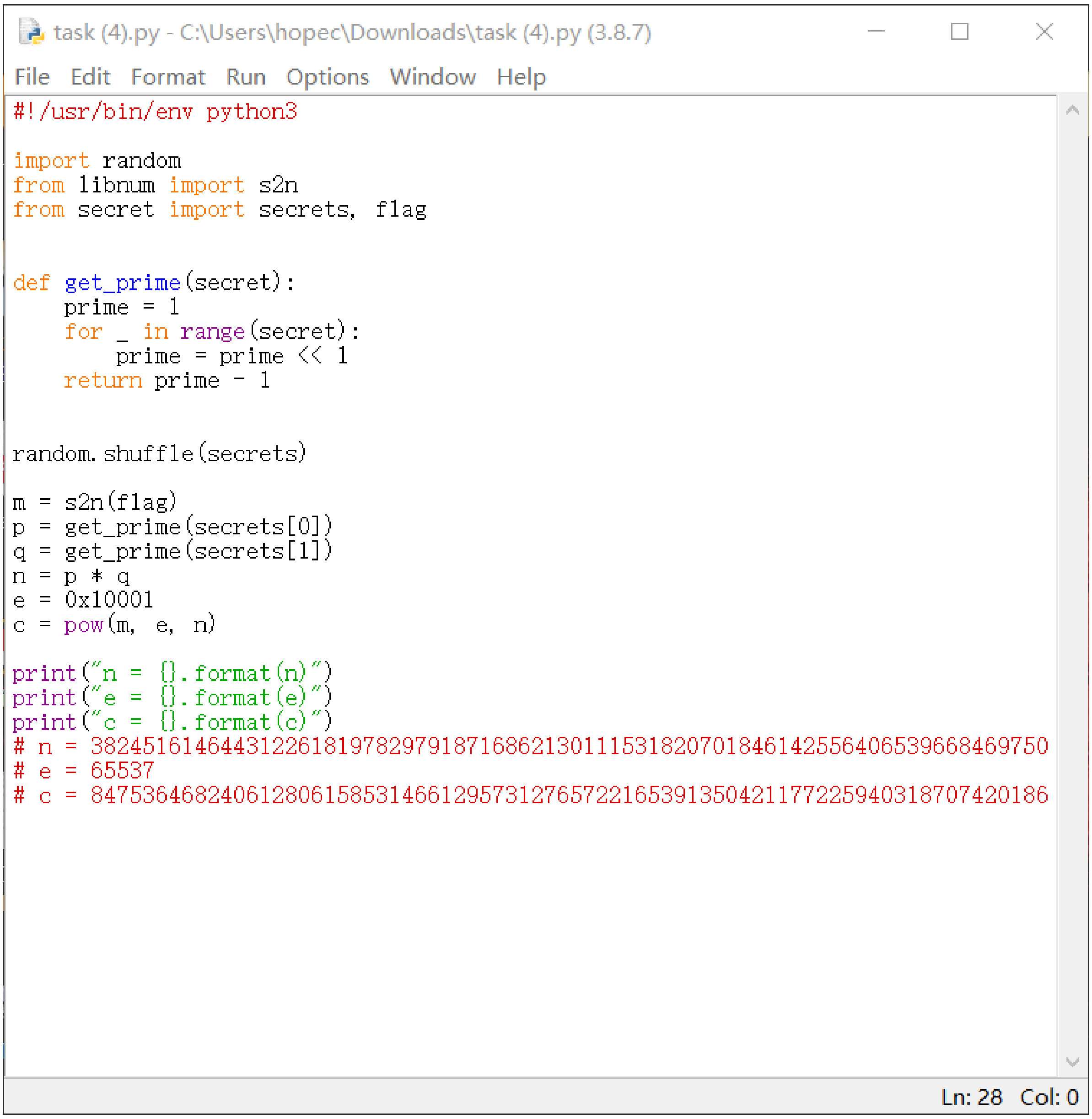
week 3 wp

crypto:

LikiPrime:

