week2-writeup-6vv+

Reverse

fake_debugger beta

先输入个hgame{aaaaaaaaaaaaaa}试试

```
eax: 127
ebx: 23
ecx: 0
zf: 0               h
--------------INFO--------------

eax: 127
ebx: 127
ecx: 0
zf: 1
--------------INFO--------------

eax: 74
ebx: 45
ecx: 1
zf: 0               g
--------------INFO--------------

eax: 74
ebx: 74
ecx: 1
zf: 1
--------------INFO--------------

eax: 34
ebx: 67
ecx: 2
zf: 0               a
--------------INFO--------------

eax: 34
ebx: 34
```

```
ecx: 2
zf: 1
--------------INFO--------------

eax: 52
ebx: 89
ecx: 3
zf: 0               m
--------------INFO--------------

eax: 52
ebx: 52
ecx: 3
zf: 1
--------------INFO--------------

eax: 104
ebx: 13
ecx: 4
zf: 0               e
--------------INFO--------------

eax: 104
ebx: 104
ecx: 4
zf: 1
--------------INFO--------------

eax: 99
ebx: 24
ecx: 5
zf: 0               {
--------------INFO--------------

eax: 99
ebx: 99
ecx: 5
zf: 1
--------------INFO--------------

eax: 66
ebx: 35
ecx: 6
zf: 0               a
```

可以看到，输入不同字符会改变eax的值，而正确的字符的ascii码为eax异或ebx，然后正确的eax值是zf=1时ebx的值，因此只需要计算每一轮zf分别等于0和1时ebx的值的异或，ecx表示循环次数，可以用来判断第几位字符

```
eax: 65
ebx: 35
ecx: 6
zf: 0
--------------INFO--------------

eax: 65
ebx: 122
ecx: 6
zf: 1               122 xor 35 = 89 (Y)
--------------INFO--------------
```

以此一位一位地类推，得到flag

`hgame{You_KnOw_debuGg3r}`

就是有点费键盘

crypto

whitegiveRSA

公钥与私钥的产生：

(1)进行加密之前，首先找出2个不同的大质数p和q

(2)计算n=p*q

(3)根据欧拉函数，求得φ(n)=φ(p)φ(q)=(p−1)(q−1)

(4)找出一个公钥e，e要满足: 1<e<φ(n) 的整数，且使e和φ(N)互质。

(5)根据e*d除以φ(n)余数为1，找到私钥d。

(6)所以,公钥就是(n,e) 私钥就是(n,d)

消息加密:

m^e除以n求余数即为c(密文)

$$m^e \equiv c \pmod{N}$$

消息解密:

c^d除以n求余数即为m(明文)

$$c^d \equiv m \pmod{N}$$

```
import gmpy2
n=882564595536224140639625987659416029426239230804614613279163
#这里我用yafu分解了n
p=857504083339712752489993810777
q=1029224947942998075080348647219
e=65537
c=747831491353896780365654517748216624798517769637260742155527
phi=(p-1)*(q-1)
d=gmpy2.invert(e,phi)
m=pow(c,d,n)
print(hex(m))
print(binascii.unhexlify(hex(m)[2:].strip("L")))
```

```
└─$ python2 main.py
0x6867616d657b7730777e794f555f6b4e6f572b523540217d
hgame{w0w~yOU_kNoW+R5@!}
```

gcd or more?

