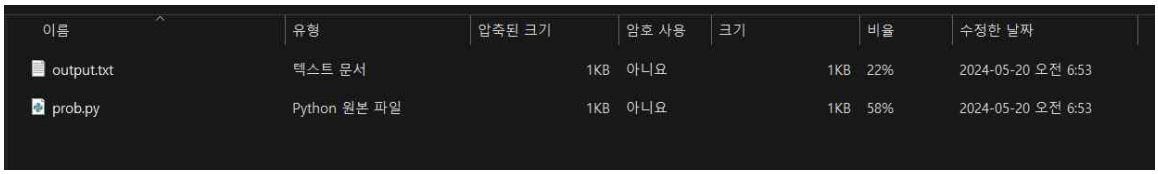
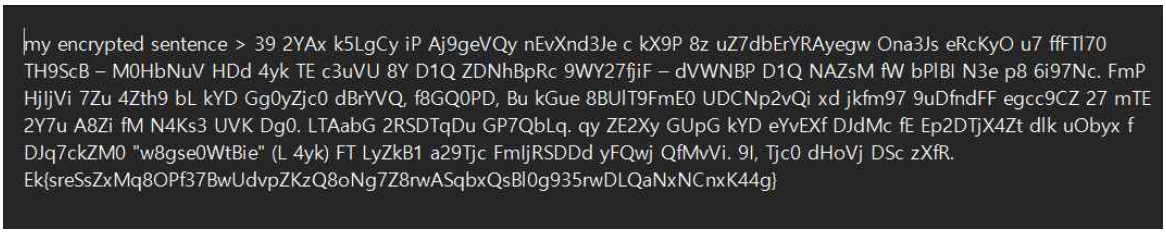
이번 CTF로 암호학에 도전해보기로 했다. 근래에 썼던 SSR 주제가 암호학이라 관심이 더 갔다. 문제를 보면, 비제네레를 아냐고 묻는다. 구글링 해 보니 비제네레는 암호화 방식의 일부이다. 특히 카이사르 암호화 방식을 일부 차용하여 만든 암호화 방식으로 보이는데, 지난번 SSR에서 이 방식에 대해 조사했던 적이 있어서 카이사르 암호의 원리를 잘 생각해보면서 접근해야겠다고 생각했다. 일단 파일을 다운받아줬다.



이름	유형	압축된 크기	암호 사용	크기	비율	수정한 날짜
output.txt	텍스트 문서	1KB	아니요	1KB	22%	2024-05-20 오전 6:53
prob.py	Python 원본 파일	1KB	아니요	1KB	58%	2024-05-20 오전 6:53

텍스트 파일 하나와 파이썬 파일 하나가 있다. 일단 텍스트 파일부터 열어줬다.



```
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 bPlBl 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}
```

my encrypted sentence 라고 나와있다. 이게 암호화된 문장인 것 같다.

다음으로 파이썬 파일을 열어봤다.

C: > Users > ddfgt > AppData > Local > Temp > 96e54ef5-1819-4813-95a7-22f86a767990_87752e5d-9ff2-4e17-aa89

```python
import random
from string import ascii_lowercase, ascii_uppercase, digits

words = ascii_uppercase + ascii_lowercase + digits
class Vigenere:
    def __init__(self, key):
        self._key = key

    def shift(self, a, d):
        if a not in words:
            return a
        index = words.index(a)
        return words[(index + d) % len(words)]

    def encrypt(self, pt):
        ct = ""
        for i in range(len(pt)):
            ct += self.shift(pt[i], self._key[i % len(self._key)])
        return ct

    def decrypt(self, ct):
        pt = ""
        for i in range(len(ct)):
            pt += self.shift(ct[i], -self._key[i % len(self._key)])
        return pt

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

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

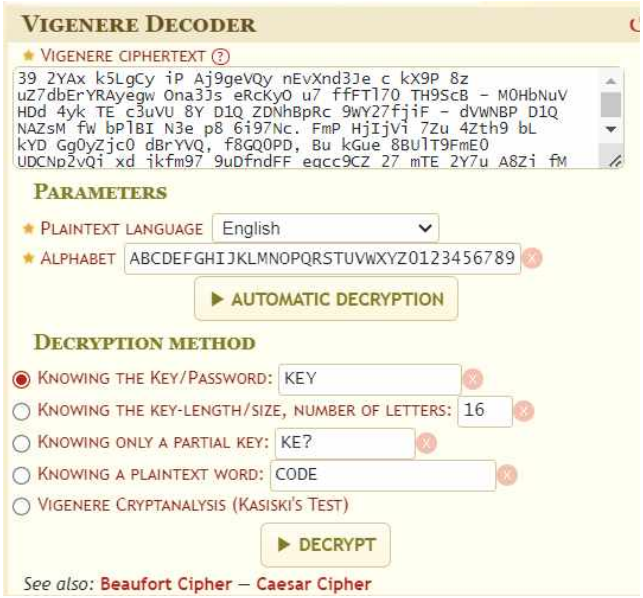
```python
def main():
    key = [random.randint(0, len(words)) for _ in range(16)]
    with open("secret", "r") as f:
        secret = f.read()

