**Assignment 1**

**Deadline: 13.06.2023**

1. Given that the Caesar's cipher was used, find the plaintext that corresponds to the following ciphertext:  
**VSRQJHEREVTXDUHSDQWU**  
  
2. Encrypt the message  
**"we are all together"**  
using a double transposition cipher (of the type described in the text) with 4 rows and 4 columns,  
  
using the row permutation  
**(1,2,3,4) -> (2,4,1,3)**  
and the column permutation  
**(1,2,3,4) -> (3,1,2,4).**  
  
3. Using the letter encoding in Table 2.1(Check book), the following   
ciphertext message was encrypted with a one-time pad: KITLKE.  
       a. If the plaintext is "thrill," what is the key?  
       b. If the plaintext is "tiller," what is the key?  
  
  
4. Suppose that, after a particular step, the values in the registers are  
  
X = (x0,x1,..., x18) = (1010101010101010101)  
Y = (y0, y1, ..., y21) = (1100110011001100110011)  
Z = (z0, z1 , . . . , z22) = (11100001111000011110000)  
List the **next 3 keystream bits** and give the contents of X, Y, and Z after these 3 bits have been generated.

5. This problem deals with the DES cipher. Answer shortly.  
  
  a. How many bits are in each plaintext block?  
  b. How many bits are in each ciphertext block?  
  c. How many bits are in the key?  
  d. How many bits are in each subkey?  
  e. How many rounds?  
  f. How many S-boxes?  
  g. An S-box requires how many bits of input?  
  h. An S-box generates how many bits of output?