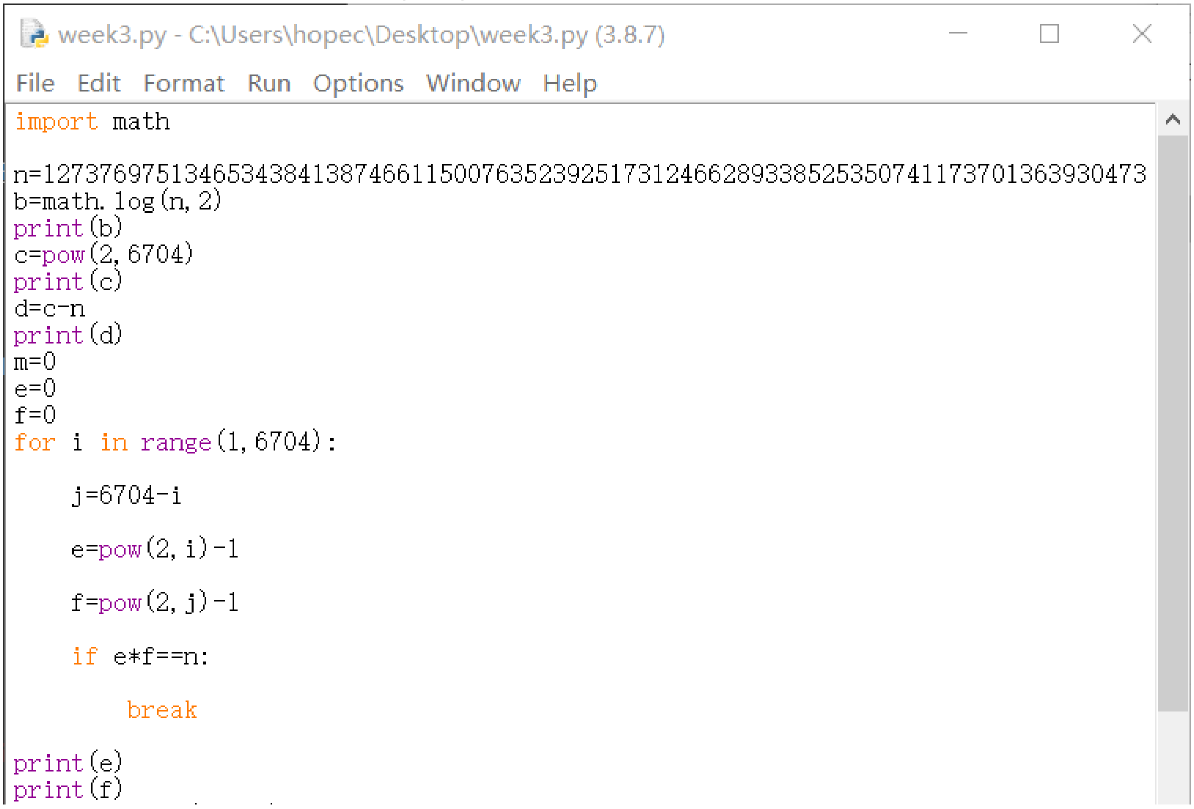
N 值巨大导致无法分解的 rsa



task (4).py - C:\Users\hopec\Downloads\task (4).py (3.8.7)
File Edit Format Run Options Window Help
Ln: 28 Col: 0

```
#!/usr/bin/env python3

import random
from libnum import s2n
from secret import secrets, flag


def get_prime(secret):
    prime = 1
    for _ in range(secret):
        prime = prime << 1
    return prime - 1


random.shuffle(secrets)

m = s2n(flag)
p = get_prime(secrets[0])
q = get_prime(secrets[1])
n = p * q
e = 0x10001
c = pow(m, e, n)

print("n = {}.format(n)")
print("e = {}.format(e)")
print("c = {}.format(c)")
# n = 38245161464431226181978297918716862130111531820701846142556406539668469750
# e = 65537
# c = 84753646824061280615853146612957312765722165391350421177225940318707420186
```

