ctfshow-吃鸡杯-Crypto-Writeup

原创

mxx307 于 2021-07-12 11:28:13 发布

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_53283643/article/details/118668706

吃鸡杯部分wp

Crypto

Cop! Run!!

题目

```
from Crypto.Util.number import *
from flag import flag

n = 1 << 8
p = getPrime(n)
print(p)

P.<t> = PolynomialRing(Zmod(p))
f = t * t + randrange(p)
print(f)

x = [randrange(p)]
x += [f(x[0])]
print([x_ >> (n - ceil(5 * n / 7)) for x_ in x])

flag = bytes_to_long(flag)
y = f(x[-1])
for i in range(7):
    y = f(y)
    flag ^^= int(y)
print(flag)

'''
92946459607669937513774102250057295249718593723232674702212854287358873135783
t^2 + 43844336985235863734419631630425915388298791521868754583032904718644333115590
[32486428330566350290959207820956263379491135921164952 66, 48839352219196239893444044850254793460281016827817903 92]
19320752909712579377866251905123132260940286615581991593359836739510231390449070254783 3
'''
```

思路

瞅了瞅题目，需要求x[0],x[1]。
给了p,f(t),x[0]和x[1]的高73位。
然后很自然地想到了二元多项式。
设aa,bb为高73位，（x,y）为低位，则有`（aa+x）^2+k-bb-y==0`(k为f(t)函数的randrange (p）)。
想归想，可是手上没有解二元多项式的工具。
之后看到了La神的CopperSmith攻击

企图开始寻找“coppersmith.sage”和这个coron()函数
Luckily，被赵师傅找到了。

```
import itertools


def small_roots(f, bounds, m=1, d=None):
    if not d:
        d = f.degree()

    R = f.base_ring()
    N = R.cardinality()

    f /= f.coefficients().pop(0)
    f = f.change_ring(ZZ)

    G = Sequence([], f.parent())
    for i in range(m + 1):
        base = N ^ (m - i) * f ^ i
        for shifts in itertools.product(range(d), repeat=f.nvariables()):
            g = base * prod(map(power, f.variables(), shifts))
            G.append(g)

    B, monomials = G.coefficient_matrix()
    monomials = vector(monomials)

    factors = [monomial(*bounds) for monomial in monomials]
    for i, factor in enumerate(factors):
        B.rescale_col(i, factor)

    B = B.dense_matrix().LLL()

    B = B.change_ring(QQ)
    for i, factor in enumerate(factors):
        B.rescale_col(i, 1 / factor)

    H = Sequence([], f.parent().change_ring(QQ))
    for h in filter(None, B * monomials):
        H.append(h)
        I = H.ideal()
        if I.dimension() == -1:
            H.pop()
        elif I.dimension() == 0:
            roots = []
            for root in I.variety(ring=ZZ):
                root = tuple(R(root[var]) for var in f.variables())
                roots.append(root)
            return roots

    return []
```

之后直接冲

才艺表演

```
load('coppersmith.sage')
from Crypto.Util.number import *
p=92946459607669937513774102250057295249718593723232674702212854287358873135783
k=43844336985235863734419631630425915388298791521868754583032904718644333115590
flag=19320752909712579377866251905123132260940286615581991593359836739510231390449070254783 3
a=32486428330566350290959207820956263379491135921164952 66
b=48839352219196239893444044850254793460281016827817903 92
aa=a<<73
bb=b<<73
P.<x,y> = PolynomialRing(GF(p))
f=x^2+2*aa*x+aa^2+k-bb-y
roots=small_roots(f,(2^73,2^73),m=3)[0]
x=[aa+roots[0],bb+roots[1]]
P.<t> = PolynomialRing(Zmod(p))
f = t * t + k
y = f(x[-1])
for i in range(7):
    y = f(y)
    flag ^^= int(y)
print(long_to_bytes(flag))
#b'ctfshow{eA5Y__b1var1aN7_c0pper5M17h}'
```

