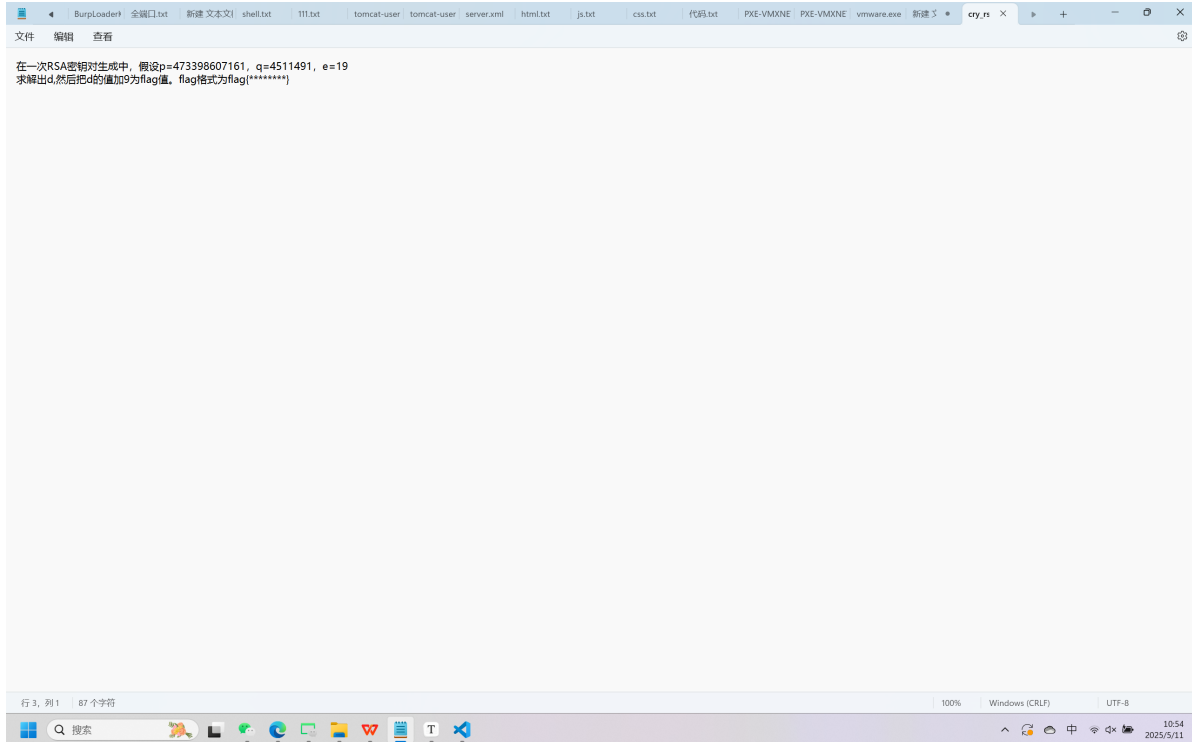


1、cry_rsa

1.获取该题目文件

在一次RSA密钥对生成中，假设 $p=473398607161$ ， $q=4511491$ ， $e=19$
求解出 d ，然后把 d 的值加9为flag值。flag格式为flag{***}这个是题目的文件

