J	K
c	L	M	N	O	P
d	Q	R	S	T	U
e	V	W	X	Y	Z

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

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

Text clar: VENI VIDI VICI

Text criptat: 55 15 33 24 55 24 14 24 55 24 13 24.

Sarcina 1: Criptați următorul text, folosind cifrul lui Polibius:

AM PARTICIPAT LA CONCURS

Sarcina 2: Decriptați următorul text cifrat folosind cifrul lui Polibius:

34543344 2451345343333411214213

Sarcina 3: Să se scrie un program pentru implementarea cifrul lui Polibius.