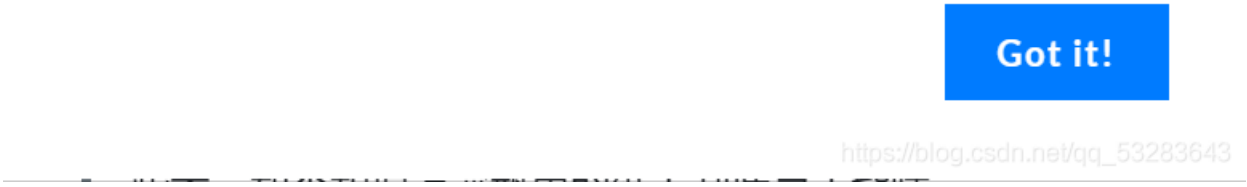
再后来，La神给了一个链接,就是他的CopperSmith攻击。
感谢La神和赵师傅！

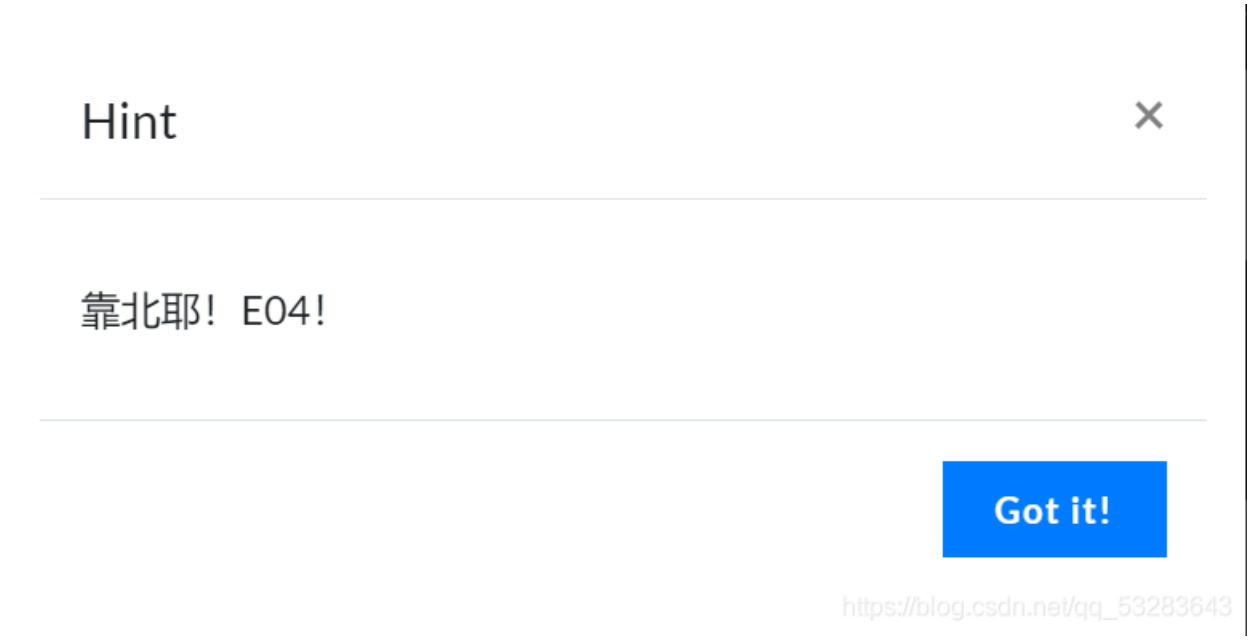
海那边漂来的漂流瓶

给了文本

```
ZJ6 -3 AI6 G8 EL NJ4 EJ/ XJ4 1O3 FU3 RU RUP EJ/ XJ4 S06 54 284 Q/6 J0 ， 5J3 VU04 T;6 2J4 431 EJ/ XU3 。 Y4 1O3 D9 G3 S06 VU/6 ， U VM4 RU/ EJI4 RU XJ/6 G4 、 VUP 1O3 G4 、 W96 1O3 G4 、 WL6 M06 G4 、 VUP 5J6 VU04 、 VUP 5J6 G4 、 AUL6 XU4 VU04 、 W96 5J/ G4 、 5; CJ84 VU04 、 S06 W.6 VU04 、 MP6 XUP6 VU04 、 RU8 U4 VU04 、 RU8 U4 G4 、 W96 S06 G4 、 EL VM/6 G4 、 QU/6 2J/ VU04 。 ZJ6 X94 EK6 2U6 SO4 BJ/6 G4 T QJ6 WL6 1J4 WJ3 QJ6 WL6 QU6 1J4 T QJ6 WL6 2L3 WJ3 QJ6 WL6 QU6 2U6 C04 M3 QUP UP G.3 Y4 AJ3 QUP RU, 。 FU6 5J/ U.6 M6 XJ4 2J04 RU04 GK4 G6 2U6 M/4 2U4 FM3 2K6 JP4 WU6 ， Y94 W96 5J/ G4 M3 5; CJ84 VU04 5 RU0 M06 1P3 U/ E9 G4 S06 1O3 Y.3 VU;4 2U6 ZJ6 -3 AI6 G8 EL NJ4 EJ/ XJ4 CP3 XU4 J94 2U4 G4 T/6 VU04 2J/ VU VU;4 2U6 Y.3 VU;4 ， Y4 S06 1J4 1O3 G;4 VU0 RU/ 5; CJ84 VU04 ZP M 06 VU; ， DJ84 J VU 54 W96 5J/ G4 J4 Z/ FM 、 J B4 FM 5 C.4 ， Y94 VU;4 VU VU/6 54 5; CJ84 VU04 1O3 1J4 2U6 5; C J84 G4 ， U06 J VU （ NJ6 T/ 284 2J4 VU ） VU VU/6 54 5; CJ84 VU04 CK6 AO3 5P4 ， 5J03 EK4 RU, RUP4 56 RUL3 2U6 2 84 J0 ， DJ84 M,4 284 2J4 VU RUP4 BJ4 W96 5J/ G4 C93 VU04 2U4 FM 。 1U,6 J;4 RU4 183 ZJ6 X94 EK6 M/4 VU WU 94 ZJ 3 VU.4 2U6 EK6 G4 1L EJI3 FU3 X96 I6 。 VU; 2JO4 M6 5J/ G0 EL 2; TJ EJO CJ86 G4 U3 TJ04 XU06 W96 J0 VU 04 5J3 UL 4 284 T/6 G4 JO6 AJ4 2U6 ， DL3 XU;6 2L4 QU/6 C/6 2U4 FM Z8 503 、 WJ3 2U4 FM3 2K6 2U6 T/6 1P3 M3 1U4 AU03 2J G4 ZJ4 RUP4 2J03 WJ6 WJ/ FUP6 TK XU.6 YL4 T/6 YJ3 N9 ， ZJ6 -3 AI6 G8 EL NJ4 EJ/ XJ4 2U6 VM03 VU04 RU, DK4 U4 1U4 D9 1J4 ZP BP6 D.3 T.6 AU4 2U6 2J CJO4 FM 1U/4 RU/ EJI4 VM3 2JI M06 1P3 2U 2J4 D9 Z8 2U6 VU; HJP 2U4 294 。
```

