

CENTRO UNIVERSITÁRIO INTERNACIONAL UNINTER

ESCOLA SUPERIOR POLITÉCNICA

BACHARELADO EM ENGENHARIA DA COMPUTAÇÃO

DISCIPLINA DE Matemática computacional

ATIVIDADE PRÁTICA

nilzilene s araújo – RU: 3312120

luis gonzaga de paulo

curitiba – Paraná

2020

atividade prática

Codificar a mensagem “APROVADO” por criptografia simétrica pelo algiritmo elementar XOR utilizando como chave criptográfica o seu ru ou parte dele.

Após a obtenção da cifra decodifica-la comprovando a reciprocidade do processo.

tabela verdade  
XOR  
0 0 0  
0 1 1  
1 0 1  
1 1 0  
  
Transformando a palavra “APROVADO” para binário:  
  
A 01000001  
P 01010000  
R 01010010  
O 01001111  
V 01010110  
A 01000001  
D 01000100  
O 01001111  
  
Os últimos 2 numeros do meu RU em binário (chave criptográfica):  
20 = 0001 0100  
  
Calcular o XOR com binário de cada letra com o binário de 20:

A XOR 20 = 0100 0001 XOR 0001 0100 = 0101 0101  
P XOR 20 = 0101 0000 XOR 0001 0100 = 0100 0100  
R XOR 20 = 0101 0010 XOR 0001 0100 = 0100 0110  
O XOR 20 = 0100 1111 XOR 0001 0100 = 0101 1011  
V XOR 20 = 0101 0110 XOR 0001 0100 = 0100 0010  
A XOR 20 = 0100 0001 XOR 0001 0100 = 0101 0101  
D XOR 20 = 0100 0100 XOR 0001 0100 = 0101 0000  
O XOR 20 = 0100 1111 XOR 0001 0100 = 0101 1011  
  
  
Descriptografando calculando XOR novamente com o resultado anterior:

0101 0101 XOR 20 = 0101 0101 XOR 0001 0100 = 0100 0001 = A  
0100 0100 XOR 20 = 0100 0100 XOR 0001 0100 = 0101 0000 = P  
0100 0110 XOR 20 = 0100 0110 XOR 0001 0100 = 0101 0010 = R  
0101 1011 XOR 20 = 0101 1011 XOR 0001 0100 = 0100 1111 = O  
0100 0010 XOR 20 = 0100 0010 XOR 0001 0100 = 0101 0110 = V  
0101 0101 XOR 20 = 0101 0101 XOR 0001 0100 = 0100 0001 = A  
0101 0000 XOR 20 = 0101 0000 XOR 0001 0100 = 0100 0100 = D  
0101 1011 XOR 20 = 0101 1011 XOR 0001 0100 = 0100 1111 = O  
  
Resposta :

APROVADO criptografado usando XOR com chave "20" em ascii (tudo em binário):

0101 0101  
0100 0100  
0100 0110  
0101 1011  
0100 0010  
0101 0101  
0101 0000  
0101 1011