

CHALLENGE NAME: [Chaos]   
DEV : [Abhinav]

CATEGORY: [Cryptography]   
LEVEL: []

2025



CHALLENGE NAME: [Chaos]

**Challenge Description**:   
You've stumbled upon a bunch of garbled nonsense—some might call them "encrypted messages," but who really knows? Most of it is just random junk, but hidden somewhere in this mess is an actual secret. No keys, no hints, just you and the chaos. Good luck figuring it out—if you even can.

**Solution:**In this challenge, participants are given an output.txt file that contains encrypted messages. Some of these messages are fake flags, while one contains the real flag. The encryption method used is a custom XOR-based encoding with a shifting pattern. The goal is to reverse the encryption and extract the real flag.  
Step 1: **Understanding the Encryption Process**  
The encryption script performs the following steps:

Reads lines from **stuff.txt** and **flag.txt.**

Stores all lines in a list and shuffles them randomly.

Encrypts each line using a custom XOR function.

Writes the encrypted messages to **output.txt.**

The XOR function works by:

Iterating over each byte of the message.

XOR-ing each byte with its index modulo 256 (i % 256).

Encoding the result using Base85.  

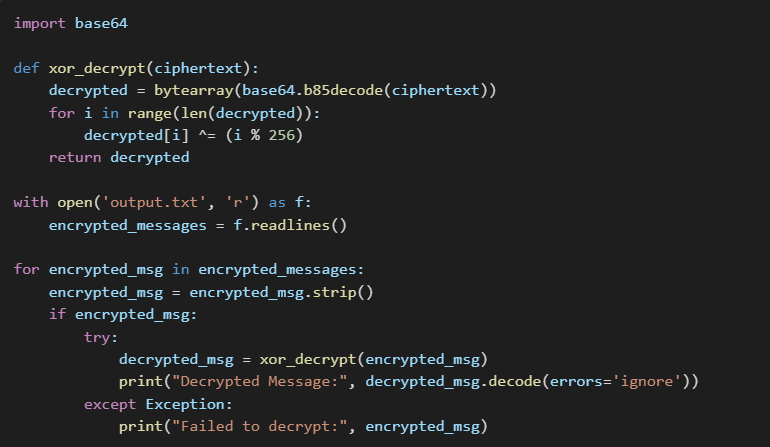

Step 2: Crafting the Decryption Script  
Since the encryption uses a simple XOR operation, participants must write a decryption script to reverse it. To decrypt:

Read **output.txt** line by line.

Decode each line from Base85.

Apply the same XOR operation (with the same index-based pattern) to reverse the transformation.

Print the decrypted messages.

A correct decryption script would look like this:  


Step 3: Running the Decryption Script.

**Flag: VishwaCTF{CrYpt0\_cRyPT0\_1g\_It\_1s\_sOm3\_7hiNg\_t0\_D0}**

DEV: [] **1**