给了hint



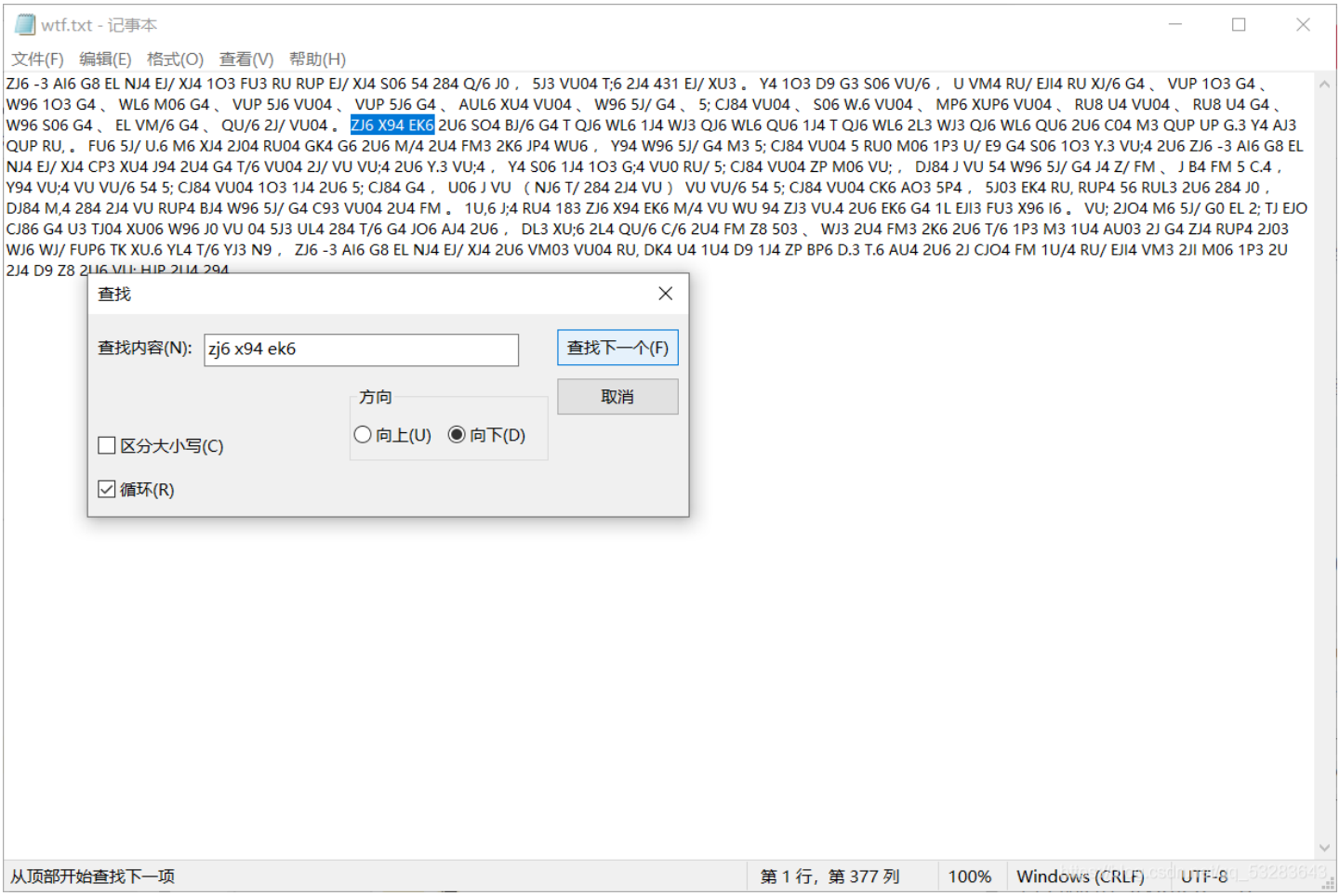


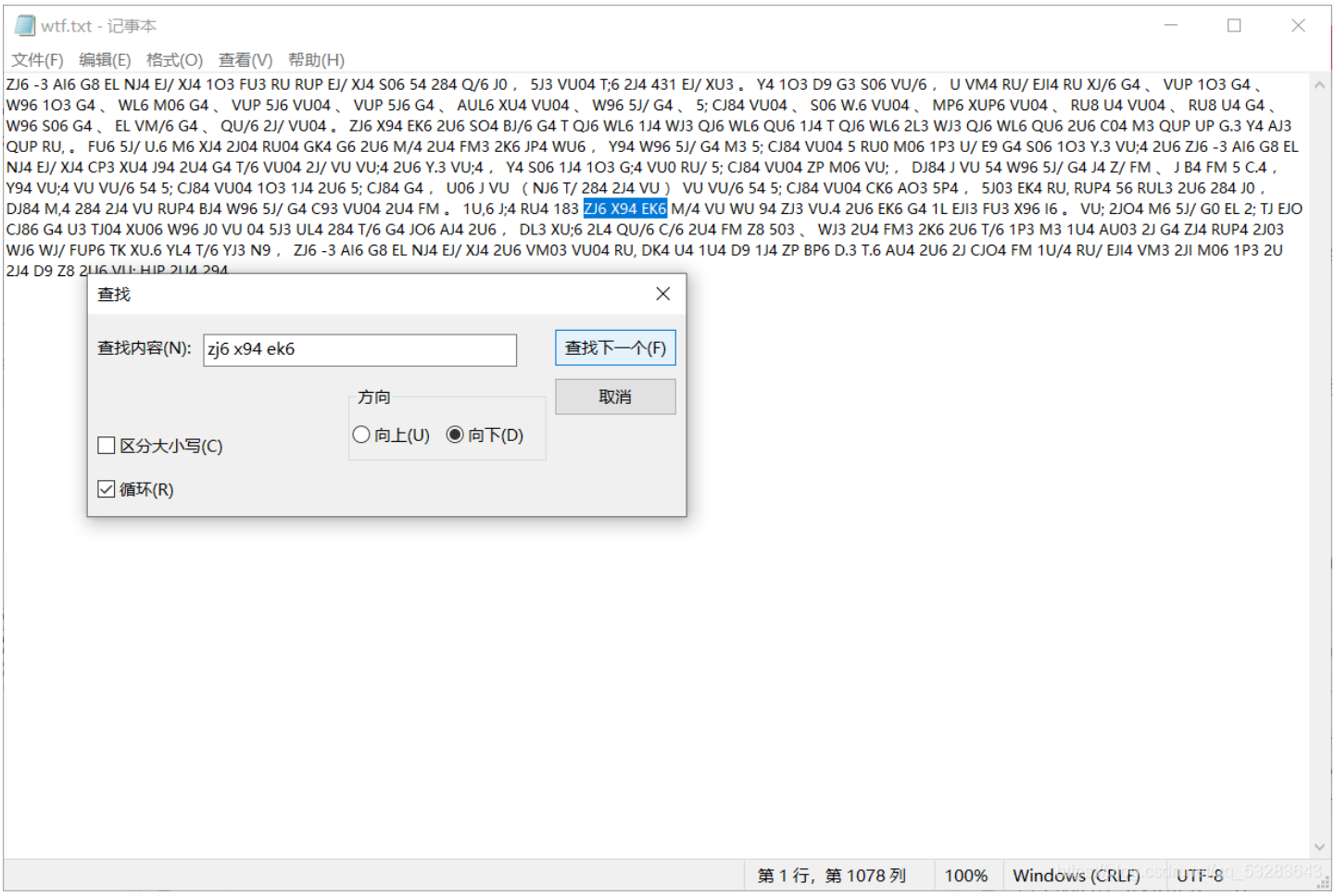
然后又是赵师傅发威，一个神奇的注音，链接。

然后下载下来，Ctrl+f，直接手撸。

开头的时候，发现是福尔摩沙的注音，后想到flag就是`fu lai ge`，直本主题搜`服 来 阁`。

然后再返回去在文本中搜索





发现有两处相同，之后就是手撸了。
第一处大致：

```
flag的内容是吃葡萄不吐葡萄皮不吃葡萄倒吐葡萄皮的汉字注音首字母拼接
```

第二处大致：

```
flag用ctfshow包裹起来
```

得flag

```
ctfshow{cptbtptpbcptdtptp}
```

群主说要出简单的题目大家把这题想简单一点

群主曰：

> 怎么简单怎么来，欢乐为主
>
> AK就AK，我觉得挺好鸭
>
> 让人怪不好意思的.png

嗯，直接`long_to_bytes(c)`

```
sage: from Crypto.Util.number import *
sage: c=75394243346637096036224513941732660494800313932203094459023193105047362873658604511327520366223395541597996117 6
....: 32868679282875095255126864786316054777423793495807239179734140516551272159708569555535692949586191405679903914010
....: 26143967170757484178933053119853432542201587362176948996959661480228276440166100656454615967439735668365031814272
....: 00927382799717969698892659967221348284815075105435159538640259700060168464420755973549903166636122203861547515404
....: 45364971920330418730955600466092622618235344566170235238065435287461708441983433834392588059302330723876845250996
....:
sage: print(long_to_bytes(c))
b'WINNER WINNER CHICKEN DINNER! This is easy but quite troll man. One should NOT expect that the ciphertext is equal to
plaintext in the real world. Flag is: ctfshow{xielunyan___KAI!}. By the way, what a stupid encryption exponent it is!\n
sage:
```



```
ctfshow{xielunyan___KAI!}
```