e=2，用上一题的脚本显示找不到d，百度到了rabin加密

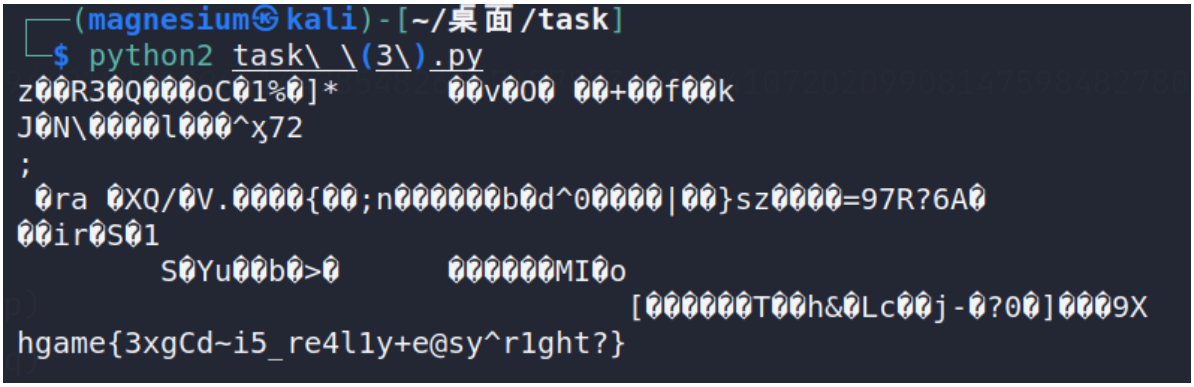
`https://en.wikipedia.org/wiki/Rabin_cryptosystem`

然后题目直接给出了p和q，不用手动分解n，就直接套公式解，从四个输出中找可能存在的真正明文

exp

```
import gmpy2
import libnum
p =
852285650211289018533149345831290834419890452250225412985505704493898396090l9
q =
111614714641364911312915294479850549131835378046002423977989457843071188836271
n = p * q
#cipher = pow(s2n(FLAG), 2, n)
#print(cipher)
c=766500368283066645619389449101598964164785482664717787314198410720209908147598
482780600728783047289961681808090727660674446745344590892305497539362350953 9
e=2


mp = pow(c, (p + 1) / 4, p)
mq = pow(c, (q + 1) / 4, q)
yp = gmpy2.invert(p, q)
yq = gmpy2.invert(q, p)
r = (yp * p * mq + yq * q * mp) % n
rr = n - r
s = (yp * p * mq - yq * q * mp) % n
ss = n - s
print libnum.n2s(r)
print libnum.n2s(rr)
print libnum.n2s(s)
print libnum.n2s(ss)
```



`hgame{3xgcd~is~really~difficult}(狗头）`

signin

#竟是数学题

c=a^p*m（mod p)

c=(a^p%p)*(m%p)%p

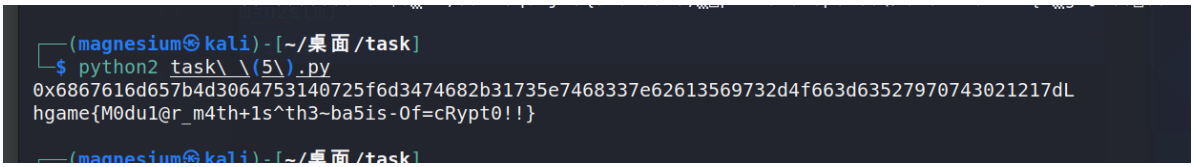
c=(a%p)*(m%p)%p　　#费马小定理

c=a*(m%p)%p

c*a^(p-2)=m%p　　#费马小定理

exp

```
a =
14347617014491508602065146132804933965669212695481800365009985286814584131904147
00730205871252139769254743410765056422278534076760587731138858658266406800231473
60447444464935801614525784110903480871654141802517672864060026452463495645509064
41425914356198841617660999185442192960753424283474312465249102209028 9
p =
14499045644623014469426369441876985849502147504339227918392565017406200417855984
44010863606079285117145064424955156641766462307695540231790402269571529814429934
92885354384799122222074255748702871095896167656675843624069307328779207379633792
65516054427154556991751196386512013558987593993749401088965883113079 7
c =
12009438288562742680204393193683347157587888452397476776456274759224360811784748
21257228593634440690942685788130344068590879058081083316199183942139081844484300
84247326673068817903131008945590119114470183031722078599931222887555377046173518
11161823941097906128492506187153832457787141992887407518049403705760 1
p2=p-2
am=pow(a,p2,p)
cm=c*am
m=cm%p
print(hex(m))
m=n2s(m)
print(m)
```

