# CTF Contest CSC

Nama: Natanael Fransisco

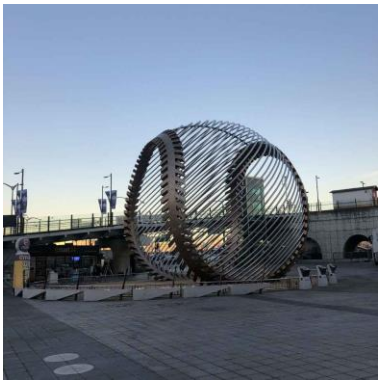
## Daftar isi

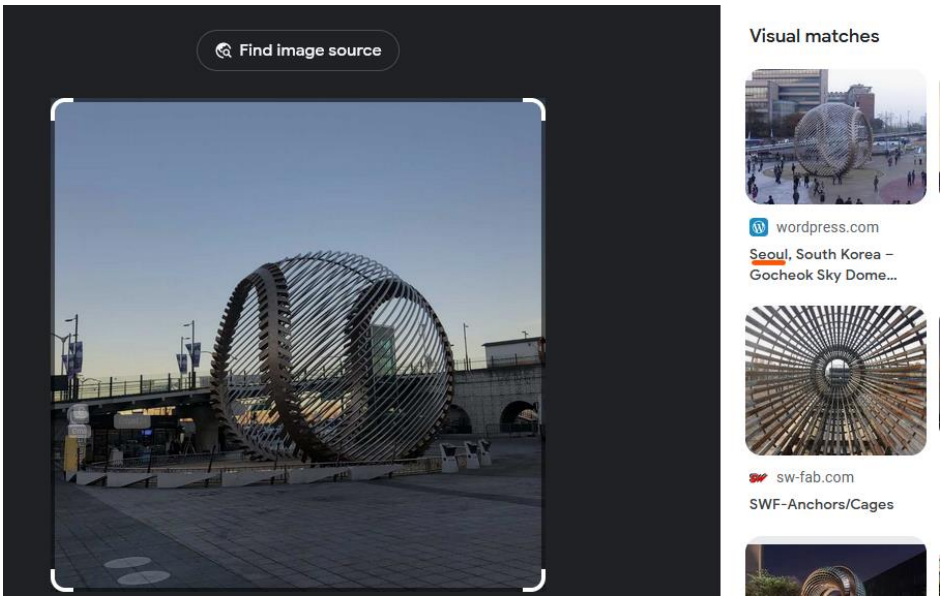


# OSINT

**Soal**
Semua Yang Ingin Saya Lakukan

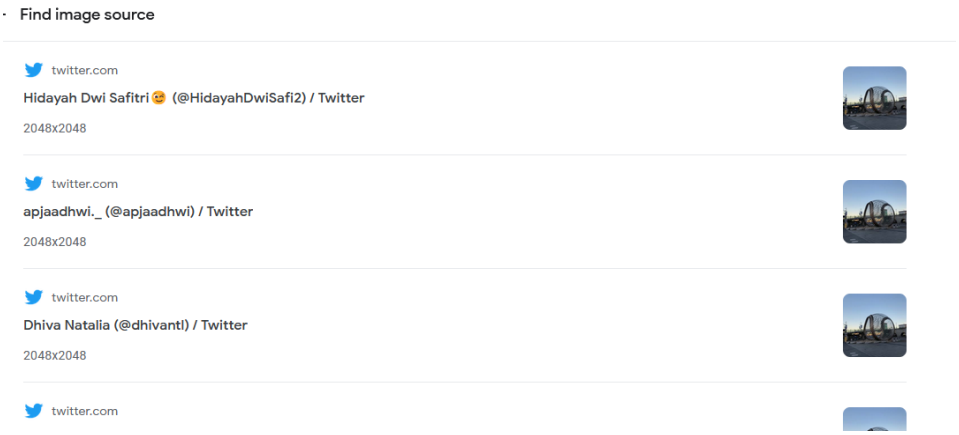
**POC**

1. Soal ini memberi 2 info format flag:
   Format: CSC{City_DDMMYY_special}
   Dan gambar monumen yang pernah di post oleh grup kpop tersebut.
   
2. Dengan 2 info ini kita disuruh mengisi format flag dengan info yang sesuai. Dengan itu, google image search biasa akan menunjukkan lokasi monumen




City = Seoul, bagian pertama dari flag sudah dapat.