The Dedication of Suspect M

看了春哥的wp，直呼：妙啊~

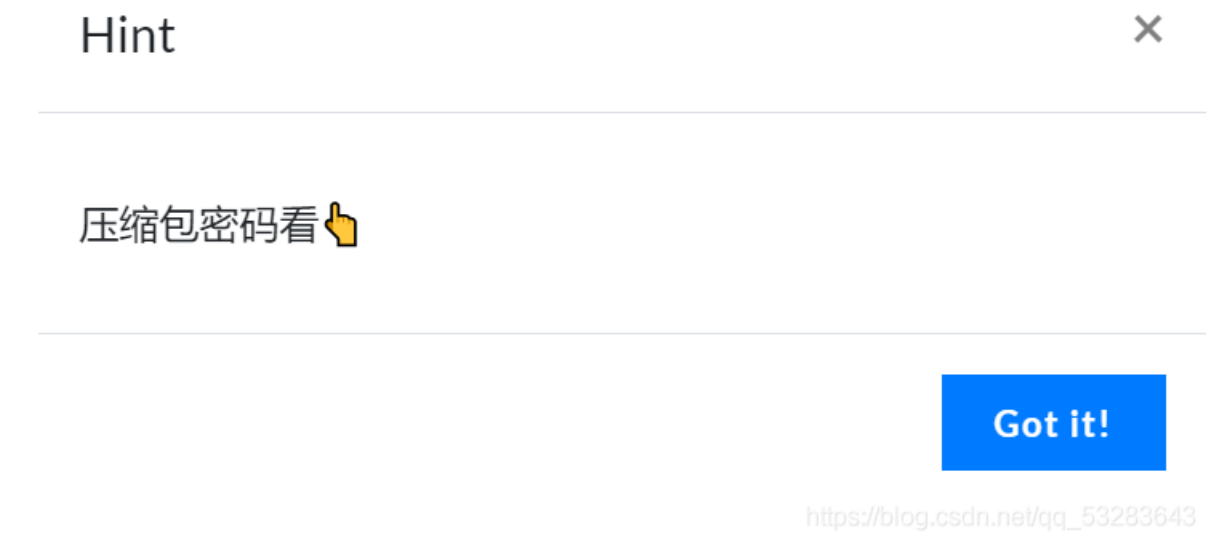
```
with open('M', 'rb') as f:
    s = f.read()
a=0x5b-0x20 ####010 editor查看，看见大部分相同的16进制，这里的a使得 16进制 + a== 0x32 (Space)#############
t = bytes([(x - a)%128 for x in s])
print(t.decode())

with open('gao.txt', 'wb') as f:
    f.write(t)
```

注：010 editor查看，看见大部分相同的16进制，这里的a使得 16进制 + a== 0x20 (Space)

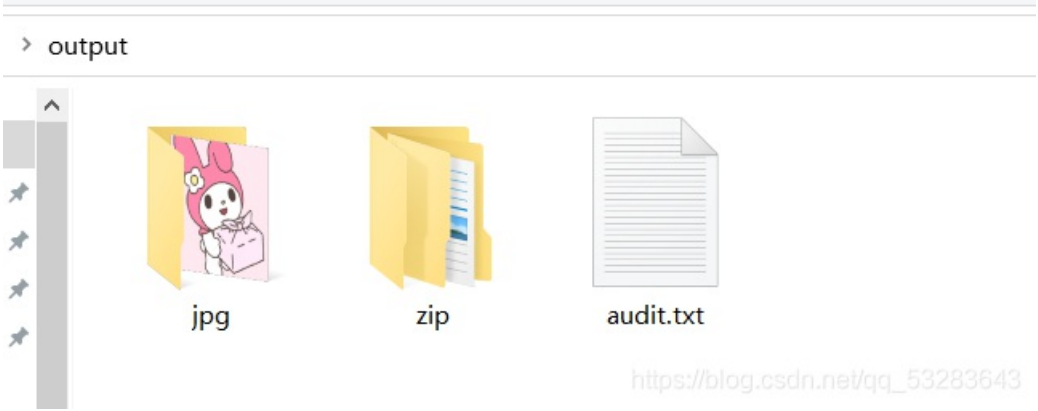
```
Process finished with exit code 0
```


