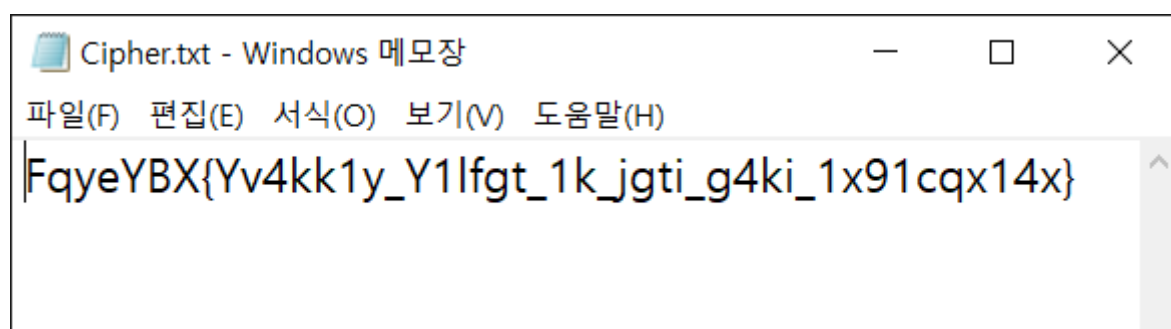


Classic Cipher -3



파일을 다운해서 받아보면 이렇게 적혀있다!



딱봐도 앞에는 HackCTF{~~~}인것 같은데 무슨 암호인지 처음에는 몰라서 찾아보았다.

찾아보니 아핀 암호라는 처음 보는 암호였다.

암호방식을 보면 $(ax + b) \bmod 26$ 으로 암호를 만드는 것 같다.

그래서 FqyeYBK와 HackCTF를 비교해보니

$$a + b \bmod 26 = 19$$

$$24*a + b \bmod 26 = 2$$

$$23*a + b \bmod 26 = 5$$

$$5*a + b \bmod 26 = 7$$

$$4*a + b \bmod 26 = 10$$

이라는 수식들이 나왔다.

$$24*a + b \bmod 26 = 2 \quad 5*a + b \bmod 26 = 7$$

$$23*a + b \bmod 26 = 5 \quad 4*a + b \bmod 26 = 10$$

이렇게 각각 두 개를 보면 $a = 23 + 26*n$ 이라는 것을 알수있다. 어차피 mod 26 으로 나누니 $a = 23$ 이라 하고 풀자!

그럼 이제 간단해보이는 $a + b \bmod 26 = 19$ 여기에 넣으면 $b = 22 + 26*n$ 이라는 것을 알수 있다. 여기서도 마찬가지로 $b = 22$ 라 하고 풀자! 그럼 이제 a와 b를 알았으니 풀면 된다!

```
C = "FqyeYBX{Yv4kk1y_Y1lfgt_1k_jgti_g4ki_1x91cqx14x}"

small = ["a", "b", "c", "d", "e",
         "f", "g", "h", "i", "j",
         "k", "l", "m", "n", "o",
         "p", "q", "r", "s", "t",
         "u", "v", "w", "x", "y",
         "z"]

large = ["A", "B", "C", "D", "E",
        "F", "G", "H", "I", "J",
        "K", "L", "M", "N", "O",
        "P", "Q", "R", "S", "T",
        "U", "V", "W", "X", "Y",
        "Z"]

a = 23
b = 22
for i in C:
    if 97 <= ord(i) <= 122:
        print(small[(a*(ord(i)-97)+b)%26], end="")
    elif 65 <= ord(i) <= 90:
        print(large[(a*(ord(i)-65)+b)%26], end="")
    else:
        print(i, end="")
```