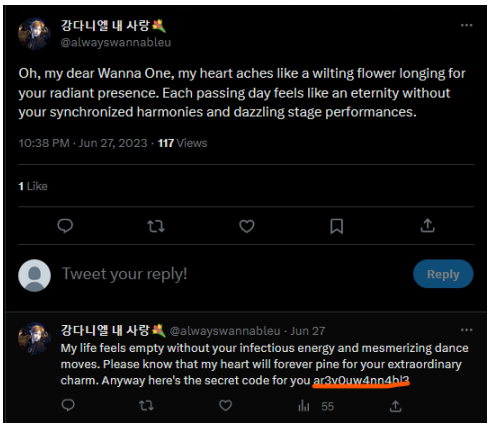
3. Bila kita klik image source di atas untuk mencari lebih lanjut hal-hal tentang image tersebut (siapa yang posting, dari web mana, sosial media apa) akan muncul twitter dengan user yang post gambar tersebut dan ada hubungannya dengan twitter.




4. Membuka akun twitter *Hidayah* akan menunjukkan clue bahwa foto tersebut di post oleh akun twitter official *wanna one*. Hal ini sesuai dengan cerita bahwa kpop grup tersebut sudah bubar.


Dari sini juga didapatkan part 2 dari flag yaitu tanggal di postnya gambar tersebut.
DDMMYY = 241218

5. Terakhir kita perlu mencari komen spesial dan ini dapat dilihat dari melihat satu-satu dan bila kita jelih ada satu komen dengan reply yang berisi spesial komen tersebut.


Part terakhir sudah didapatkan, special = ar3y0uw4nn4bl3

**Flag**
CSC{Seoul_241218_ar3y0uw4nn4bl3}

# Reverse Engineering

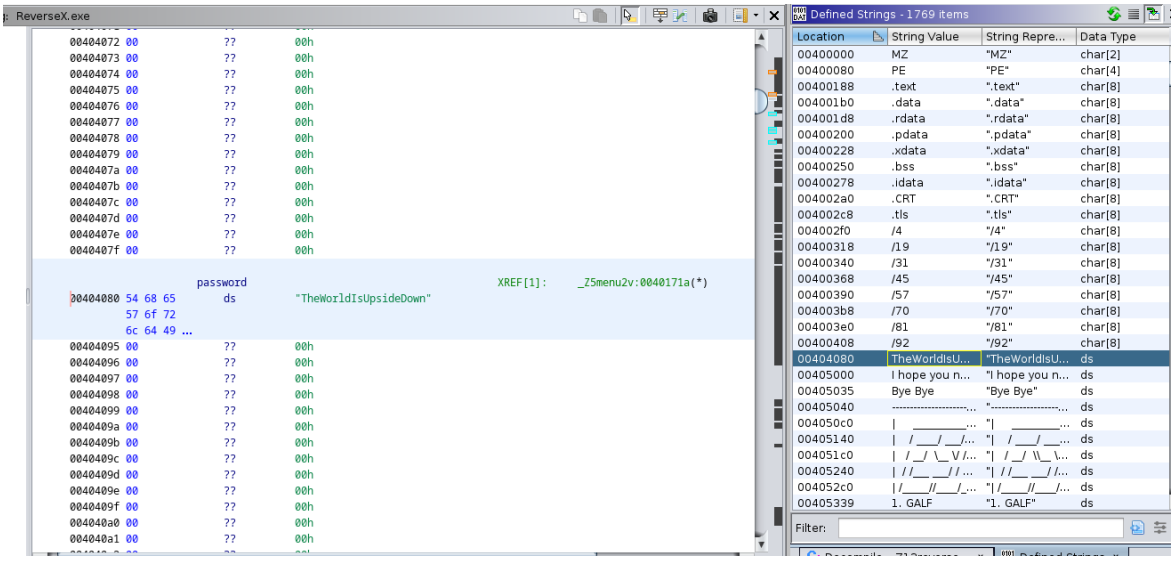
**Soal**
ESREVER

**POC**

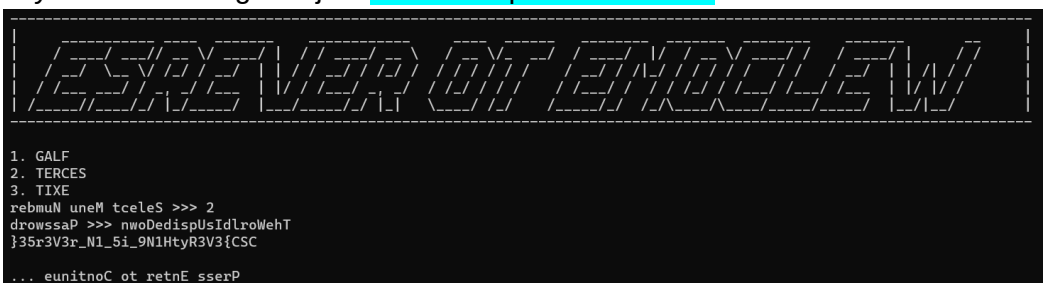
1. Kita diberikan sebuah .exe yang dapat diexecute dan mengeluarkan suatu command line menu.


