WhitegiveRSA

描述

N = 882564595536224140639625987659416029426239230804614613279163
e = 65537
c = 747831491353896780365654517748216624798517769637260742155527

题目地址

[https://www.baidu.com]

解题过程

1. 在http://factordb.com/这个网站将N分解为p(857504083339712752489993810777)和q(1029224947942998075080348647219)
2.

```
import binascii
import sys
sys.setrecursionlimit(1000000)
def ByteToHex(bins):
    return ''.join(["%02X" % x for x in bins]).strip()
def n2s(num):
    t = hex(num)[2:-1]  # python
    if len(t) % 2 == 1:
        t = '0' + t
    #print(t)
    return(binascii.a2b_hex(t).decode('latin1'))
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)
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        print('modular inverse does not exist')
        return 'null'
    else:
        return x % m
c = 747831491353896780365654517748216624798517769637260742155527
p = 857504083339712752489993810777
q = 1029224947942998075080348647219
e = 65537
n = p * q
d = modinv(e, (p - 1) * (q - 1))
m = pow(c, d, n)
#print 'm \n', m
print (m)

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"),))
```

输出结果为

```
25599744719368613322506956018967498313805867172277298220 77
十进制:
25599744719368613322506956018967498313805867172277298220 77
十六进制:
6867616d657b7730777e794f555f6b4e6f572b523540217d
ascii:
hgame{wOw~yOU_kNoW+R5@!}
```

得到flag