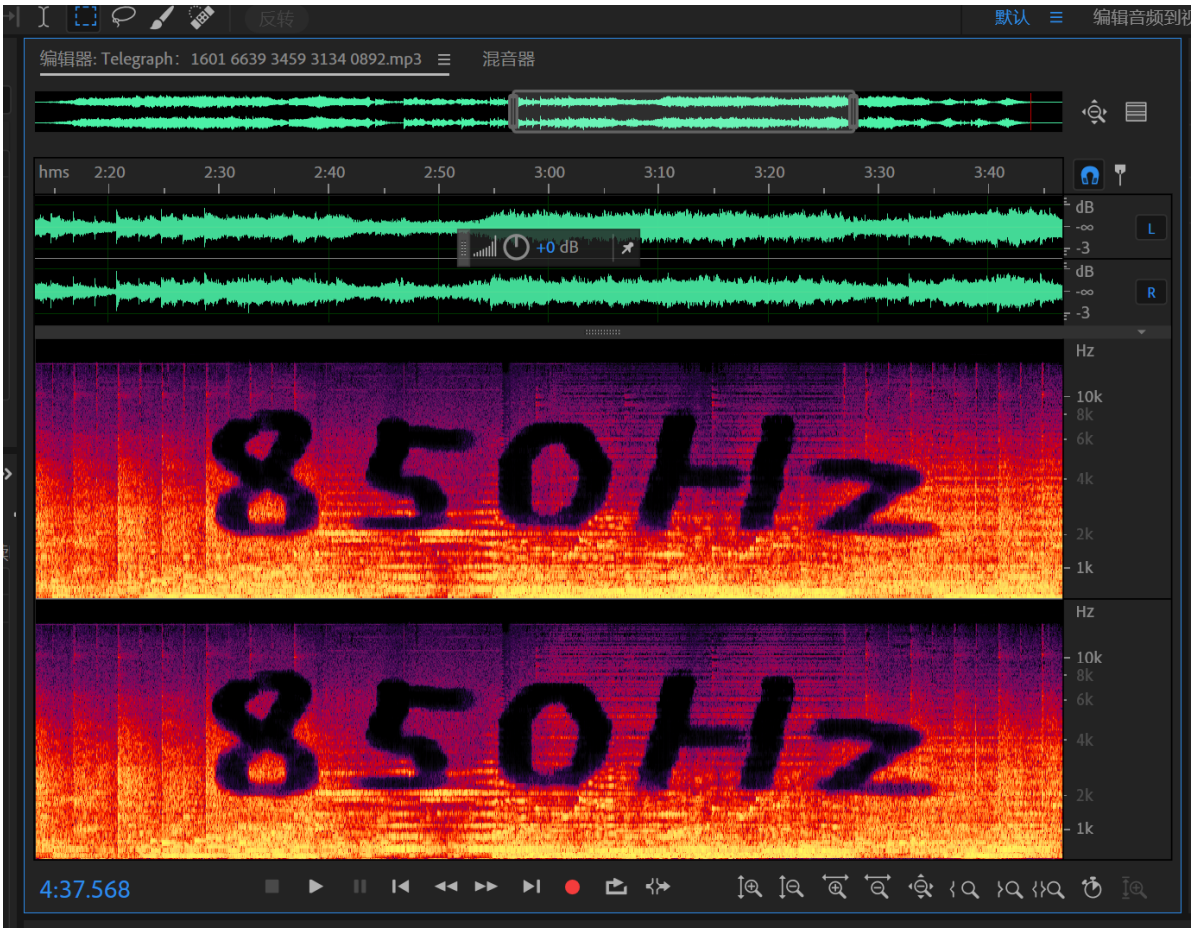


misc

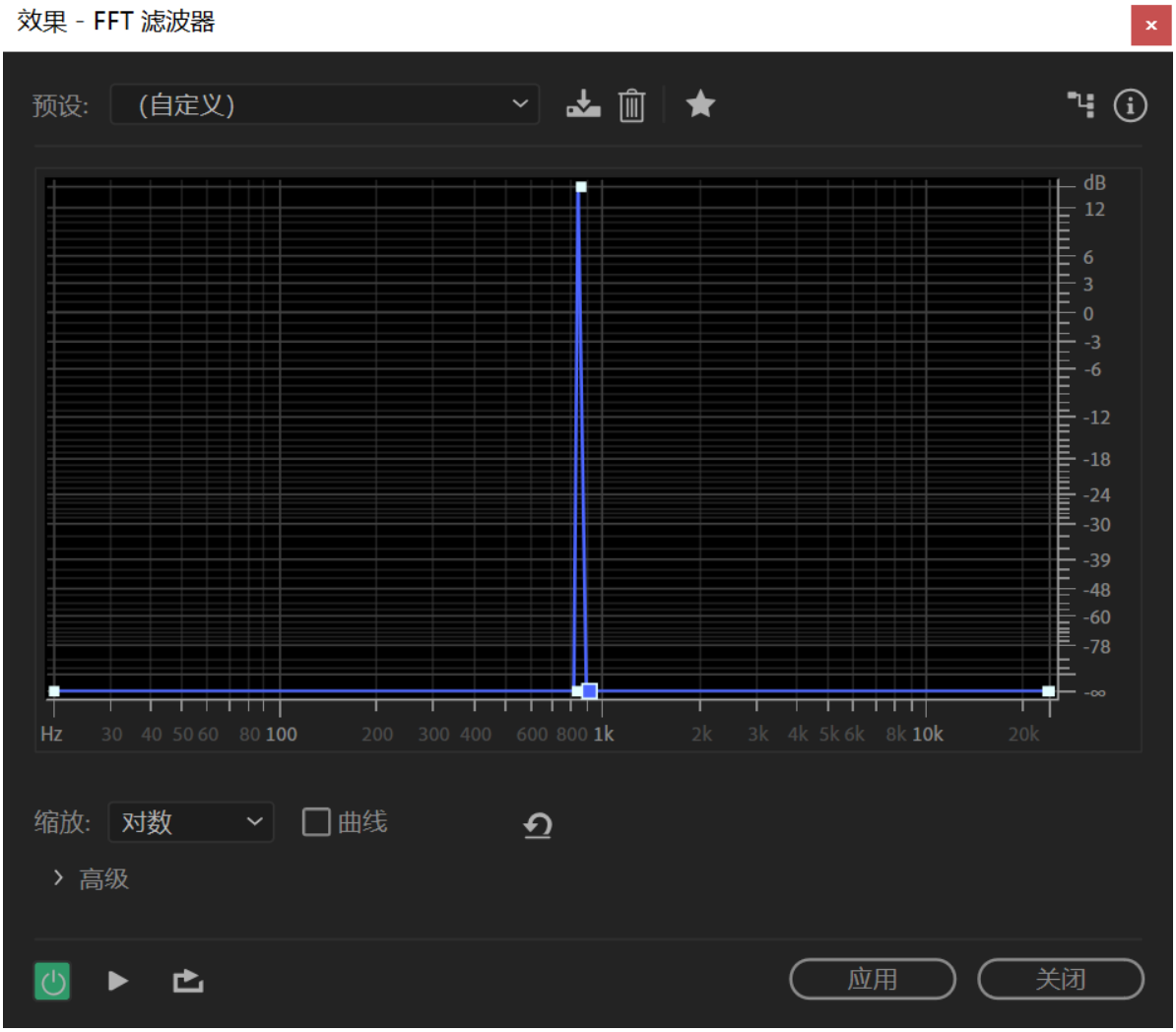
Telegraph：1601 6639 3459 3134 0892

这名字很可疑，百度一下，我就知道

好吧，那咱打开au，显示频谱



打开滤波器，过滤850Hz



oh我的上帝，这熟悉的点杠隔

然后把莫斯电码写下来

-.--/---/..-/.-./..-./.-../.-/--./../.../---.../....-/--./-----/-----/-../.../-----/-./--./-.../..-/-/-./-----/-/....-/--./-----/-----/-../--/.-/-./-----/...--/----./...--/.----/-----/-.-/..