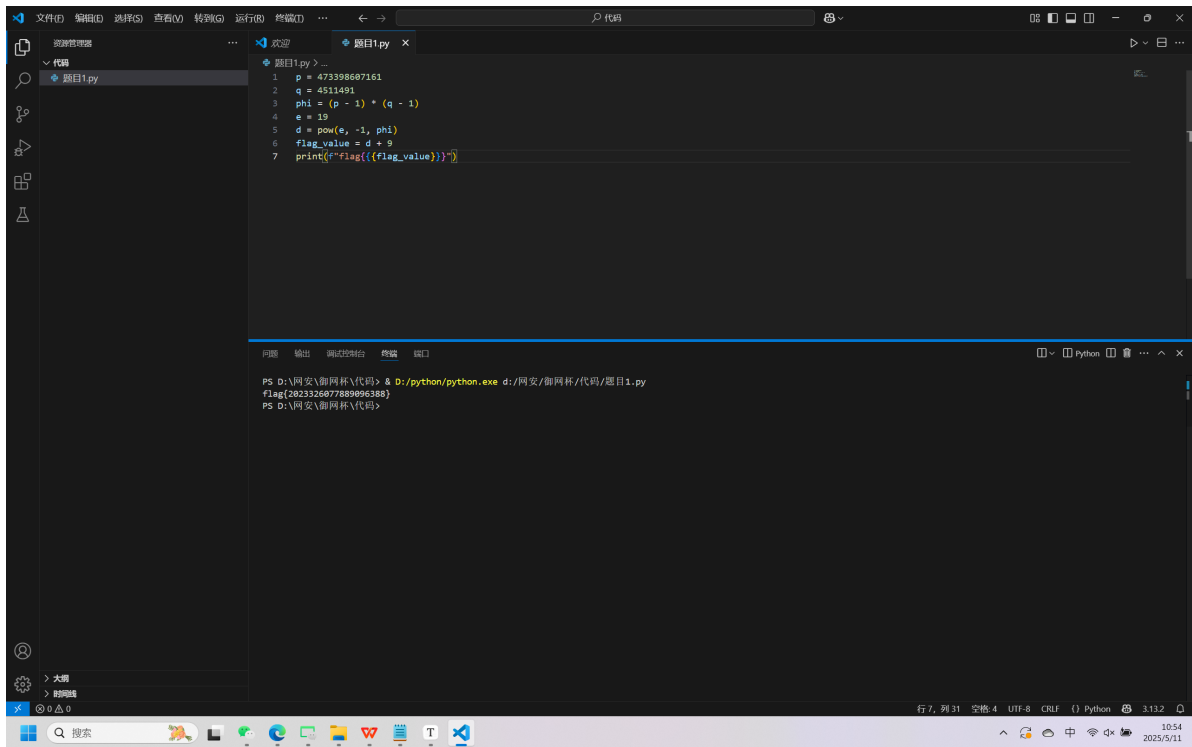


2.题解思路

- 2.1.随意选择两个大的质数 p 和 q ， p 不等于 q ，计算 $N=pq$ 。
- 2.2.根据欧拉函数，不大于 N 且与 N 互质的整数个数为 $(p-1)(q-1)$
- 2.3.选择一个整数 e 与 $(p-1)(q-1)$ 互质，并且 e 小于 $(p-1)(q-1)$
- 2.4.用以下这个公式计算 d ： $d \times e \equiv 1 \pmod{(p-1)(q-1)}$
- 2.5.将 p 和 q 的记录销毁。

3.使用python编码求解

我们直接使用python编码求出 d 和flag

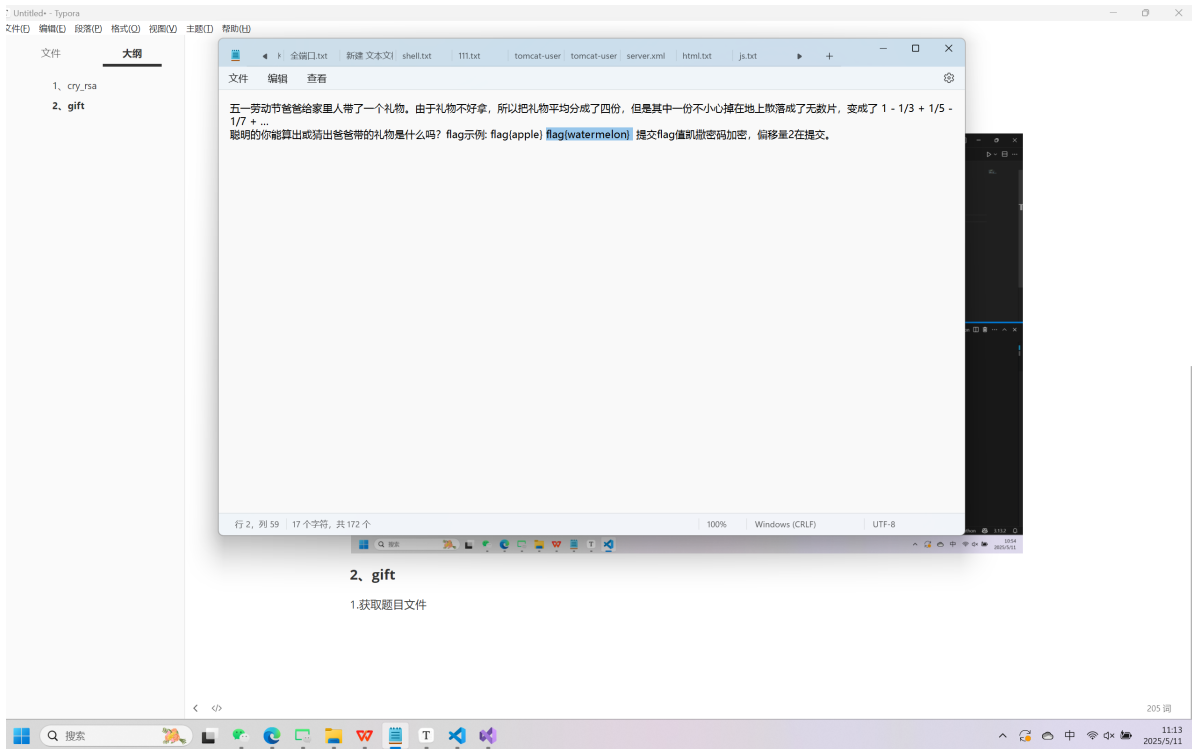


```
1 p = 473398687161
2 q = 4511491
3 phi = (p - 1) * (q - 1)
4 e = 19
5 d = pow(e, -1, phi)
6 flag_value = d + 9
7 print(f"flag{{{flag_value}}}")
```

```
PS D:\网安\御网杯\代码> & D:/python/python.exe d:/网安/御网杯/代码/题目1.py
flag[263236877889863383]
PS D:\网安\御网杯\代码>
```