Misc

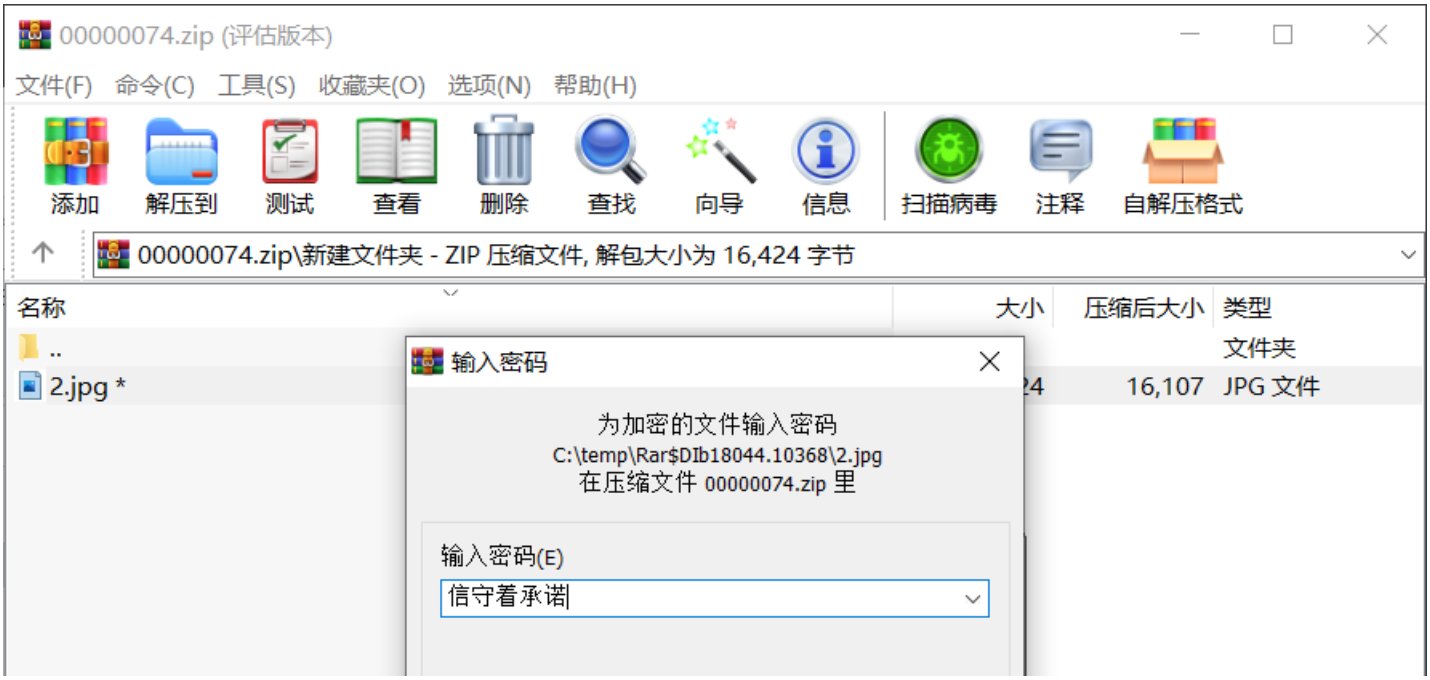
信守着承诺

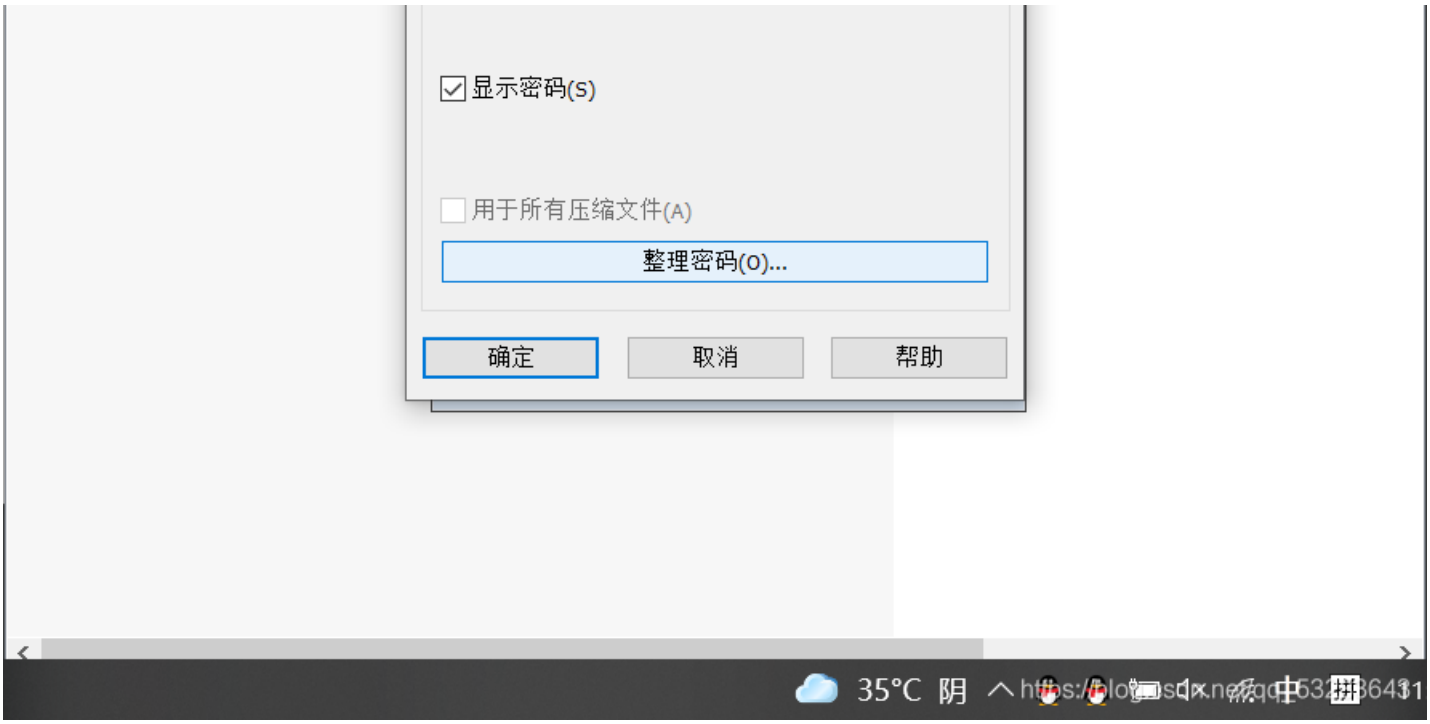


小手很灵性
直接foremost 分解，一张图片，一个加密的压缩包

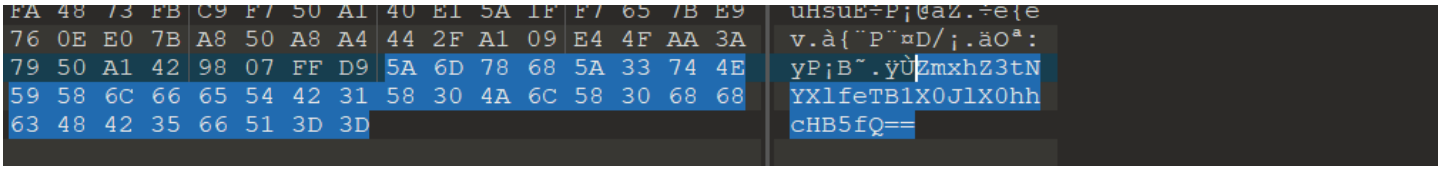


密码：信守着承诺（题目名，小手很灵性）





然后010 Editor查看压缩包里的图片
在最后看见了base64编码




```
flag{May_y0u_Be_Happy}
```

I am happy!