20-Web-Week2-Writeup

Crypto

WhitegiveRSA

1. 看到题目中所给的信息

   描述

   N = 882564595536224140639625987659416029426239230804614613279163

   e = 65537

   c = 747831491353896780365654517748216624798517769637260742155527

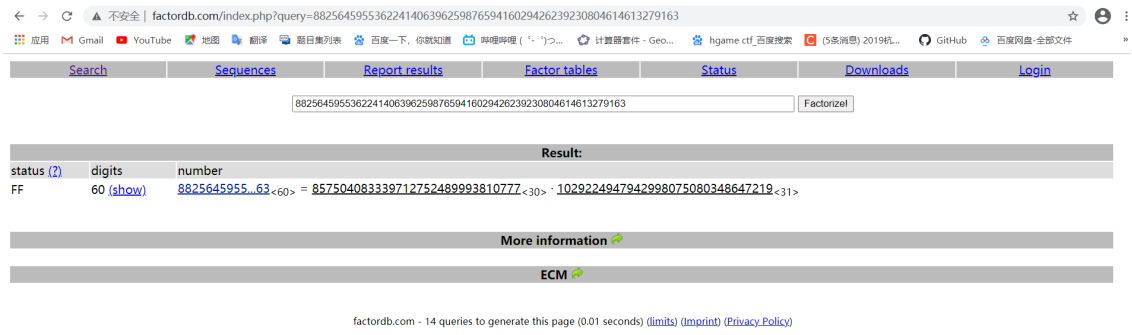
   这三个值分别是模值、公钥指数、密文，应该是利用RSA加密算法来求明文

2. 进入分解模值的网站

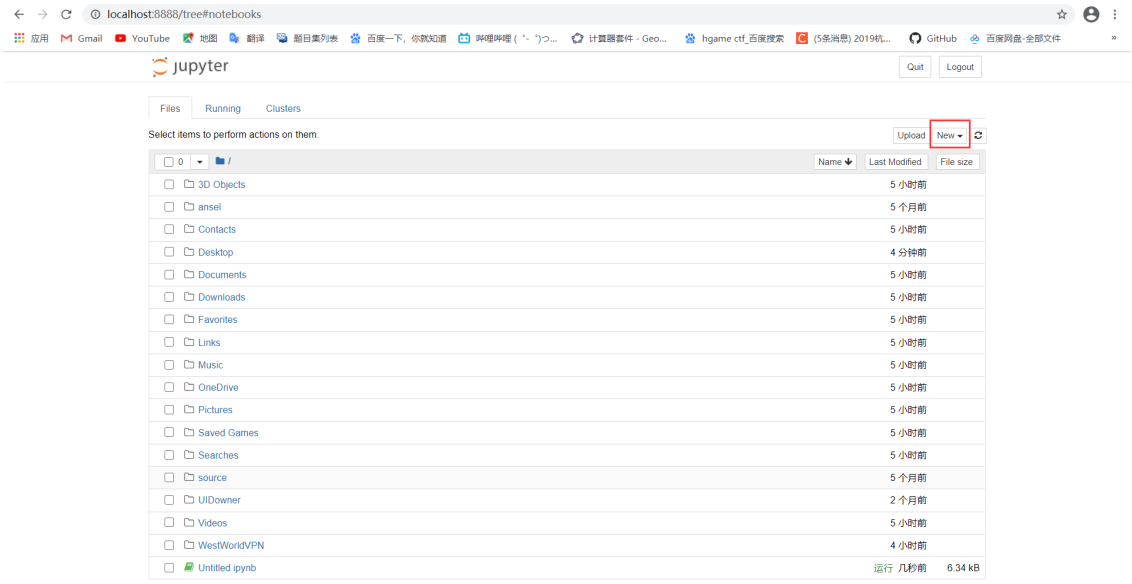
   将模值N = 882564595536224140639625987659416029426239230804614613279163输入，得到两个素数

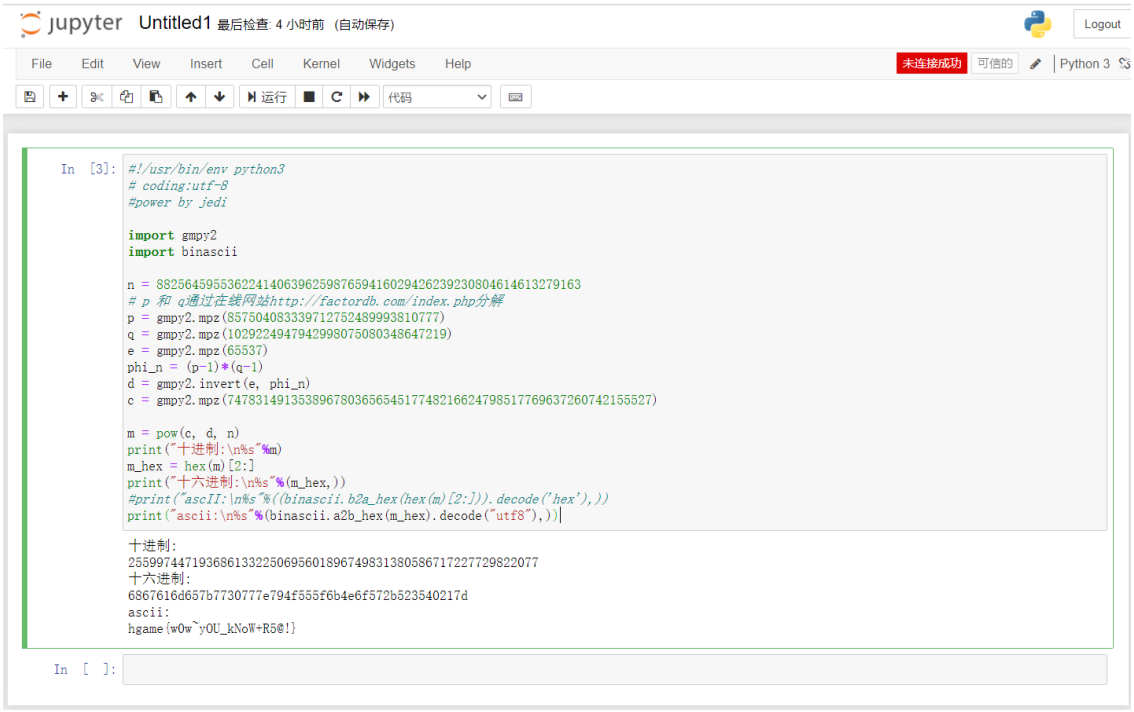
   p = 857504083339712752489993810777

   q = 10292249479429980750803486472l9



3. 用Anaconda自带的Jupyter里的python3运行解明文的代码，得到flag






```
<html>
#!/usr/bin/env python3
# coding:utf-8
#power by jedi

import gmpy2
import binascii

n = 882564595536224140639625987659416029426239230804614613279163
p = gmpy2.mpz(857504083339712752489993810777)
q = gmpy2.mpz(1029224947942998075080348647219)
e = gmpy2.mpz(65537)
phi_n = (p-1)*(q-1)
d = gmpy2.invert(e, phi_n)
c = gmpy2.mpz(747831491353896780365654517748216624798517769637260742155527)

m = pow(c, d, n)
print("十进制:\n%s"%m)
m_hex = hex(m)[2:]
print("十六进制:\n%s"%(m_hex,))
#print("ascII:\n%s"%((binascii.b2a_hex(hex(m)[2:])).decode('hex'),))
print("ascii:\n%s"%(binascii.a2b_hex(m_hex).decode("utf8"),))
</html>
```

得到flag

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