

## TAG CRYPTO 1

Nome: Thomaz Veloso Rebelo da Silva

Data: 28/02/2020

## CRYPTOPALS SET 1

### CHALLENGES:

1-

Um programa em C++ que printa o hex dado, em ASCII com %s do printf

Depois um programa em python que traduz de ASCII para base64.

(O base64 funciona de maneira simples falando pegando os 8 bytes de uma letra depois ele lê apenas 6 em sequência e faz assim sucessivamente para encriptar a sua string)

2-

O python tem um operador exclusivo para o XOR que é “ ^ ” sendo assim a função ficar bem mais simples e ainda mais com o import da biblioteca “ from common import FixedXor “ dando FixedXor.FixedXor(valor1 , valor2 ) ele já faz todo processo para resolve-lo

(O XOR ou “Ou exclusivo” exemplo pratico :  $A \oplus B = (\bar{A} \times B) + (A + \bar{B})$  )

3-

Escolhendo a melhor saída de acordo com a pontuação fazendo uma função dentro de outra para testar essa pontuação, fazendo ela testar a melhor possível para poder achar o resultado final.