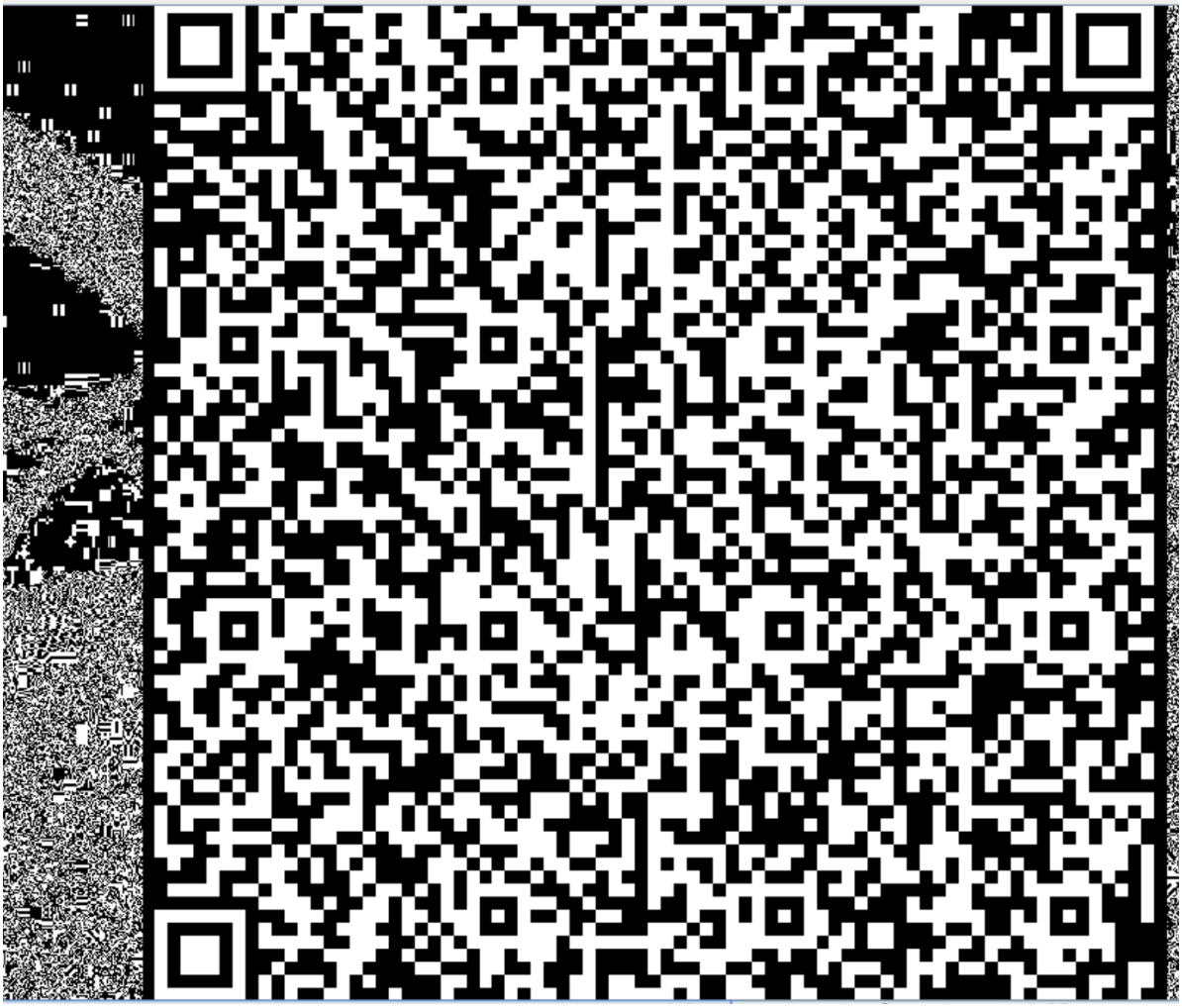
解密得

`yourflagis:4gOOdsOngbutnOt4gOOdmanO39310ki`

转化大写包上hgame{}就能交

Hallucigenia

放进stegsolve康康有小惊喜



扫一扫

```
gmBCrkRORUkAAAAA+jrgsWajaqOBeC3IQhCEIQhCKZw1MxTzSlNKnmJpivW9IHVPrTjvkkuI3sP7bWAE
dIHWCbDsGsRkZ9IUJC9AhfZFbpqrmZBtI+ZvptWC/KCPrLOgFeRPOcI2WyqjndfUWlNj+dgWpe1qSTEc
durXzMRAc5EihsEflmIN8RzuguWq61JWRQpSI51/KHHT/6/ztPZJ33SSKbieTa1C5koONbLcf9aYmsVh
7RW6p3SpASnUSb3JuSvpUBKxscbyBjiOpOTq8jcdRsx5/IndXw3VgJV6iO1+6jl4gjVpWouViO6ih9Zm
ybSPkhaqyNUxVXpV5cYU+Xx5sQTfKystDLipmqaMhxIcgvplLqF/LWZzIS5PvwbqOvrSlNHVEYchCEIQ
ISICSZJijwu5OrRQHDyUpaF0y///p6FEDCCDFsuW7YFoVEFEST0BAACLgLOrAAAAAggUAAAAtAAAAFJE
SEkNAAAAChoKDUdOUIk=
```

b64解出来看见行末有个GNP.根据题目应该是要翻转过来

```
00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F
-----------------------------------------------------------------
82 60 42 AE 44 4E 45 49  00 00 00 00 FA 3A E0 B1   | .`B.DNEI.....:..
66 A3 6A AD 01 78 2D C8  42 10 84 21 08 42 29 9C   | f.j..x-.B..!.B).
35 33 14 F3 4A 53 4A 9E  62 69 8A F5 BD 20 75 4F   | 53..JSJ.bi... uO
AD 38 EF 92 4B 88 DE C3  FB 6D 60 04 74 81 D6 09   | .8..K....m`.t...
B0 EC 1A C4 64 67 D2 14  24 2F 40 85 F6 45 6E 9A   | ....dg..$/@..En.
AB 99 90 6D 23 E6 6F A6  D5 82 FC A0 8F AC BD 20   | ...m#.o........
15 E4 4F 39 C2 36 5B 2A  A3 9D D7 D4 5A 53 63 F9   | ..O9.6[*....ZSc.
