Criptografie - Tema 4

Popescu Paul - Constantin
Facultatea de Matematică

Exerciţiu: Să se cripteze mesajul

CRIPTAREAESTEARTASECRETELOR

folosind cheia k=5, mesajul criptat să se mai cripteze încă odată cu cheia k=8. Ce se poate spune despre rezultat? Se folosește alfabetul (A-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	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

Pas 1: Cheia k = 5 pentru mesajul initial

m	C	R	I	P	T	A	R	E	A	E	S	T	E	A	R	T	A	S	E	C	R	E	T	E	L	O	R
m	2	17	8	15	19	0	17	4	0	4	18	19	4	0	17	19	0	18	4	2	17	4	19	4	11	14	17
k	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
c	7	22	13	20	24	5	22	9	5	9	23	24	9	5	22	24	5	23	9	7	22	9	24	9	16	19	22
c	H	W	N	U	Y	F	W	J	F	J	X	Y	J	F	W	Y	F	X	J	H	W	J	Y	J	Q	T	W

Mesajul obtinut: HWNUYFWJFJXYJFWYFXJHWJYJQTW

Pas 2: Cheia k = 8 pentru noul mesaj criptat

c	H	W	N	U	Y	F	W	J	F	J	X	Y	J	F	W	Y	F	X	J	H	W	J	Y	J	Q	T	W
c	7	22	13	20	24	5	22	9	5	9	23	24	9	5	22	24	5	23	9	7	22	9	24	9	16	19	22
k	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
c	15	4	21	2	6	13	4	17	13	17	5	6	17	13	4	6	13	5	17	15	4	17	6	17	24	1	4
c	P	E	V	C	G	N	E	R	N	R	F	G	R	N	E	G	N	F	R	P	E	R	G	R	Y	B	E

Mesajul obtinut: PEVCGNERNRFGRNEGNFRPERGRYBE

Observatii: Criptarea succesivă cu doi pași de cifru Cezar (cu chei $k = 5$ și $k = 8$) este echivalentă cu o singură criptare cu cheia:

$$k_{\text{total}} = k_1 + k_2 = 5 + 8 = 13$$

Astfel, mesajul final este **exact rezultatul** aplicării cifrului Cezar cu $k = 13$ asupra textului original.

m	C	R	I	P	T	A	R	E	A	E	S	T	E	A	R	T	A	S	E	C	R	E	T	E	L	O	R
m	2	17	8	15	19	0	17	4	0	4	18	19	4	0	17	19	0	18	4	2	17	4	19	4	11	14	17
k	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
c	15	4	21	2	6	13	4	17	13	17	5	6	17	13	4	6	13	5	17	15	4	17	6	17	24	1	4
c	P	E	V	C	G	N	E	R	N	R	F	G	R	N	E	G	N	F	R	P	E	R	G	R	Y	B	E

Mesajul obtinut: PEVCGNERNRFGRNEGNFRPERGRYBE

Proprietate interesantă:
Dacă aplicăm încă o dată cifrul Cezar cu k = 13, mesajul revine la forma inițială. Aceasta se datorează faptului că alfabetul are 26 litere, iar 13 este exact jumătate, deci aplicarea de două ori inversează complet transformarea.