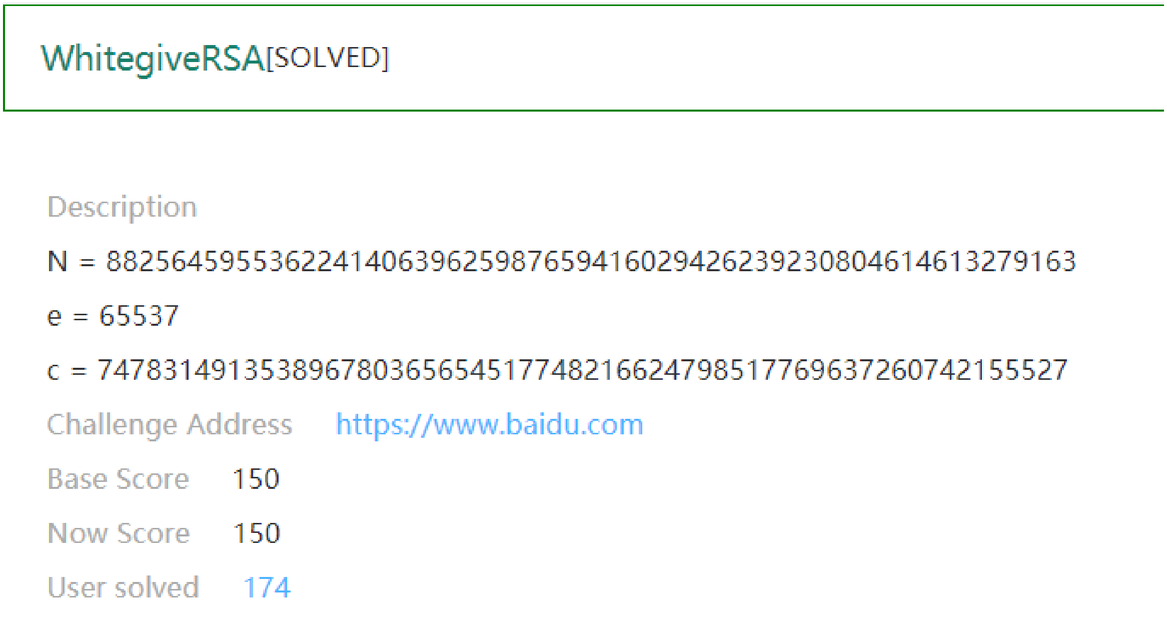
HGAME 2020 Week2 wp

sage 就做了一题白给的保命。

WhitegiveRSA



WhitegiveRSA[SOLVED]

Description

N = 882564595536224140639625987659416029426239230804614613279163

e = 65537

c = 747831491353896780365654517748216624798517769637260742155527

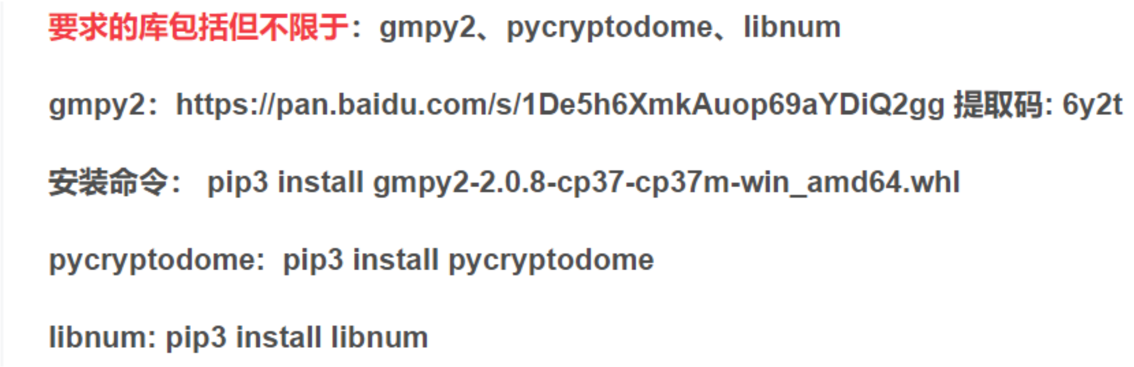
Challenge Address https://www.baidu.com

Base Score 150

Now Score 150

User solved 174

百度，得到RSA学习资料 https://blog.csdn.net/vhkjhwbs/article/details/101160822



要求的库包括但不限于：gmpy2、pycryptodome、libnum

gmpy2：https://pan.baidu.com/s/1De5h6XmkAuop69aYDiQ2gg 提取码: 6y2t

安装命令： pip3 install gmpy2-2.0.8-cp37-cp37m-win_amd64.whl

pycryptodome：pip3 install pycryptodome

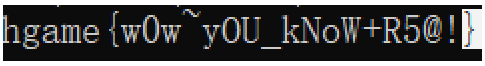
libnum: pip3 install libnum

配置好一些必要的环境（~~狗头，这是关键~~），贴一个已知 p,q,e,c 求 m 的脚本（题目中 n,e 不太大，n 先用 yafu 分解为 q 和 p）

```
# coding:utf8

p = 857504083339712752489993810777
q = 1029224947942998075080348647219
e = 65537
c = 747831491353896780365654517748216624798517769637260742155527

# 计算d
```

```python
def egcd(a, b):
  if a == 0:
    return (b, 0, 1)
  else:
    g, y, x = egcd(b % a, a)
    return (g, x - (b // a) * y, y)

d = egcd((p - 1) * (q - 1), e)[2]
if d < 0:
    d += (p - 1) * (q - 1)

m = hex(pow(c,d,p*q))[2:-1].decode('hex')
print (m)
```

运行...



```
hgame{w0w~yOU_kNoW+R5@!}
```

搞定!