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

if __name__ == '__main__':
    main()
```

대충 코드를 봤을 때, 아까 내가 본 텍스트 파일은 이 코드를 실행시켜 만든 텍스트 파일인 것 같다. 일단 코드를 분석해보자.

1. words; 영문 대소문자와 숫자를 포함한다. 텍스트 파일에서 본 것처럼 암호화를 했을 때 보이는 부분이 어떤 문자로 구성될지 설정하는 부분 같다.

2. 비제네레 클래스
 1) init 함수
 : def를 이용해서 init 함수를 만들어줬는데, self와 key가 매개변수로 설정되어있다. (참고: self는 파이썬에서, 클래스 내부에서 가장 첫 번째로 나와야 하는 변수라고 이해) 아마 여기서 key를 정의하는 것 같다.
 2) shift 함수
 : def를 이용해서 shift 함수를 만들어줬는데, 카이사르 암호화 원리가 거의 동일하다고 생각했다. 카이사르 암호는 알파벳을 옆으로 몇 칸 미는 거였다. 이 비제네레 암호도 비슷하게 평문을 몇 칸 밀어서 암호화 하는 방식인 것 같다.
 3) encrypt/decrypt
 : 암호화, 복호화를 구현한 부분인 것 같다. 둘 다 같은 키를 사용했다.
 4) main 함수
 : key가 구현되어 있는 부분이다. 이 비제네레 암호문을 풀 결정적인 단서가 있는 부분이다. 일단 key는 0부터 words의 길이의 정수까지를 만들어낸다. words는 대문자 26개, 소문자 26개, 숫자 10개 총 62개이다. 그러므로 key는 0부터 62까지의 정수로 구성되고, for _ in range 16 이라고 되어 있다. 이는 0-62까지의 숫자 중 16개가 랜덤으로 설정된다는 의미이다. 그러면 key에는 0-62까지의 숫자 중 16개가 랜덤으로 뽑혀 리스트 형식으로 저장이 된다. 추정하건대 아마 이것은 원래의 평문을 다른 알파벳으로 치환하기 위해 얼마나 밀어야 하는지 결정하는 값이 될 것이다.

일단 코드를 분석해봤을 때 이렇다. 그리고 나서 암호문을 해석해보려 구글링을 통해 비제네레 암호를 해독하는 사이트를 찾아 봤는데, key값을 입력하라고 한다. 그런데 16개씩이나 있는 key 리스트의 정수를 뭘 어떻게 입력해야 하는 건지 모르겠다. 어쩌면 내가 생각하는 key 값이 shift의 의미가 아닌가 싶기도 하다.



비제네레 암호 해독 사이트의 모습이다. 보이는 것처럼 내가 뭐라도 알아야 해독을 하는데 코드 상으로는 어떻게 해도 보이지가 않는다.

더 이상 코드를 보기만 해서는 뭐가 안 나올 것 같아서 파이썬에 저 코드를 넣어 실행시켜보기로 한다.

```
======================= RESTART: C:/Users/ddfgt/Desktop/key ==============
Traceback (most recent call last):
  File "C:/Users/ddfgt/Desktop/key", line 38, in <module>
    main()
  File "C:/Users/ddfgt/Desktop/key", line 29, in main
    with open("secret", "r") as f:
FileNotFoundError: [Errno 2] No such file or directory: 'secret'
>>>
```

오류가 뜬다. secret이라는 파일이 없다고 뜨길래 코드를 다시 살펴봤다.

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

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

if __name__ == '__main__':
    main()
```

with open(“secret”,“r”) as f: ... 이 부분이 문제인 것 같다.

secret을 열도록 한 건가 싶어서 위에서부터 어디서 secret이 처음 나오나 찾아봤는데 없다. 그리고 또 의문인 게 f로 저것들을 오픈한다는 것 같은데 f가 뭔지 모르겠다. 이 오류는 모르겠어서 다시 코드로 돌아가본다.

key 리스트에 16개의 정수가 들어간다는 게 아무래도 이해가 잘 안 가서 찾아 보니, 16개의 정수는 평문 중 첫째 자는 리스트의 첫 번째 정수 만큼, 둘째 자는 두 번째 정수 만큼, 셋째 자는 세 번째 정수 만큼...이렇게 해서 암호문 끝까지 도는 것 같다. 혹시나 해서 암호문 글자가 몇 글자인지 보니 583 글자이다.

여기까지 풀었는데 더 이상은 잘 모르겠다. key 리스트에 저장된 정수의 용도는 알겠으나 key 리스트에 저장된 정수가 각각 몇인지도 모르고, 파이썬 코드의 오류는 왜 나는 것이고 어떻게 고쳐야 뭔가 출력되는 결과를 볼 수 있는지도 모르겠다.