1. convertire mesaj in hex:

a3dfe4842dcf7f7ffd0b23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1
969defbe2015b816e23ad092cfa86eb015aa85f17443ff0467eea223d2b2803de101f1609f3caf
f7

10100011 11011111 11100100 10000100 00101101 11001111 01111111 01111111 11111101
00001011 00100011 01000010 01101101 11011100 11000111 00111111 00101110 01101000
10100010 10110111 00011100 00010001 10101100 00011001 01001000 01011011
01110111 10011010 00000000 10100010 01110001 00011001 11100010 10000100
00110100 10001100 11110000 11100110 11100001 10010110 10011101 11101111 10111110
00100000 00010101 10111000 00010110 11100010 00111010 11010000 10010010
11001111 10101000 01101110 10110000 00010101 10101010 10000101 11110001
01110100 01000011 11111111 00000100 01100111 11101110 10100010 00100011 11010010
10110010 10000000 00111101 11100001 00000001 11110001 01100000 10011111 00111100
10101111 11110111

1010001111011111111001001000010000101101110011110111111101111111111111010000101
1001000110100001001101101110111001100011100111111001011100110100010100010101
101110001110000010001101011000001100101001000010110110111011110011010000000
000101000100111000100011001111000101000010000110100100011001111000011100110
1110000110010110100111011110111110111110001000000001010110111000000101101110
001000111010110100001001001011001111101010000110111010110000000101011010101
010000101111100010111010001000011111111100000100011001111110111010100010001
00011110100101011001010000000001111011110000100000000111110001011000001001111
10011110010101111111110111

convertire cheie in hex:

79c6f5f356b8efd6bad76d5a75de5be36dbae1d6fd6f8e1be1be3c77b77dddceb6739e9addcd
ded5a6daeb873be75edaf7479de387fcf75f78f386fa79df1a71ce3aef475beb6736e3d6fd7f96d
a75ae1e778ef873d7b8775d75df4f1beb5e3bf3c71de1f6dd7357bde3d735eb6f5ed767dae5f7
5b77

01111001110001101111010111110011010101101011100011101111110101101011101011010
11101101101010110100111010111011110010110111110001101101101101110101110000111
010110111111010110111110001110000110111110000110111110001111000111011110110111
011111011101110111001110101101100111001110011110100110101101110111001101110111
101101010110100110110110101110101110000111001110111110011101011110110110101111
1011110100011110011101111000111000011111111100111101110101111101111000111100111
00001101111101001111001110111110001101001110001110011100011101011101111010001
110101101111101011011001110011011011100011110101101111110101111111100101101101
10100111010110101110000111100111011110001110111110000111001111010111101110000
111011101011101011101011101111101001111000110111110101101011110001110111111001

1110001110001110111100001111101101101110101110011010101111011110111110001111010
1110011010111101011011011110101111011010111011001111101101011100101111101110101
01101101110111

REZULTAT:
0111100111000110111101011111001101010110101110001110111111010110101110101101010
1110110110101011010011101011101111001011011111000110110110110111010111000011 1
0101101111110101101111100011100001101111100001101111100011110001110111101101111
0111110111011101110011101011011001110011100111101001101011011101110011011101111
1001110110011110010011111001101111101010101111010010011000001000010010011111 1
1110001100100110111111000111001011011001110111100100001110001000100000101000
1001100011110011001101000011100110000001100111001100101010100110101011101010 1
0001111111100110011010011111101101010001100111111000100111000110001111011100 0
0001110111110001100110011111100011100100110101110111011011100101111000001010 1
1010010011011000110111100111000100001110011101110101010110110100101110010001
0111011000110110011010011010001000001001110110010001010010111001000111111100
0000000001011000011101101011010100101011111111010110100101101011101001111010
1100101111110100100000000

1010001111011111111001001000010000101101110011110111111101111111111111101000010
1100100011010000100110110111011100110001110011111100101110011010001010001010
1101110001110000010001101011000001100101001000010110110111011110011010000000
0001010001001110001000110011110001010000100001101001000110011110000011100110
1110000110010110100111011110111110111110001000000001010110111000000101101110
0010001110101101000010010010110011111010100001101110101100000000101011010101
0100001011111000101110100010000111111111100000100011001111110111010100010001
0001111010010101100101000000000111101111000010000000111110001011000001001111
1001111001010111111110111