2、gift

1.获取题目文件



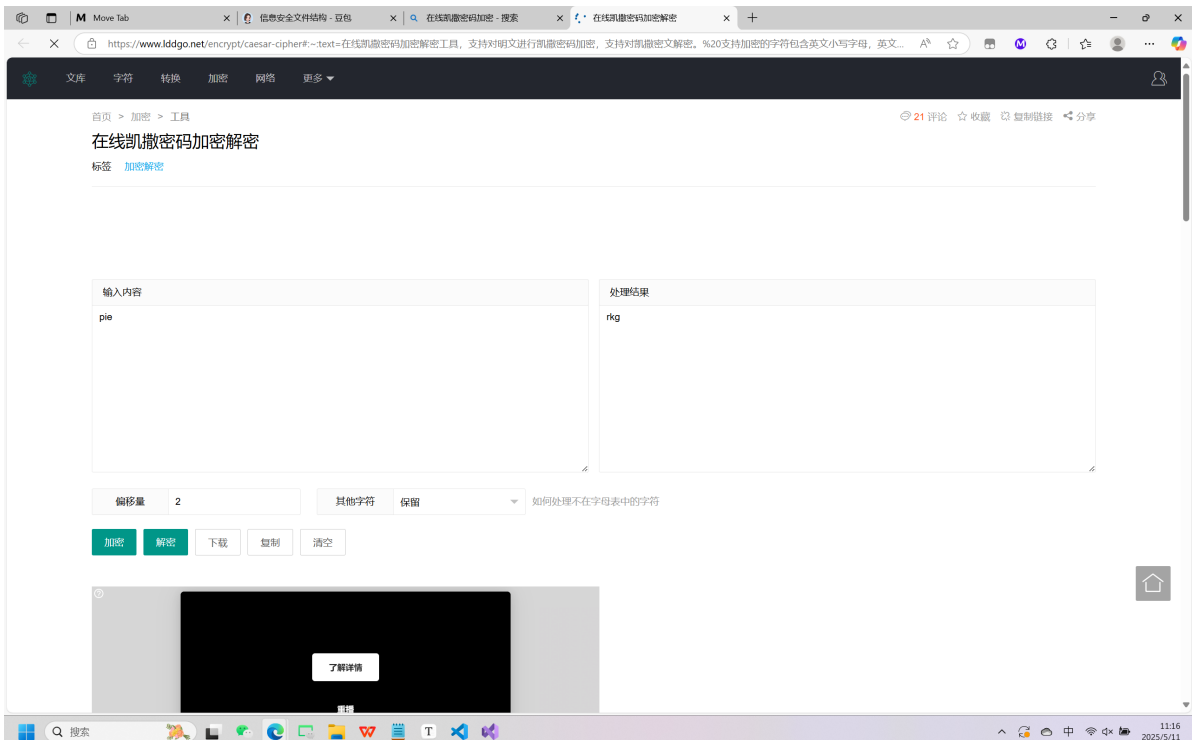
2.题目解析

应为 $1 - 1/3 + 1/5 + \dots$ 是莱布尼兹公式，为 $\pi/4$

那么总和为 π ，常见谐音礼物一个一个试试pizza, pie

3.使用在线凯撒加密工具

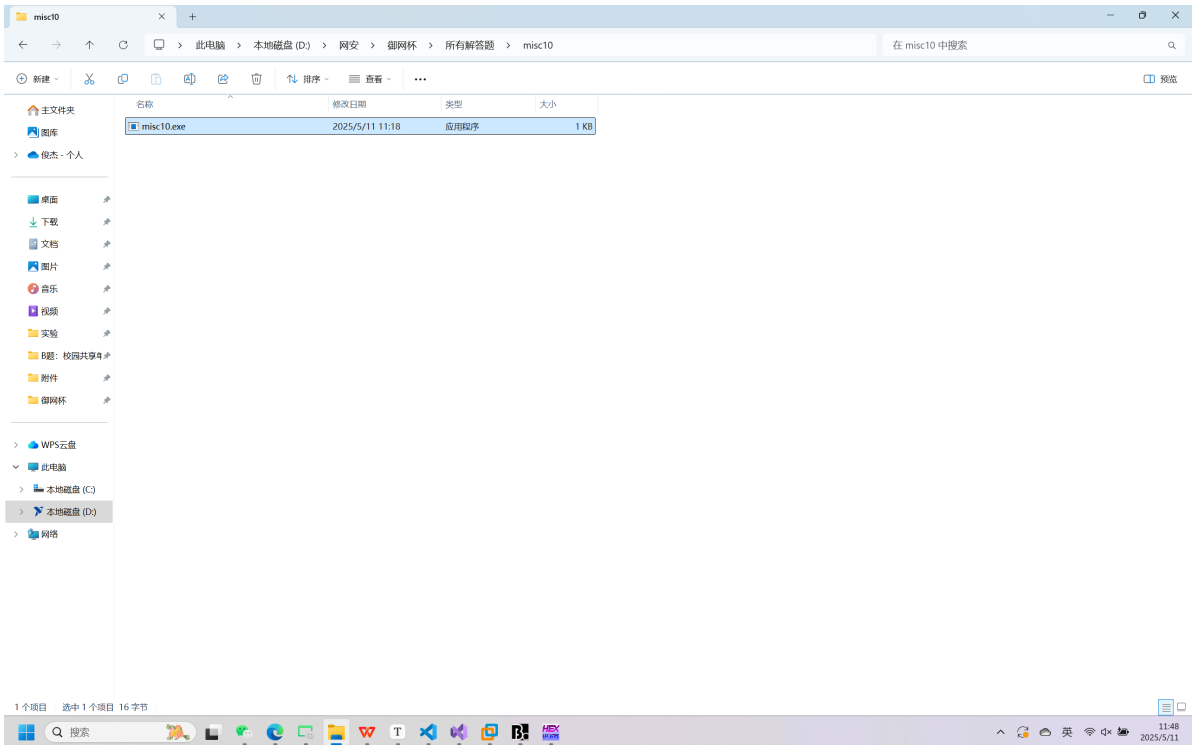