Bila kita masukkan 1:
Kita dapat flag bohongan
Bila kita masukkan 2:
Kita diminta suatu password
Bila kita masukkan 3:
.exe akan exit

2. Dari semua ini tentunya yang menarik hanya opsi 2. Dari itu, saya mencoba untuk mencari password dengan membalikkan ReverseX.exe sehingga bisa lihat sedikit banyak dari source code pembuatnya. Hal ini saya lakukan dengan tool *ghidra.*
3. Ketika import file ke ghidra, saya langsung melihat strings yang ada untuk mengetahui apakah ada string yang aneh. Salah satu yang mencolok ada string “TheWorldIsUpsideDown” ketika dicari posisinya ada ditunjukkan bahwa ini ada kaitannya dengan password.




4. Saya langsung memasukkan ini “TheWorldIsUpsideDown” ke opsi 2 saat menjalankan .exe dan alhasil gagal. Namun, saya langsung berasumsi semuanya reverse sehingga saya reverse string menjadi ”nwoDedispUsIdlroWehT“ dan alhasil berhasil.




**Flag**

CSC{3V3RytH1N9_i5_1N_r3V3r53}

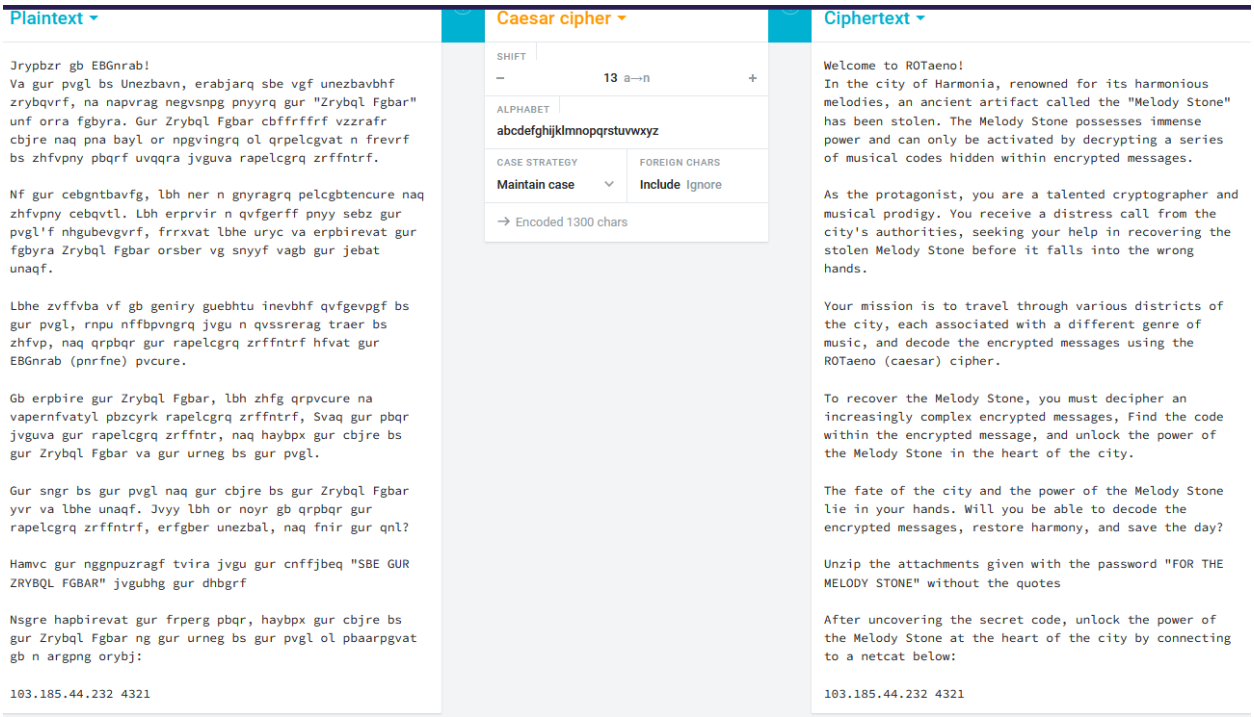
# Cryptography

**Soal**

ROTaeno

