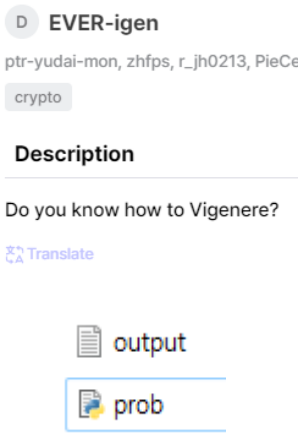
5 월 Dreamhack CTF Season 5 Round #10 (🌱Div2) write-up

SWING 32 기 한재희

여러 문제 중에 플래그 형식이 안 나와있는 EVER-igen 문제에 흥미가 생겨 선택했다.



문제를 다운 받고 압축을 푸니 텍스트파일과 파이썬 파일이 나왔다. 문제 설명에 있는 Vigenere 에 대해 우선 찾아봤다.

비즈네르 암호라고 key 를 가지고 암호화 하는 방법이란걸 알았다.

다른 사람들이 만든 코드를 보면 key 에 대한 원래 단어와 암호화된 단어가 코드 안에 있는데 드림핵 문제에는 안나와있다. 파이썬 코드를 실행해보니

```
y", line 29, in main
    with open("secret", "r") as f:
FileNotFoundError: [Errno 2] No such file or directory: 'secret'
```

이렇게 나와서 아까 텍스트 파일의 이름을 secret 으로 바꾸고 실행해봤지만 오류는 없어지지 않았다.

텍스트 파일을 확인해보니

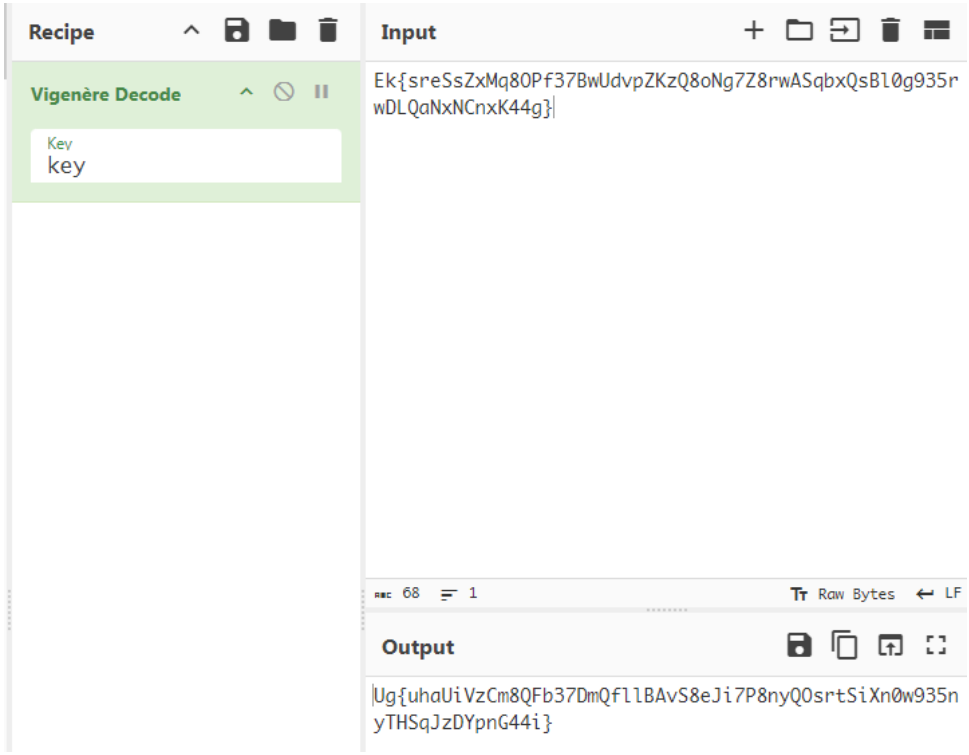
my encrypted sentence > 39 2YAx k5LgCy iP Aj9geVQy nEvXnd3Je c kX9P 8z uZ7dbErYRAyegw Ona3Js eRcKyO u7 ffFTl70 TH9ScB – M0HbNuV HDd 4yk TE c3uVU 8Y D1Q ZDNhBpRc 9WY27fjiF – dVWNBP D1Q NAZsM fW bPlBI N3e p8 6i97Nc. FmP HjIjVi 7Zu 4Zth9 bL kYD Gg0yZjc0 dBrYVQ, f8GQ0PD, Bu kGue 8BUlT9FmE0 UDCNp2vQi xd jkfm97 9uDfndFF egcc9CZ 27 mTE 2Y7u A8Zi fM N4Ks3 UVK Dg0. LTAabG 2RSDTqDu GP7QbLq. qy ZE2Xy GUpG kYD eYvEXf DJdMc fE Ep2DTjX4Zt dlk uObyx f DJq7ckZM0 "w8gse0WtBie" (L 4yk) FT LyZkB1 a29Tjc FmIjRSDDd yFQwj QfMvVi. 9I, Tjc0 dHoVj DSc zXfR.
Ek{sreSsZxMq8OPf37BwUdvpZKzQ8oNg7Z8rwASqbxQsBl0g935rwDLQaNxNCnxK44g}

맨 밑에 있는

Ek{sreSsZxMq8OPf37BwUdvpZKzQ8oNg7Z8rwASqbxQsBl0g935rwDLQaNxNCnxK44g}

이게 플래그가 암호화된 부분 같다.

찾아보니까 CyberChef 이 사이트에서 암호화 된 비즈네르 코드에서 키를 입력하면 해석해주는 것 같았다.



이 key 가 뭔지를 찾아야 될 텐데 파이썬 코드를 수정하면 key 가 랜덤으로 나오는 것 같았다.

```
assert "Vigenere", "cipher" in secret
cipher = Vigenere(key)
secret_enc = cipher.encrypt(secret)
print(f"my encrypted sentence > {secret_enc}")
```

코드 마지막 부분에 암호화된 문장이 나오는 부분을 보고

```
def main():
    key = [random.randint(0, len(words)) for _ in range(16)]
    with open("secret", "r") as f:
        secret = f.read()
```

뭔가 이 open 하고 secret 이 부분을 수정해줘야 실행될 거 같은데 텍스트 파일 이름인 output 으로도 바꿔보고 지우기도 해보고 여러가지 해봤는데 실행이 안된다.. 뭔가 파이썬 코드로 저 텍스트 파일을 읽어줘야 플래그로 해석이 될거 같은데.. 한 부분만 고쳐주면 될거 같은데 도저히 모르겠다.. 그래도 비즈네르 암호학이라는 게 있다는 사실을 새롭게 알게 되었다.