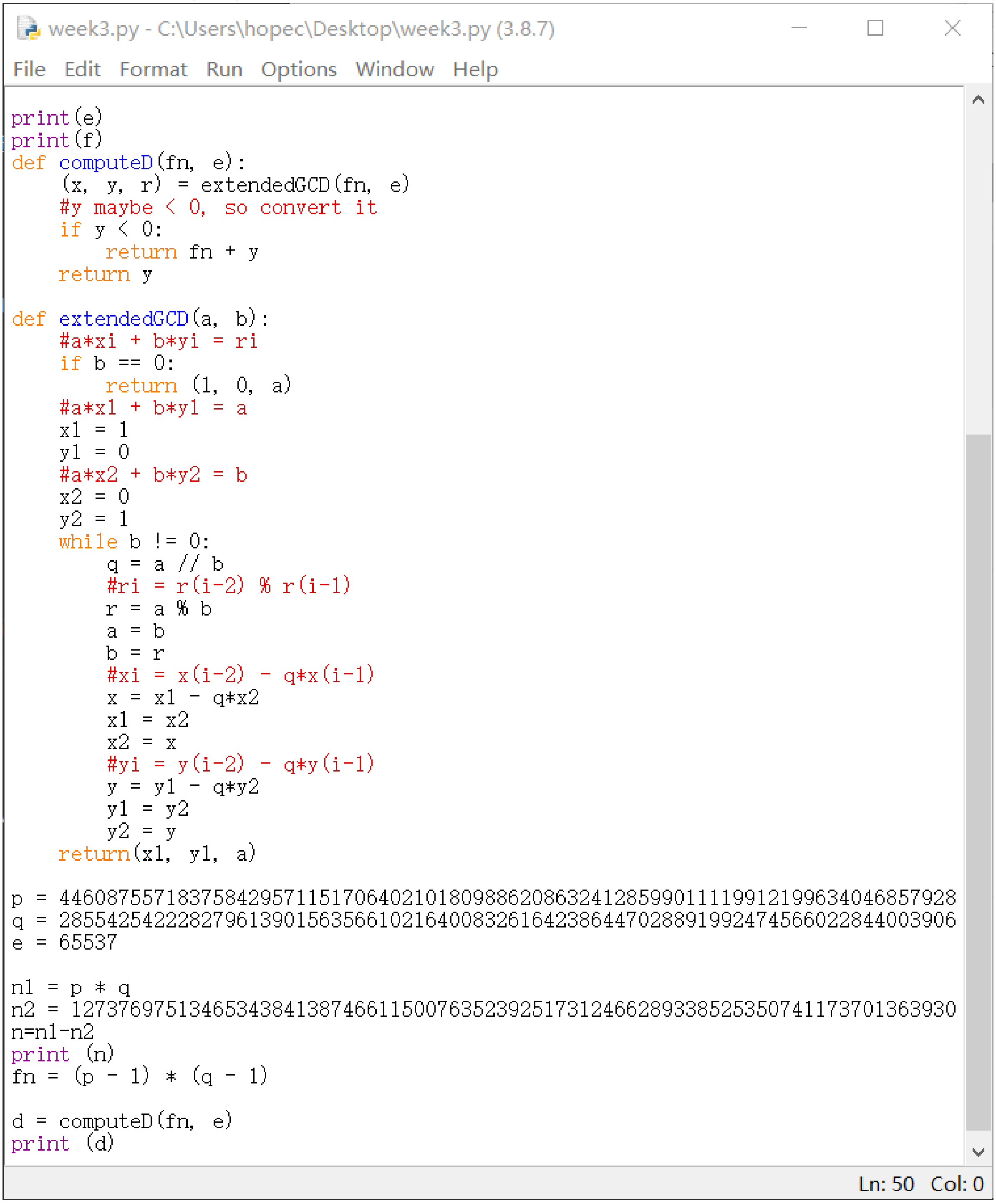
所幸我们知道 N 的产生方式：p 、q均是 2**n-1 形式的质数，由此编写脚本：



week3.py - C:\Users\hopec\Desktop\week3.py (3.8.7)
File Edit Format Run Options Window Help

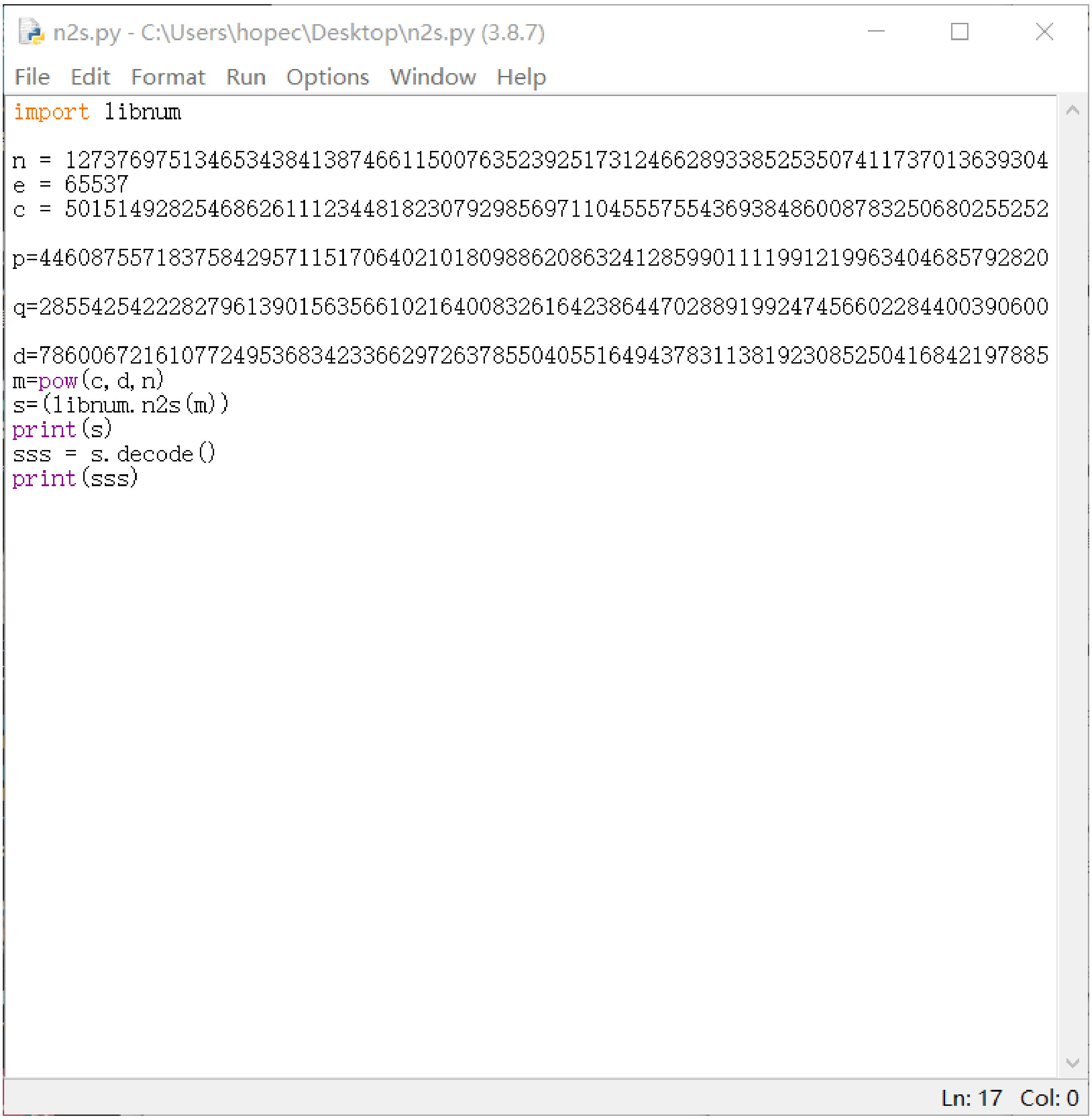
```
import math

n=127376975134653438413874661150076352392517312466289338525350741173701363930473
b=math.log(n,2)
print(b)
c=pow(2,6704)
print(c)
d=c-n
print(d)
m=0
e=0
f=0
for i in range(1,6704):

    j=6704-i

    e=pow(2,i)-1

    f=pow(2,j)-1

    if e*f==n:

        break

print(e)
print(f)
```