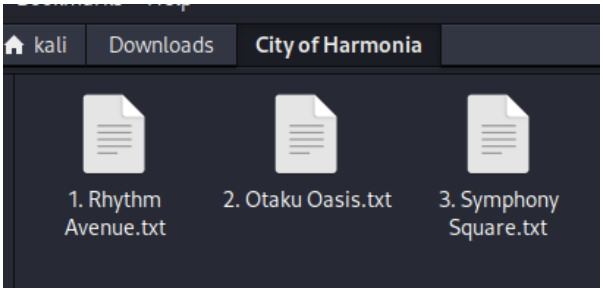
**POC**

1. Dalam soal ini kita diberi file district.zip dan welcome.txt. Karena nama soalnya memberi clue ROT maka saya menggunakan ROT cipher untuk mengubah text welcome.txt dengan ROT13.

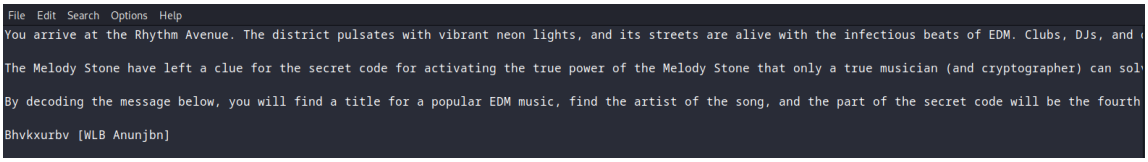



Inti dari isinya adalah mencari suatu kode rahasia yang ada di dalam district.zip yang dipecah ke beberapa attachment yang memiliki tantangan masing-masing setelah itu kode akan dimasukkan ke netcat dari ip di soal.

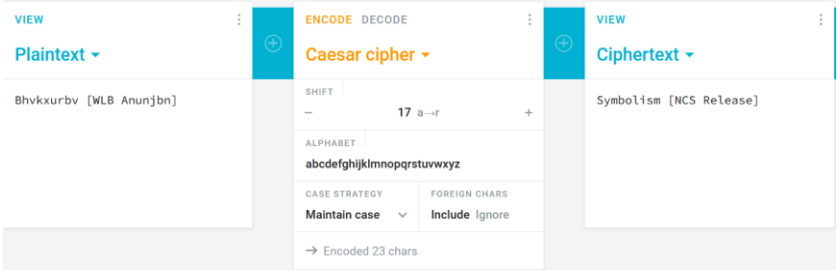
2. Ketika district.zip diunzip akan didapatkan 3 attachment:



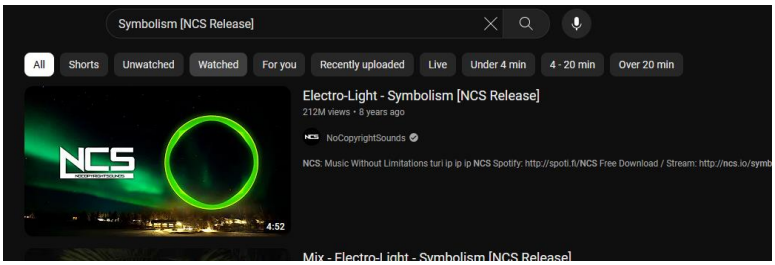

3. <u>1. Rhythm Avenue.txt:</u>




Text ini menyuruh kita mencari nama artis dari lagu yang telah dienkripsi dengan ROT di line paling bawah dan mengambil huruf ke-4 dan ke-6 dari nama artis.

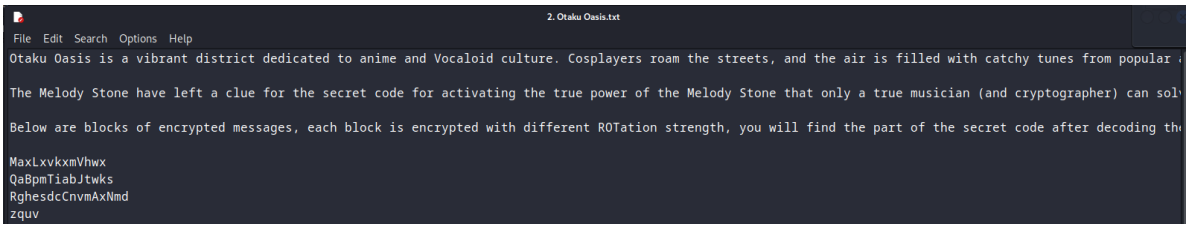


Ketika kita cari judul lagu tersebut di youtube.com maka kita akan dapat nama artis Electro-Light.




