

week 2 wp

crypto:

whitegiveRSA:

查看题目给的条件

描述

$N = 882564595536224140639625987659416029426239230804614613279163$

$e = 65537$

$c = 747831491353896780365654517748216624798517769637260742155527$

题目地址 <https://www.baidu.com>

基准分数 150

当前分数 150

完成人数 167

先将 N 分解得出 p 、 q

factordb.com/index.php?query=882564595536224140639625987659416029426239230804614613279163

中、日、英、简、繁、藏、蒙、维、哈、柯、藏、蒙、维、哈、柯、藏、蒙、维、哈、柯


882564595536224140639625987659416029426239230804614613279163

因子化!

结果:

882564595536224140639625987659416029426239230804614613279163 = 85750408339712752489993810777 <30> | 1029224947942998075080348647218 <31>

RSAtool 计算 d (注意 e 必须使用 16 位即 10001)

 RSA TOOL 2 v1.7

Random data generation
 Seedfile loaded. 0%

Keysize (Bits)

Number Base

10

Public Exponent (E) [HEX]

1st Prime (P)

857504083339712752489993810777

2nd Prime (Q)

1029224947942998075080348647219

Modulus (N) 0 Bits

882564595536224140639625987659416029426239230804614613279163

Private Exponent (D)

121832886702415731577073962957377780195510499965398469843281

Factoring info (Prime factors): 0
PRIME FACTOR: 857504083339712752489993810777
PRIME FACTOR: 1029224947942998075080348647219

☐ Use MPQS method only ☐ No time checks Time left(max.): ~ 0h 0m 2s

Done. tE!

编写脚本

```
n2s.py - C:/Users/hopec/Desktop/n2s.py (3.8.7)
File Edit Format Run Options Window Help

import libnum

n = 882564595536224140639625987659416029426239230804614613279163
e = 65537
c = 747831491353896780365654517748216624798517769637260742155527
p=85750408339712752489993810777
q=1029224947942998075080348647219
d=121832886702415731577073962957377780195510499965398469843281
m=pow(c, d, n)
s=(libnum.n2s(m))
print(s)
sss = s.decode()
print(sss)
```

Ln: 8 Col: 62

run 得出 flag

```
===== RESTART: C:/Users/hopec/Desktop/n2s.py =====
b'hgame{w0w~y0U_kNoW+R5@!}'
hgame{w0w~y0U_kNoW+R5@!}
```

signin

脚本计算 m 并 n2d 输出

```
*task.py - C:/Users/hopec/Downloads/task.py (3.8.7)
File Edit Format Run Options Window Help

import libnum
s = "FLAG"
print(libnum.n2d(s))
n = 1179402567
#a = number.getPrime(1024)
#p = number.getPrime(1024)
#c = a ** p * m % p

a = 122904563952461622882768588918075210060104382601212298680805266125744694996254602515640108051748147681089759417074185367490933698108681355725681993537821407756282916098257015586399467313042691089516
p = 13810056036428633642160304675098165932751445251441917331010862166364161004516104258195299187265606281863834757979640039157714572778514680395296743143705351421389177536011800783337599430447944478929
c = 45203138092630691501933107480977549995504104222924142793515364857499646451396308223520466408961665863198659467334350963273145605258619512937751961484491676576984537093372775209451960952989519546662
print(a)
print(p)
print(c)
m=pow(a,p,p)
m=c*pow(m,p-2,p)%p
print(m)
s=(libnum.n2s(m))
print(s)
sss = s.decode()
print(sss)
```

Ln:

```
run 得出 flag
===== RESTART: C:/Users/hopec/Desktop/nzs.py
b'hgame{M0dul@r_m4th+1s^th3~ba5is-0f=cRypt0!!}'
hgame{M0dul@r_m4th+1s^th3~ba5is-0f=cRypt0!!}
>>>
```