偏移量为2，使用在线凯撒密码加密（偏移量 2）



得出flag{rkg}

3、草甸方阵的密码

1.获取题目

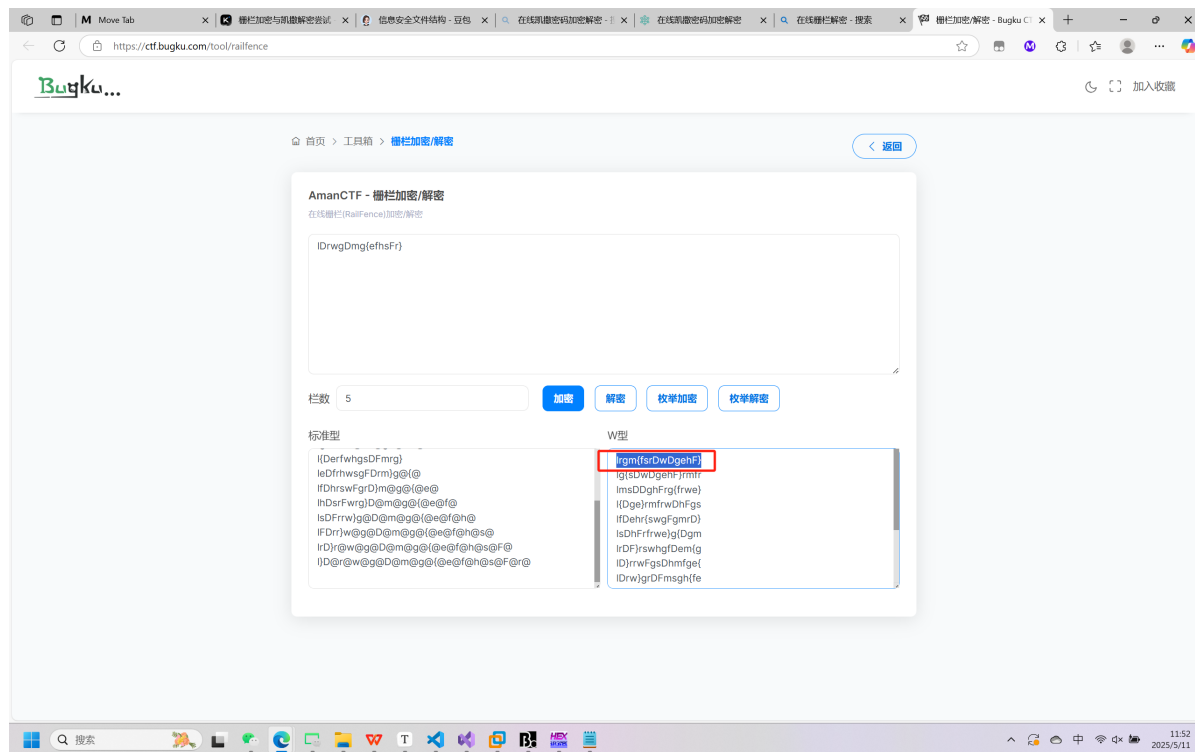


2.题解思路

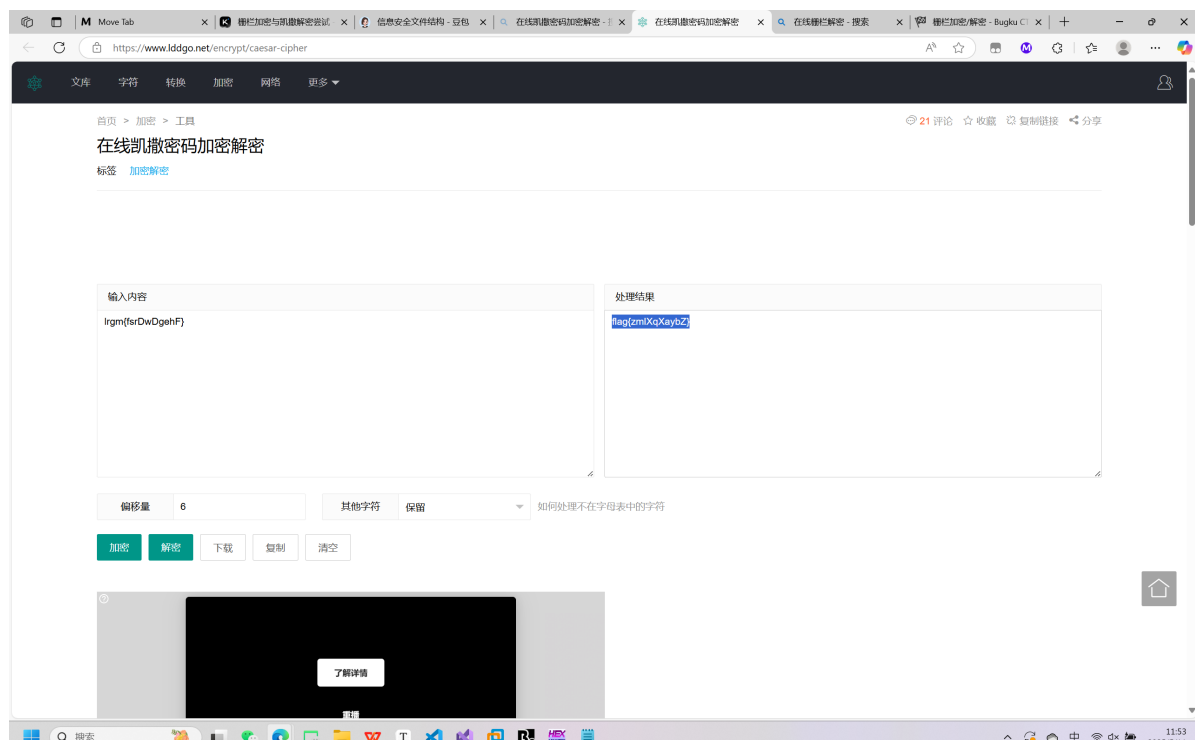
我们先打开，发现又安全问题，打不开，隔离一下，来到虚拟机打开，发现仍然不行，我们用记事本打开，发现字符串IDrwgDmg{efhsFr}，直接交给随波逐流，发现不行，看一下题目思路题目内容：题目描述：考古学家在阿尔卑斯山麓发现了一处古罗马牧羊场遗址，残垣断壁间散落着刻满符号的石板。研究显示，这些符号出自青年时期的凯撒之手——彼时他尚未成为征服高卢的统帅，而是在草甸间放牧的少年。传说中，这位未来的军事天才曾将羊群训练成移动方阵，并用栅栏排列出隐秘的防御阵型