0111100111000110111101011111001101010110101110001110111111010110101110101101010
1110110110101011010011101011101111001011011111000110110110110111010111000011 1
0101101111110101101111100011100001101111100001101111100011110001110111101101111
0111110111011101110011101011011001110011100111101001101011011101110011011101111
1011010101101001101101101011101011100001110011101111100111010111101111000111100111
1011101000111100111011110001110000111111111001111011101011111011110000111100111
0000110111110100111001110111110001101001110001110011100011101011101111010001
1101011011111010110110011100110110111000111101011011111110101111111100101101101
1010011101011010111000011110011101111000111011111000011100111101011110111000
1110111010111010111010111011111010011110001101111101011010111100011101111110001
1110001110001110111100001111101101101110101110011010101111011110111100011110 1010
1110011010111101011011011110101111011010111011001111101101011100101111

10111010110110111 0111

79c6f5f356b8efd6bad76d5a75de5be36dbae1d6fd6f8e1be1be3c77b77dddceb6739e9addcd
ded5a6daeb873be75edaf7479de387fcf75f78f386fa79df1a71ce3aef475beb6736e3d6fd7f96d
a75ae1e778ef873d7b8775d75df4f1beb5e3bf3c71de1f6dd7357bde3d735eb6f5ed767dae5f7
5b77

One Time Pad este un sistem de criptare perfect sigur daca este folosit corect.

2. da, acel text este:

   o9/khC3Pf3/9CyNCbdzHPy5oorccEawZSFt3mgCicRnihDSM8Obhlp3vviAVuBbiOtCSz6husBWqhfF
   0Q /8EZ+6iI9KygD3hAfFgnzyv9w==

XOR

   Orice text clar poate obtinut dintr-un text criptat cu OTP dar cu alta cheie..

AKA

a3dfe4842dcf7f7ffd0b23426ddcc73f2e68a2b71c11ac19485b779a00a27119e284348cf0e6e1
969defbe2015b816e23ad092cfa86eb015aa85f17443ff0467eea223d2b2803de101f1609f3caf
f7

XOR

4F 72 69 63 65 20 74 65 78 74 20 63 6C 61 72 20 70 6F 61 74 65 20 6F 62 74 69 6E 75 74
20 64 69 6E 74 72 2D 75 6E 20 74 65 78 74 20 63 72 69 70 74 61 74 20 63 75 20 4F 54 50
20 64 61 72 20 63 75 20 61 6C 74 61 20 63 68 65 69 65 2E 2E

REZULTAT:
a39096ed4eaa5f0b987357620eb0a64d0e18cdd668748c762a2f1ef475d6517d8bea40fedd93
8fb6e98ac65435db648b4aa4f3bb880dc535e5d1a154279e76478dd703b3def45cc1629905f6
5981d9

deci, cheia e (in base64):

o5CW7U6qXwuYc1diDrCmTQ4YzdZodIx2Ki8e9HXWUX2L6kD+3ZOPtumKxlQ122SLSqTzu4gNxTXl0aFUJ552R43XA7Pe9FzBYpkF9lmB2Q==

3. Folosita pt a encripta inca un mesaj => securitate redusa (recipientul va putea incerca sa o foloseasca pentru alte mesaje criptate, care nu ii erau destinate, reusind sa le decripteze).

Folosita pt a decripta alt mesaj => rezultate inconsistente, cel mai probabil false (in general, cheile nu persista de la o criptare la alta)

2)

1. sistem: Cezar

exemplu criptare: **The quick brown fox jumps over the lazy dog.**

=>
esp bftnv mczhy qzi ufxad zgpc esp wlkj ozr.

strategie: fiecare litera se schimba cu litera la 11 pozitii distanta (a -> l)

decriptare:
esp bftnv mczhy qzi ufxad zgpc esp wlkj ozr.
=> **The quick brown fox jumps over the lazy dog.**

securitate: foarte slaba. sunt 26 de strategii pentru criptare, astfel ca o tehnica de decriptare ar putea fi incercarea, pe rand, de a inlocui fiecare litera cu litera aflata la k pozitii distanta

2. sistem: rail fence cypher

criptare: textul este scris in zigzag. exista o cheie, reprezentand cate numere contine o diagonala
exemplu criptare: GeeksforGeeks => GsGsekfrek eoe
decriptare: se incearca, pe rand, determinarea numarului de elemente pe diagonala. pentru fiecare astfel de numar, se imparte stringul in grupuri care vor corespunde fiecarui rand.
securitate: nu prea, mai ales pentru textele scurte

3) E = **A**
W =
3. G = T

D = H
J = E

O = R

alice and bob are the worlds most famous cryptographic couple since their invention in they have at once been called inseparable and have been the subject of numerous divorces travels and torments in the ensuing years other characters have joined their cryptographic family theres eve the passive and submissive eavesdropper mallory the malicious attacker and trent trusted by all just to name a few while alice bob and their extended family were originally used to explain how public key cryptograph