Part 1 of 3 dari secret code:
Electro-Light. = cr

4. 2. Otaku Oasis.txt;




Bagian ini hanya menyuruh kita untuk mendekripsi 4 line akhir yang terlihat terenkrispi. Disini kita ada clue bahwa tiap line memiliki ROTasi yang berbeda sehingga tiap line harus dicari satu per satu dan ketika kita sudah dekripsi per line akan muncul secret codenya berdasarkan cluenya.


line 1

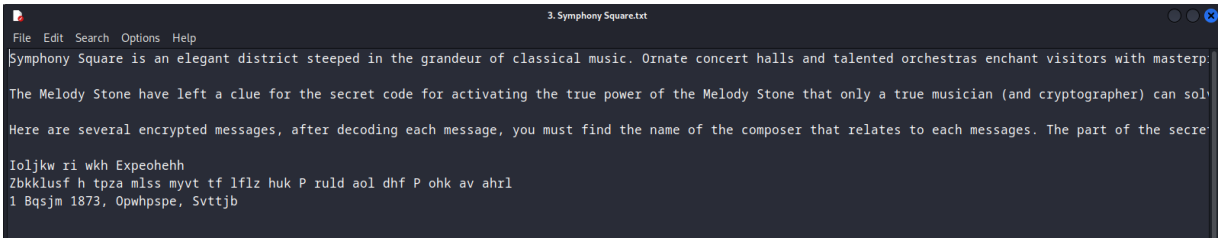

line 2


line 3

Dari 3 line ini berati secret codenya adalah line 4 yang dishift 1 ke bawah.

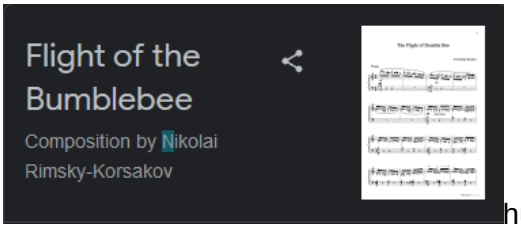

yptu

5. 3. Symphony Square.txt:



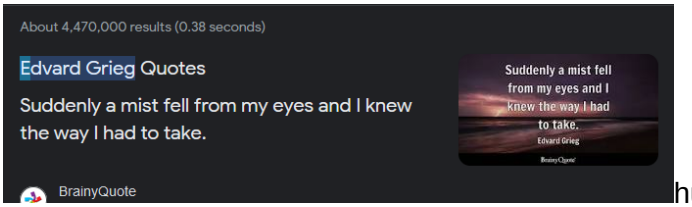

Secret code yang kali ini didapat dari huruf pertama nama tiap composer dari tiap pesan terenkripsi ini. Kasus ini dapat diselesaikan dengan cipher sebelumnya dan sedikit googling.


line 1



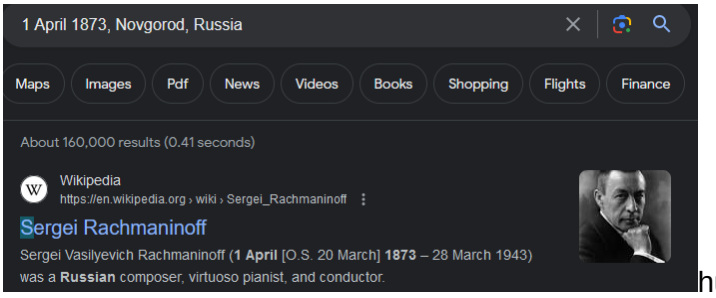

huruf = n


line 2




huruf = e


line 3




huruf = s

Jadi kita akan mendapatkan bagian yaitu nes.

