

2Enc Hacklabs.id

Ketika saya membuka instagram Hacklabs.id dan melihat soal dari 2Enc





hacklabs.id Hello Players! 👁👁👁

How's your first Cryptography challenge? Easy right? 😊

Now we provide you more challenging problem of Crypto. This challenge is created by DarkAngels.

Further descriptions and hints are included in the given link below with the files:  
[https://drive.google.com/file/d/1I0NHa6fWEFu58H5V1gVWe\\_b1ljzm6Mek/view?usp=sharing](https://drive.google.com/file/d/1I0NHa6fWEFu58H5V1gVWe_b1ljzm6Mek/view?usp=sharing)

Flag format : CSC {...}  
Good luck! 😊

Dari caption saya mengetahui bahwa 2enc merupakan suatu file yang di download dari google drive, ketika saya selesai mendownload file tersebut dan mengecek isi file tersebut, dan hanya menemukan 2 text file, bernama 2enc.txt dan hint\_2enc.txt

2enc.txt	48	48	Text Document	18/09/2020 7:33
hint_2enc.txt	296	211	Text Document	18/09/2020 7:42

Dan di dalam 2enc.txt saya hanya menemukan string dengan broken bytes character

2enc.txt - Notepad

File Edit Format View Help

p[oed]RVy[o]ntMGDuMGrKp[l]g[eBOc[l]g[]E[]KwycwGp

Dan pada file hint\_2ecn.txt berisikan hint menyelesaikan txt file

hint\_2enc.txt - Notepad

File Edit Format View Help

As the Author said, the difficulty is EASY.

Hint #1: Two Cryptography Implementations

Hint #2: Heard there's a cryptanalysis tools which can solve this easily, or you could

ask Mr. Snakes

Hint #3: What are those unreadable characters ? I wonder how to get them back to normal.

Setelah melihat hint dan bertanya dengan teman saya, dia mengajarkan mengenai pembacaan character dengan bytes (menyangkut pada hint 3) oleh karna itu dibuatlah python

script, yang berfungsi untuk melakukan bruteforce dengan menggunakan kombinasi key sebanyak 255

```
XOR.py X
Python Scripts > XOR.py > ...
1 import base64
2
3 with open('2enc.txt', 'rb') as fileInput:
4     cipher = fileInput.read()
5     print(f"{cipher}\n")
6
7 #bruteforce cipher text using XOR 1-255
8 # for key in range(255):
9 #     kunci = key
10 #     plain = ""
11 #     for c in cipher:
12 #         plain += chr(c^kunci)
13 #     print(f"key {kunci} : {plain}\n")
14 #     print(base64.b64decode(plain))
15
16 #decode using known keys
17 kunci = 33
18 plain = ""
19 for c in cipher:
20     plain += chr(c^kunci)
21 print(f"key {kunci} : {plain}\n")
22 print(base64.b64decode(plain))
```

Dengan menggunakan code (yang dicomment) saya menemukan bahwa key yang digunakan ialah 33, hal ini dikarenakan identik dengan base64

```
key 33 : Q1NDe0swX1N10Ulfet1fSjQ5MF9DcnB0MF85d19jVXBVfQ==
```

Kemudian menggunakan coding yang sama, (bagian yang tidak dicomment) kemudian saya menemukan hasil decrypt base64 tersebut menghasilkan flag

```
key 33 : Q1NDe0swX1N10Ulfet1fSjQ5MF9DcnB0MF85d19jVXBVfQ==
b'CSC{K0_Su9I_y9_J490_Crpt0_9w_cUpU}'
C:\Users\Alexander Michael\Documents\Python Scripts>
```