得到 e、f 即为 p、q，写求 d 的脚本：

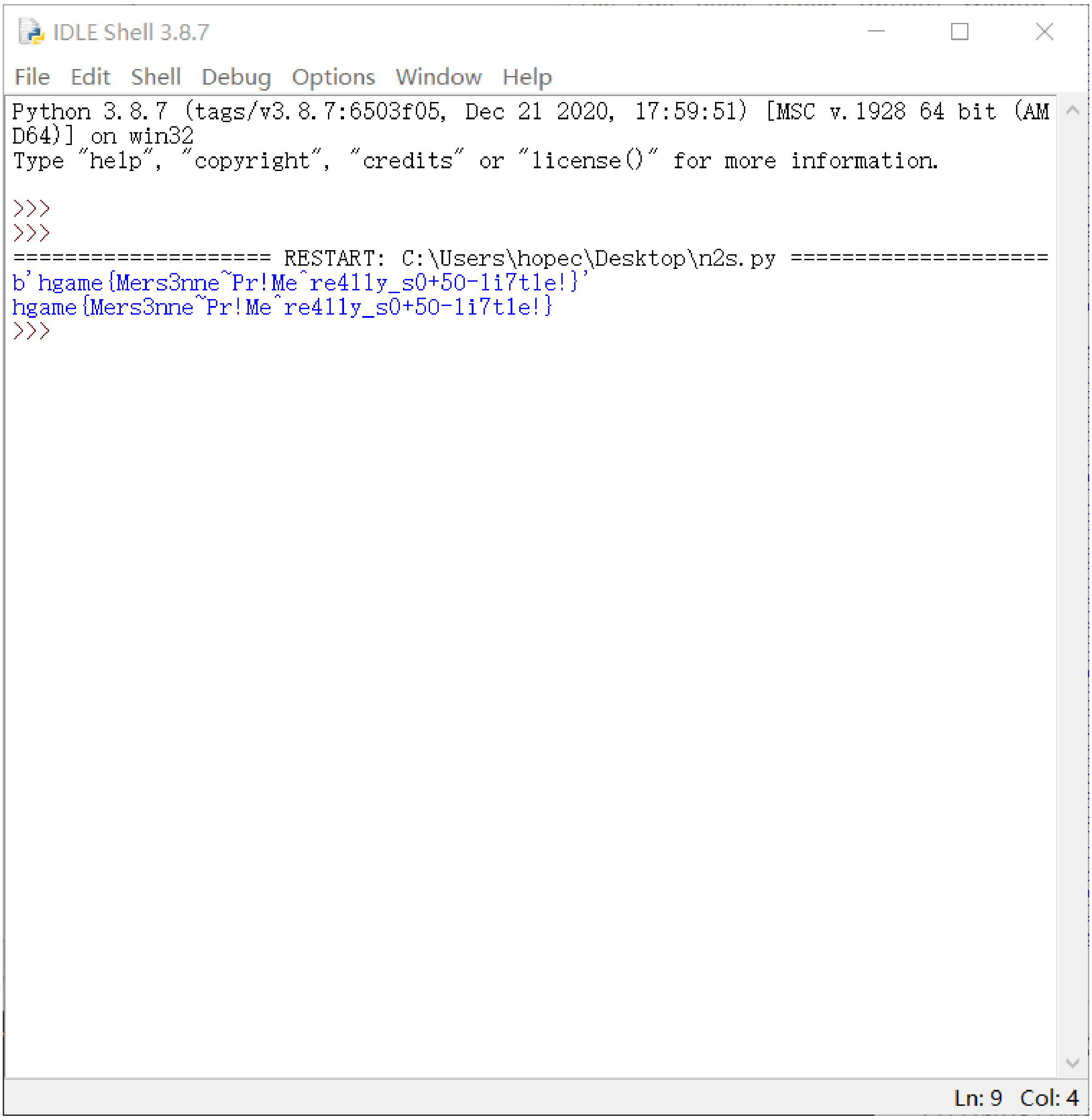

week3.py - C:\Users\hopec\Desktop\week3.py (3.8.7)
File Edit Format Run Options Window Help
Ln: 50 Col: 0

```
print(e)
print(f)
def computeD(fn, e):
    (x, y, r) = extendedGCD(fn, e)
    #y maybe < 0, so convert it
    if y < 0:
        return fn + y
    return y

def extendedGCD(a, b):
    #a*xi + b*yi = ri
    if b == 0:
        return (1, 0, a)
    #a*x1 + b*y1 = a
    x1 = 1
    y1 = 0
    #a*x2 + b*y2 = b
    x2 = 0
    y2 = 1
    while b != 0:
        q = a // b
        #ri = r(i-2) % r(i-1)
        r = a % b
        a = b
        b = r
        #xi = x(i-2) - q*x(i-1)
        x = x1 - q*x2
        x1 = x2
        x2 = x
        #yi = y(i-2) - q*y(i-1)
        y = y1 - q*y2
        y1 = y2
        y2 = y
    return(x1, y1, a)

p = 4460875571837584295711517064021018098862086324128599011119912199634046857928
q = 2855425422282796139015635661021640083261642386447028891992474566022844003906
e = 65537

n1 = p * q
n2 = 127376975134653438413874661150076352392517312466289338525350741173701363930