D8 16 A5 ED 6A 49 31 1C  76 EA D7 CC C4 40 73 91   | ....jI1.v....@s.
22 86 C1 1F 96 62 0D F1  1C EE 82 E5 AA EB 52 56   | ".....b........RV
45 0A 52 23 9D 7F 28 71  D3 FF AF F3 B4 F6 49 DF   | E.R#..(q......I.
74 92 29 B8 9E 4D AD 42  E6 4A 0E 35 B2 DC 7F D6   | t.)..M.B.J.5....
98 9A C5 61 ED 15 BA A7  74 A9 01 29 D4 49 BD C9   | ...a....t..).I..
B9 2B E9 50 12 B1 B1 C6  F2 06 38 8E A4 E4 EA F2   | .+.P......8.....
37 1D 46 CC 79 FC 89 DD  5F 0D D5 80 95 7A 88 ED   | 7.F.y..._....z..
7E EA 39 78 82 35 69 5A  8B 95 88 EE A2 87 D6 66   | ~.9x.5iZ.......f
C9 B4 8F 92 16 AA C8 D5  31 55 7A 55 E5 C6 14 F9   | ........1UzU....
7C 79 B1 04 DF 2B 2B 2D  0C B8 A9 9A A6 8C 87 12   | |y...++-........
1C 82 FA 65 2E A1 7F 2D  66 73 21 2E 4F BF 06 EA   | ...e...-fs!.O...
3A FA D2 94 D1 D5 11 87  21 08 42 10 21 22 02 49   | :.......!.B.!".I
92 62 8F 0B B9 D2 B4 50  1C 3C 94 A5 A1 74 CB FF   | .b.....P.<...t..
FF A7 A1 44 0C 20 83 16  CB 96 ED 81 68 54 41 44   | ...D. ......hTAD
49 3D 01 00 00 8B 80 B3  AB 00 00 00 02 08 14 00   | I=..............
00 00 B4 00 00 00 52 44  48 49 0D 00 00 00 0A 1A   | ......RDHI......
0A 0D 47 4E 50 89                                 | ..GNP.
```

反转后保存成png文件，是一个长得很别致的flag

翻转一下就好

hgame{tenchi_souzou_dezain_bu}