6. Kode yang didapat adalah cryptunes, ini kita masukkan ke netcat 103.185.44.232 4321

```
┌──(kali㉿kali)-[~/Downloads]
└─$ netcat 103.185.44.232 4321
You are at a very sacred room at the heart of the city, to activate the power of the M
perfect melody, what is the perfect melody? (submit your answer in all UPPERCASE)
CRYPTUNES
You have activated the Melody Stone, the Melody Stone shines a very bright beacon indi
 discovered, and now you have proven yourself worthy of the power of the Melody Stone.

After resonating with the Melody Stone, A string(flag) filled within your mind.
CSC{the_melody_stone_is_the_friendship_we_made_along_the_way}
```

**Flag**

CSC{the_melody_stone_is_the_friendship_we_made_along_the_way}

**Soal**

Xorror

**POC**

1. Dalam soal ini, kita diberi 2 file chall.py dan output.txt yang dimana chall.py sebenarnya adalah code asli untuk menghasilkan output.txt.

```python
import random
import re

flag = open('flag.txt','rb').read()
assert len(flag) == 44 and flag.startswith(b"CSC{"), "Hello! in case you didn't know, you are not supposed to run th

key = random.randint(1,255)

enc = []
enc.append(flag[0] ^ key)
for i in range(1, len(flag)):
    enc.append(flag[i] ^ flag[i-1])

f = open('output.txt','w')
f.write(str(enc))
f.write('\n')
f.close()
```

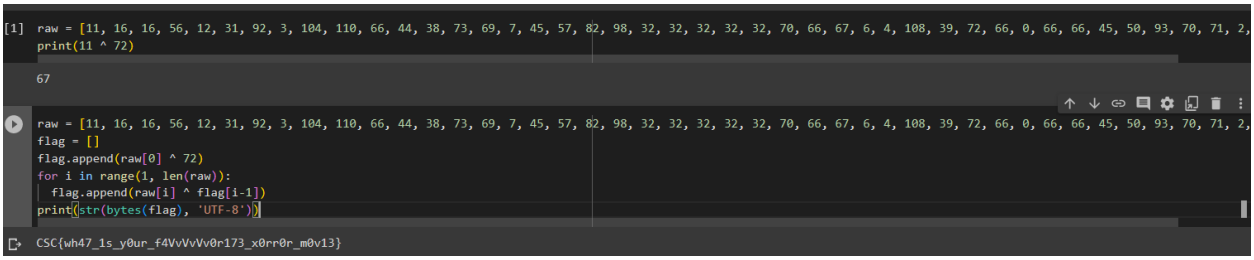
chall.py

```
[11, 16, 16, 56, 12, 31, 92, 3, 104, 110, 66, 44, 38, 73, 69, 7, 45, 57, 82, 98, 32, 32, 32, 32, 32, 70, 66, 67, 6, 4, 108, 39, 72, 66, 0, 66, 66, 45, 50, 93, 70, 71, 2, 78]
```

output.txt

2. Untuk kasus ini, Solusi yang saya gunakan adalah untuk membalikkan proses kerja dari kodenya. Dimana melihat dari chall.py karena prosesnya semua dari xor maka ketika output di xor dengan salah satu saja dari input akan mendapatkan input lain.
   Contoh:
   Output = 11
   Penjelasan:
   Kita dapat asumsi karena di awal kode ada “CSC{“ kita dapat anggap C menjadi 11. Dari proses kode, string flag diambil dan diambil tiap indexnya sehingga jika flag[0] secara string adalah “C” yang dalam bentuk int adalah 67.
   Jika kita XOR:
   Output ^ ‘C’ = key
   11 ^ 67 = 72
   Melihat bahwa proses xor untuk index flag[0] adalah dengan kunci yang random kita dapat membalikkan proses XOR untuk mendapat nilai kuncinya.

3. Kita sudah dapat key 72, dari ini kita dapat melakukan proses for loop sama seperti di chall.py sehingga kita dapat membuat kode seperti ini.




Penjelasan:

- Kita buat variabel list dari output.txt
- Kita tampung flag ke dalam variabel flag
- Gunakan saja for proses yang sama seperti chall.py untuk membuat variabel enc dimana disini kita membuat variabel flag.
- Perlu diingat karena, di chall.py proses index kedua dan seterusnya menggunakan input dari index pertama (flag[0] bukan enc[0]) dari flag asli maka kita bukan menggunakan raw[i-1] yang merupakan list dari output.txt tetapi flag[i-1] yang merupakan nilai dari flag asli (dalam kode milik saya).
- Setelah itu, kita hanya perlu ubah ke bentuk bytes dan cast lagi ke str tipe UTF-8 sehingga dapat di print dalam format string flagnya.

**Flag**

CSC{wh47_1s_y0ur_f4VvVvVv0r173_x0rr0r_m0v13}