n=n1-n2
print (n)
fn = (p - 1) * (q - 1)

d = computeD(fn, e)
print (d)
```

再求 m 后用 n2s 转化为字符串：


n2s.py - C:\Users\hopec\Desktop\n2s.py (3.8.7)
File Edit Format Run Options Window Help
Ln: 17 Col: 0

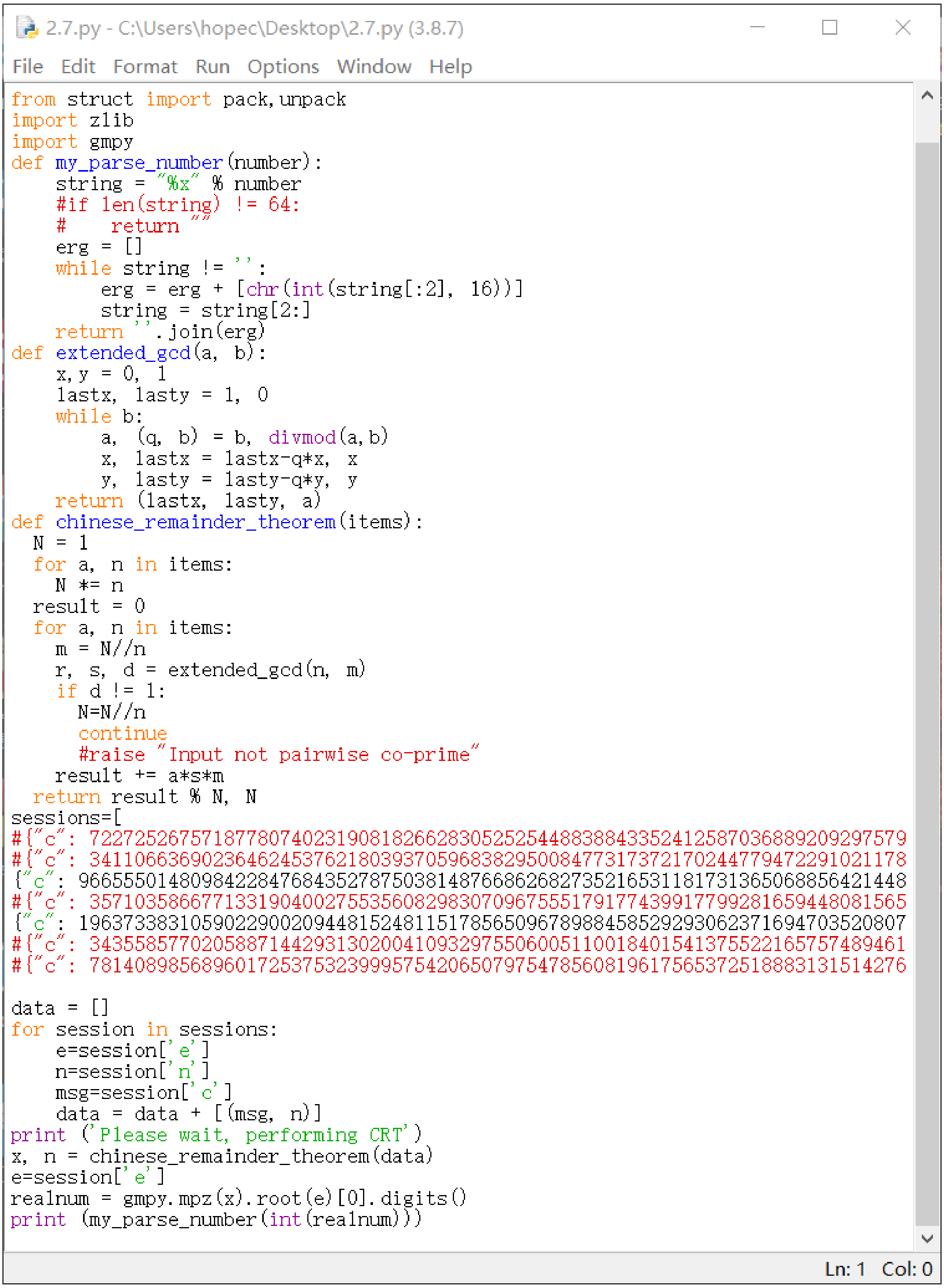
```
import libnum

n = 1273769751346534384138746611500763523925173124662893385253507411737013639304
e = 65537
c = 5015149282546862611123448182307929856971104555755436938486008783250680255252

p=446087557183758429571151706402101809886208632412859901111991219963404685792820

q=285542542228279613901563566102164008326164238644702889199247456602284400390600

d=786006721610772495368342336629726378550405516494378311381923085250416842197885
m=pow(c, d, n)
s=(libnum.n2s(m))
print(s)
sss = s.decode()
print(sss)
```



```
Python 3.8.7 (tags/v3.8.7:6503f05, Dec 21 2020, 17:59:51) [MSC v.1928 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.

>>>
>>>
==================== RESTART: C:\Users\hopec\Desktop\n2s.py ====================
b'hgame{Mers3nne~Pr!Me^re4lly_s0+50-1i7tle!}'
hgame{Mers3nne~Pr!Me^re4lly_s0+50-1i7tle!}
>>>
```