注意传说是说使用栅栏加密，出自凯撒之手，我们试一下用栅栏爆破加密，再用凯撒解密

3.使用栅栏, 凯撒在线加密解密工具



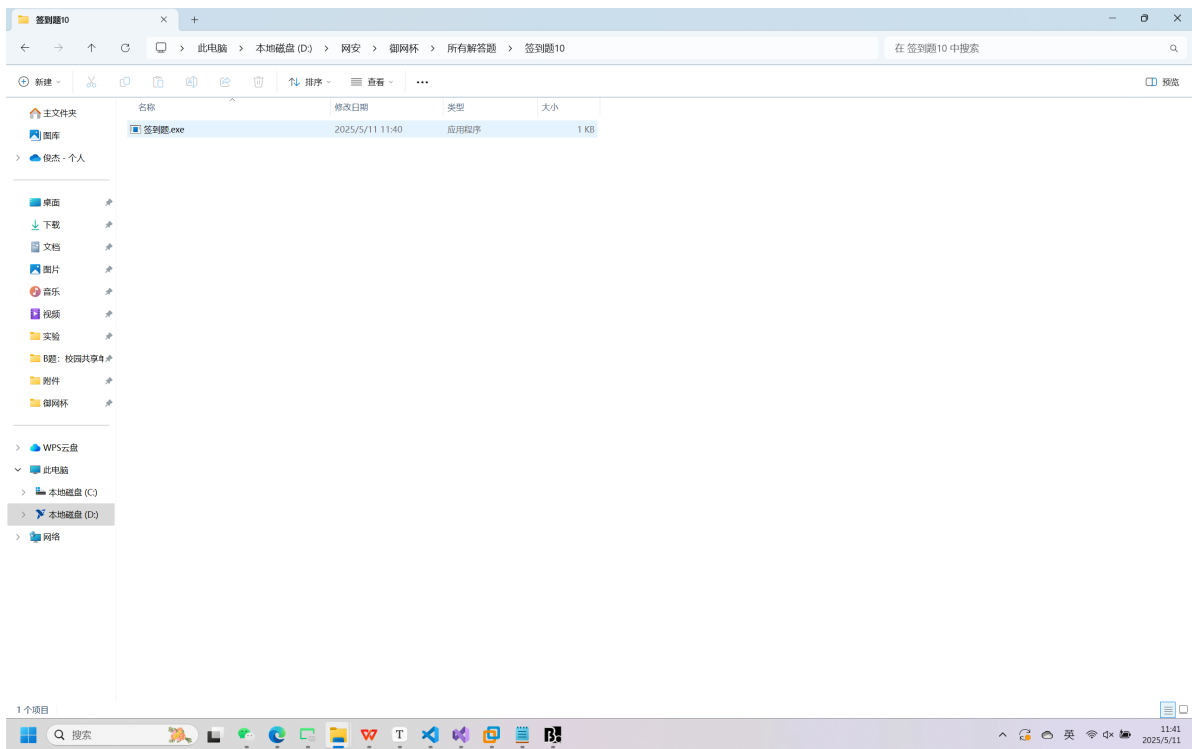
我们看到就这个像flag, 拿走用凯撒试试



偏移量一个一个试试, 发现偏移量为6解除flag

4、easy-签到题

1.获取题目



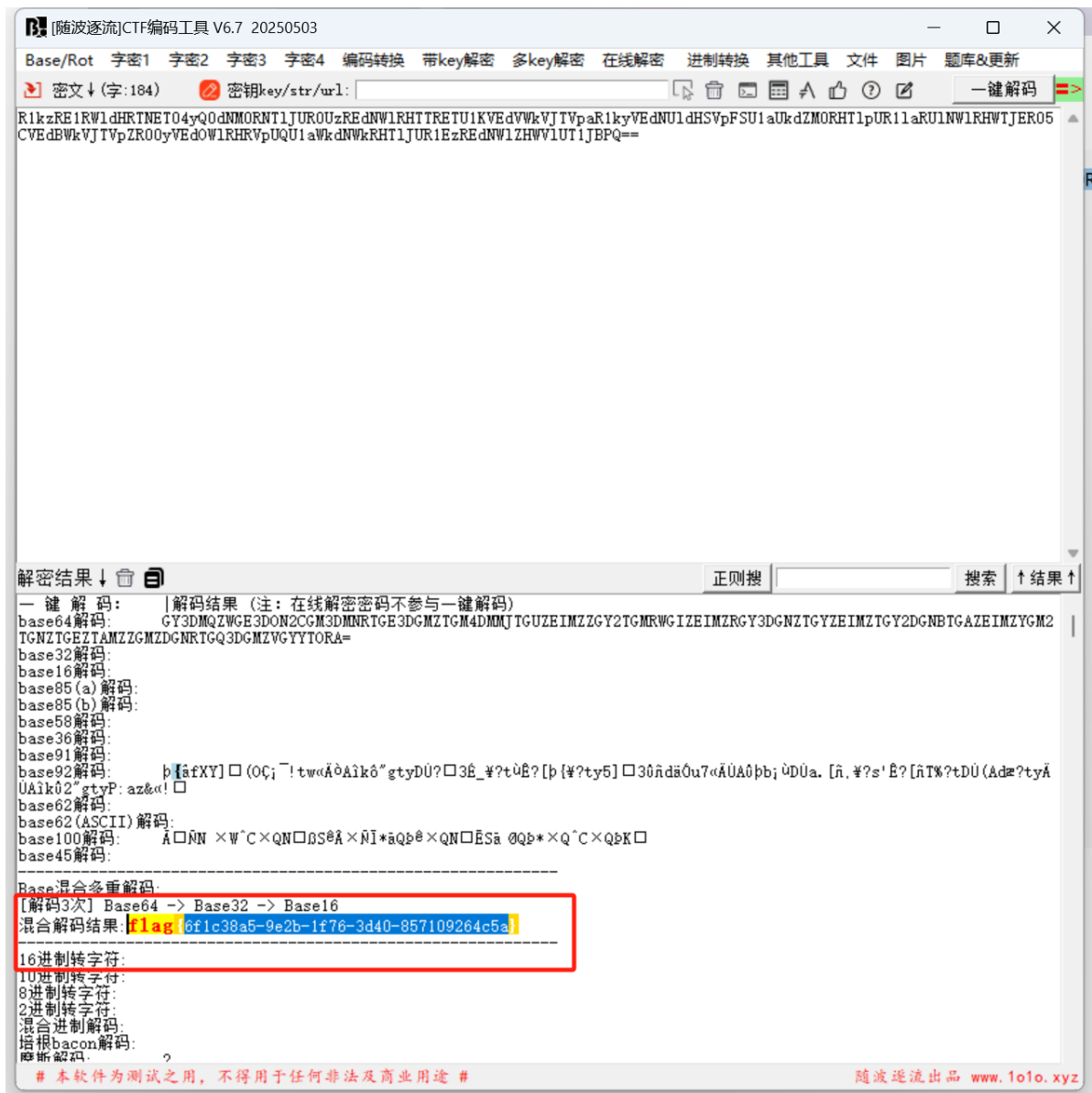
2.题目思路

我们这个题目用记事本打开

```
R1kzRE1RWIdHRTNET04yQ0dNM0RNTIJUR0UzREdNWIRHTTRETU1KVEdVWkVJTVpaR1kyVEdNUIdHSVpFSU1aUkdZM0RHTIpUR1laRUINWIRHWTJE  
R05CVEdBWkVJTVpZR00yVEdOWIRHRVpUQU1aWkdNWkRHTIJUR1EzREdNWIZHWVIUT1JBPQ==
```

以等号结尾，看起来像base加密，直接放入随波逐流

3.使用随波逐流工具



得到flag

5、ez_xor