4)

23	II V IV	RWQ	BN FK OS PW TA ZE	IYM

Reflector: UKW-B	1st Rotor:	2nd Rotor:	3rd Rotor:
Rotor	II	V	IV
Ring Setting	R	W	Q
Initial Position	I	Y	M

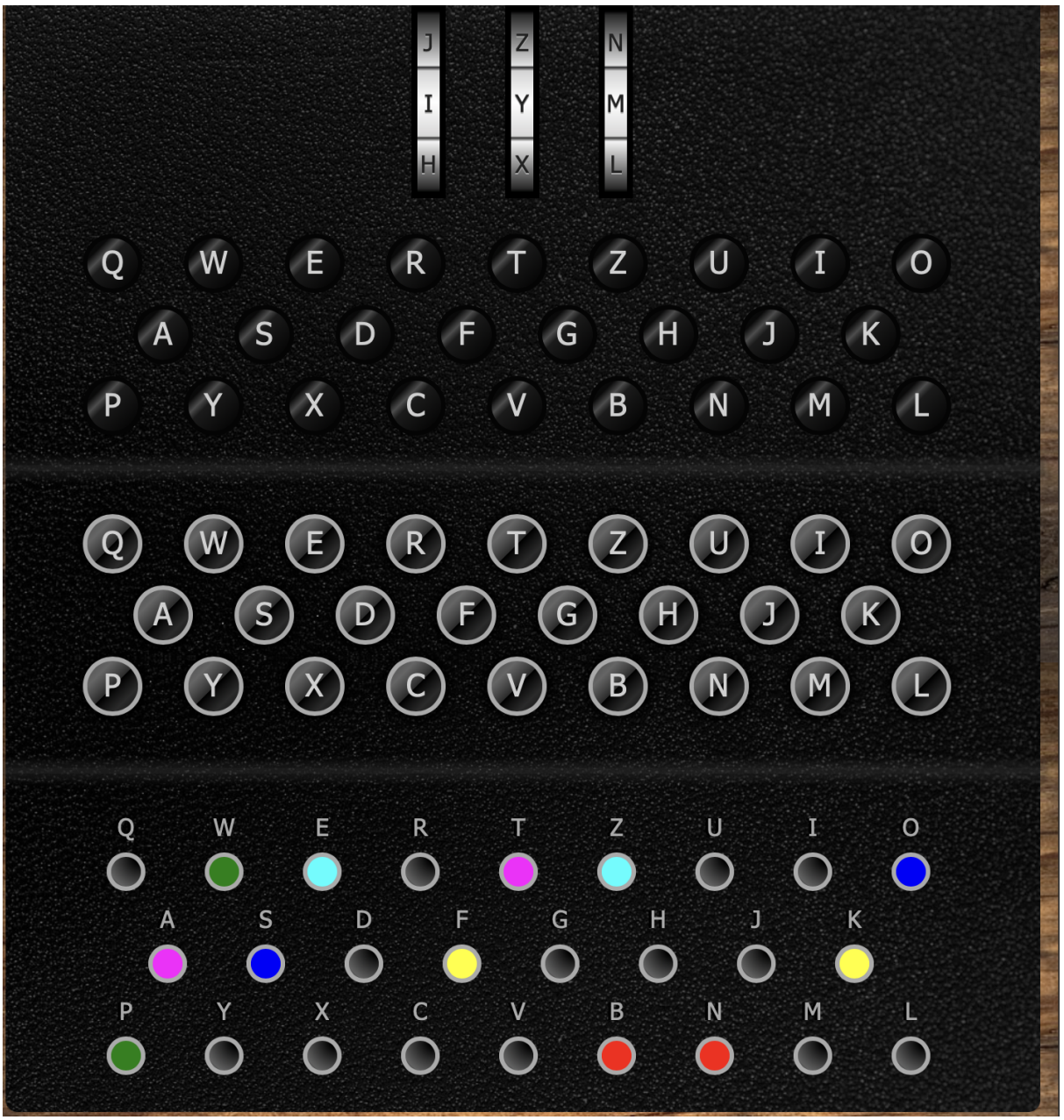
CRIPTARE:

Plaintext:	Ciphertext:
MATEI	RLSFE

DECRIPTARE (pentru aceasta, a trebuit setata masina din nou in pozitia initiala)

Ciphertext:	Plaintext:
RLSFE	MATEI

exemplu de text care nu ar putea fi criptarea numelui: MQWES (in Enigma, o litera niciodata nu se mapeaza in ea => imposibil pt M si E)


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