Detyra Shifrimi i Vernamit

Detyra 1.

Të bëhet dekriptimi i mesazhit "**FCCEQSHD**" duke e përdorur qelesin "**XBMORNYZ**", përmes shifruesit të Vernamit- ONE TIME PAD.

Cypertext = **FCCEQSHD**

Key = **XBMORNYZ**

Plaintext = ?

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
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	26

Formula → (Cyphertext – Key) mod26 = Plaintext

Cyphertext:

F	C	C	E	Q	S	H	D
6	3	3	5	17	19	8	4

Zbritje

Key:

X	B	M	O	R	N	Y	Z
24	2	13	15	18	14	25	26

Barazim

(6-24)	(3-2)	(3-13)	(5-15)	(17-18)	(19-14)	(8-25)	(4-26)
-18mod26	**1mod26**	**-10mod26**	**-10mod26**	**-1mod26**	**5mod26**	**-17mod26**	**-22mod26**

Plaintext:

8	1	16	16	25	5	9	4
H	A	P	P	Y	E	I	D

Plainext = "**HAPPYEID**"

Detyra 2.

Të bëhet enkriptimi i mesazhit "**GEZUARVITINERI**" duke e përdorur qelesin "**KXTWBMPXRNYSMZ**", përmes shifruesit të Vernamit- ONE TIME PAD.

Plaintext = **GEZUARVITINERI**

Key = **KXTWBMPXRNYSMZ**

Cyphertext = ?

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
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	26

Formula → (Plaintext + Key) mod26 = Cyphertext

Plaintext:

G	E	Z	U	A	R	V	I	T	I	N	E	R	I
7	5	26	21	1	18	22	9	20	9	14	5	18	9

Mbledhje

Key:

K	X	T	W	B	M	P	X	R	N	Y	S	M	Z
11	24	20	23	2	13	16	24	18	14	25	19	13	16

Barazim

(7+11)	(5+24)	(26+20)	(21+23)	(1+2)	(18+13)	(22+16)	(9+24)	(20+18)	(9+14)	(14+25)	(5+19)	(18+13)	(9+16)
18 mod26	**29 mod26**	**46 mod26**	**44 mod26**	**3 mod26**	**31 mod26**	**38 mod26**	**33 mod26**	**38 mod26**	**23 mod26**	**39 mod26**	**24 mod26**	**31 mod26**	**25 mod26**

Cyphertext:

18	3	20	18	3	5	12	7	12	23	13	24	5	25
R	C	T	R	C	E	L	G	L	W	M	X	E	Y

Cyphertext = "**RCTRCELGLWMXEY**"