HappyNewYear!!:

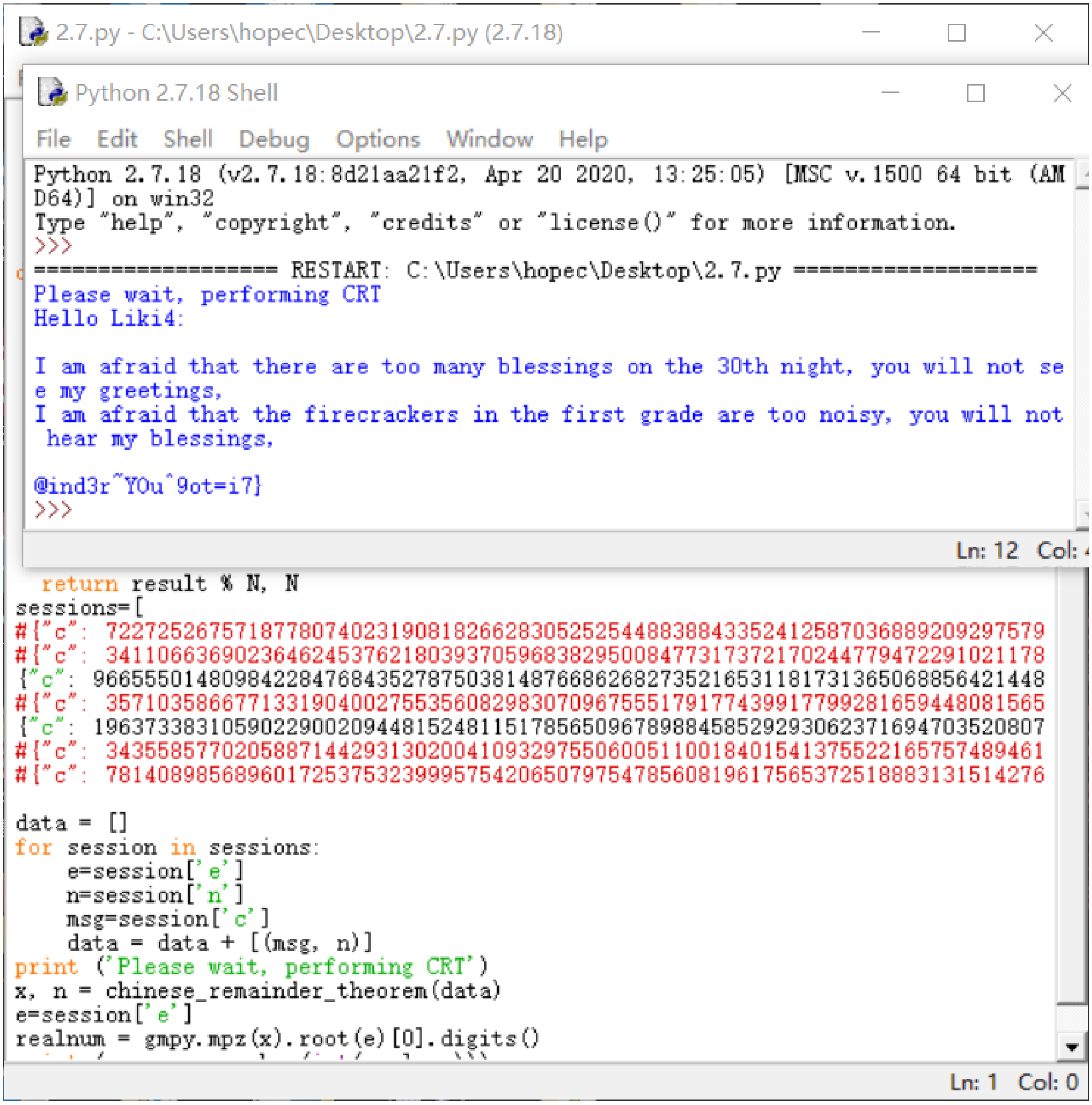
打开发现好多段 e 同为 3 的 rsa 加密语句，考虑低加密指数广播攻击：



2.7.py - C:\Users\hopec\Desktop\2.7.py (3.8.7)
File Edit Format Run Options Window Help
Ln: 1 Col: 0

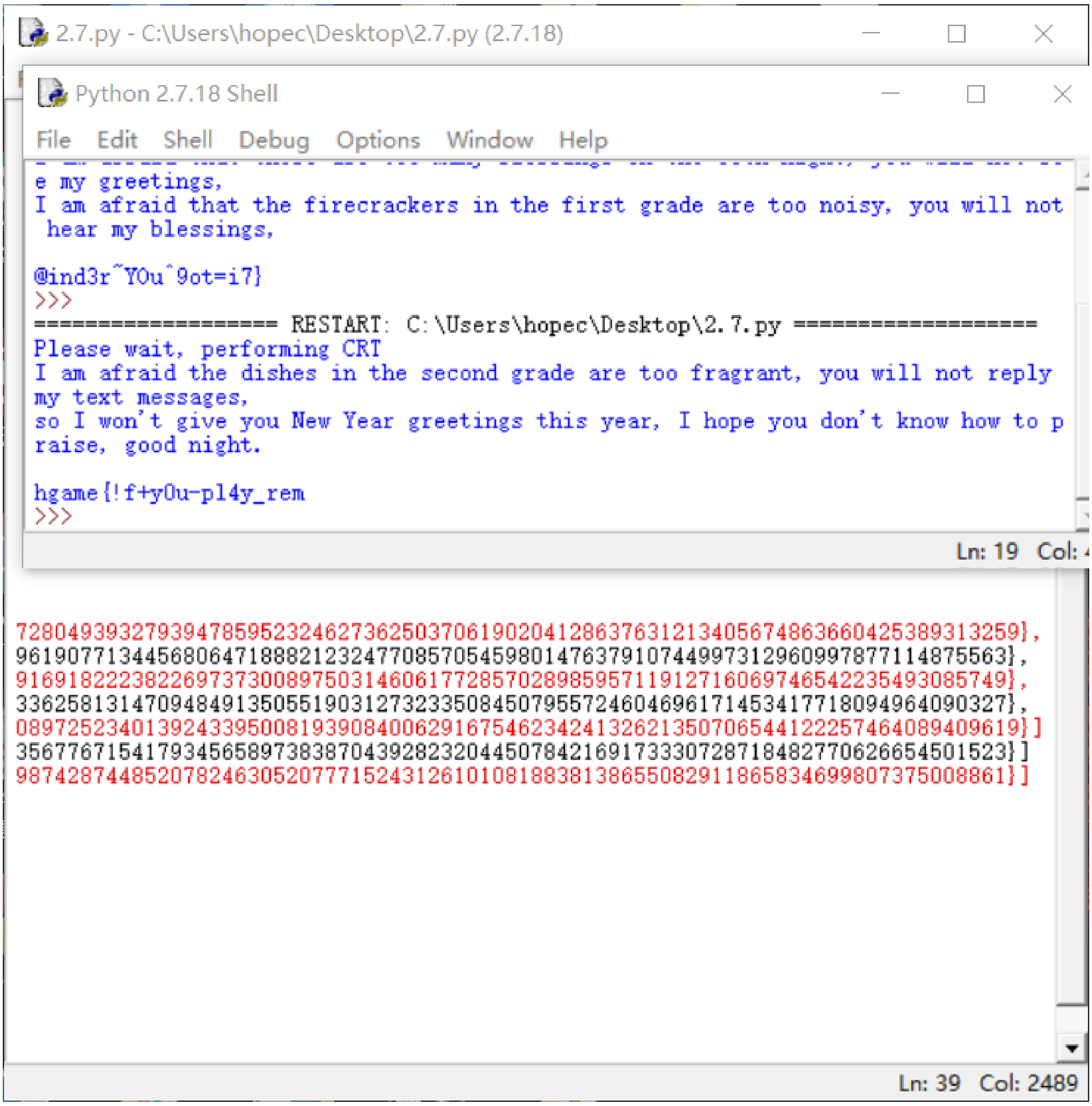
```python
from struct import pack,unpack
import zlib
import gmpy
def my_parse_number(number):
    string = "%x" % number
    #if len(string) != 64:
    #    return ""
    erg = []
    while string != '':
        erg = erg + [chr(int(string[:2], 16))]
        string = string[2:]
    return ''.join(erg)
def extended_gcd(a, b):
    x,y = 0, 1
    lastx, lasty = 1, 0
    while b:
        a, (q, b) = b, divmod(a,b)
        x, lastx = lastx-q*x, x
        y, lasty = lasty-q*y, y
    return (lastx, lasty, a)
def chinese_remainder_theorem(items):
  N = 1
  for a, n in items:
    N *= n
  result = 0
  for a, n in items:
    m = N//n
    r, s, d = extended_gcd(n, m)
    if d != 1:
      N=N//n
      continue
      #raise "Input not pairwise co-prime"
    result += a*s*m
  return result % N, N
sessions=[
#{"c": 7227252675718778074023190818266283052525448838843352412587036889209297579
#{"c": 3411066369023646245376218039370596838295008477317372170244779472291021178
{"c": 96655501480984228476843527875038148766862682735216531181731365068856421448
#{"c": 3571035866771331904002755356082983070967555179177439917799281659448081565
{"c": 19637338310590229002094481524811517856509678988458529293062371694703520807
#{"c": 3435585770205887144293130200410932975506005110018401541375522165757489461
#{"c": 7814089856896017253753239995754206507975478560819617565372518883131514276

data = []
for session in sessions:
    e=session['e']
    n=session['n']
    msg=session['c']
    data = data + [(msg, n)]
print ('Please wait, performing CRT')
x, n = chinese_remainder_theorem(data)
e=session['e']
realnum = gmpy.mpz(x).root(e)[0].digits()
print (my_parse_number(int(realnum)))
```

