3S CTF

Crypto-what's This Song

SWING 32 기 한재희

■ 문제 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
제가 좋아하는 노래의 가사가 랜섬웨어에 의해 암호화됐어요..
CTF를 풀며 음악을 들을 수 있도록 가사를 정상적으로 복호화해주세요

FLAG 형식은 3S()입니다.

뭔가 복호화 하는 문제인거 같다.

```
import os
import random

def get_seed(size):
    return int(os.urandom(size).hex(), 16)

input = None
output = ""

salt = get_seed(16)
random.seed(salt)

crypto = "fedcba9876543210"
malware = list(crypto)
random.shuffle(malware)
malmware = ''.join(malware)

with open("input.txt", "r") as lyrics_file:
    input = lyrics_file.read()

for char in input:
    encoded_char = (bytes(char.encode()).hex())
    output += malware[crypto.index(encoded_char[0])]
    output += malware[crypto.index(encoded_char[1])]

with open("output.txt", "w") as result_file:
    result_file.write(str(output))
```

일단 코드는 이러하고



Output 에 있는걸 아스키코드로 복호화도 해봤지만 아무것도 얻지 못했다. 그래서 16 바이트 짜리 salt 변수를 만들어서 암호화 코드에 사용된 시드 값을 찾아주는 코드를 만들어봤다.

```
import os

def get_seed(size):
    return int(os.urandom(size).hex(), 16)

salt = get_seed(16)
print(f"The seed value is: {salt}")
```

근데 실행해보니까 계속 바뀌고 malware 에 관한 시드가 아닌 것 같아서 뭐가 문제일까..

파이썬에서 실행 해보니까

```
Traceback (most recent call last):
   File "C:/Users/user/Desktop/g.py", line 18, in <module>
    with open("input.txt", "r") as lyrics_file:
FileNotFoundError: [Errno 2] No such file or directory: 'input.txt'
>>>>
```

이런 오류가 떠서 시드값을 넣고 input 텍스트 파일을 만들어서 넣어봤지만 실패했다.