多次尝试得出两段flag：



```
Python 2.7.18 (v2.7.18:8d21aa21f2, Apr 20 2020, 13:25:05) [MSC v.1500 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
=================== RESTART: C:\Users\hopec\Desktop\2.7.py ===================
Please wait, performing CRT
Hello Liki4:

I am afraid that there are too many blessings on the 30th night, you will not se
e my greetings,
I am afraid that the firecrackers in the first grade are too noisy, you will not
 hear my blessings,

@ind3r~YOu^9ot=i7}
>>>
```

```
  return result % N, N
sessions=[
#{"c": 7227252675718778074023190818266283052525448838843352412587036889209297579
#{"c": 3411066369023646245376218039370596838295008477317372170244779472291021178
{"c": 96655501480984228476843527875038148766862682735216531181731365068856421448
#{"c": 3571035866771331904002755356082983070967555179177439917799281659448081565
{"c": 19637338310590229002094481524811517856509678988458529293062371694703520807
#{"c": 3435585770205887144293130200410932975506005110018401541375522165757489461
#{"c": 7814089856896017253753239995754206507975478560819617565372518883131514276

data = []
for session in sessions:
    e=session['e']
    n=session['n']
    msg=session['c']
    data = data + [(msg, n)]
print ('Please wait, performing CRT')
x, n = chinese_remainder_theorem(data)
e=session['e']
realnum = gmpy.mpz(x).root(e)[0].digits()
```



2.7.py - C:\Users\hopec\Desktop\2.7.py (2.7.18)
Python 2.7.18 Shell
File Edit Shell Debug Options Window Help
Ln: 19 Col:
Ln: 39 Col: 2489

```
e my greetings,
I am afraid that the firecrackers in the first grade are too noisy, you will not
 hear my blessings,

@ind3r~Y0u^9ot=i7}
>>>
=================== RESTART: C:\Users\hopec\Desktop\2.7.py ===================
Please wait, performing CRT
I am afraid the dishes in the second grade are too fragrant, you will not reply
my text messages,
so I won't give you New Year greetings this year, I hope you don't know how to p
raise, good night.

hgame{!f+y0u-pl4y_rem
>>>
```

```
728049393279394785952324627362503706190204128637631213405674863660425389313259},
96190771344568064718882123247708570545980147637910744997312960997877114875563},
91691822238226973730089750314606177285702898595711912716069746542235493085749},
33625813147094849135055190312732335084507955724604696171453417718094964090327},
08972523401392433950081939084006291675462342413262135070654412225746408940 9619}]
35677671541793456589738387043928232044507842169173330728718482770626654501523}]
98742874485207824630520777152431261010818838138655082911865834699807375008861}]
```