Buuctf RSAROLL 题解

原创

偷一个月亮 于 2020-08-31 21:27:48 发布 749 收藏

分类专栏： CTF Python 文章标签： rsa

本文链接：https://blog.csdn.net/yiqiushi4748/article/details/108329838

题目内容如下：

题目介绍：

RSA roll！roll！roll！

Only number and a-z

（don’t use editor

which MS provide）

```
{920139713,19}

704796792
752211152
274704164
18414022
368270835
483295235
263072905
459788476
483295235
459788476
663551792
475206804
459788476
428313374
475206804
459788476
425392137
704796792
458265677
341524652
483295235
534149509
425392137
428313374
425392137
341524652
458265677
263072905
483295235
828509797
341524652
425392137
475206804
428313374
483295235
475206804
459788476
306220148
```

如上得知N和e

```
D:\tools\toolssss\crypto\yafu-1.34
λ yafu-x64.exe factor(920139713)

fac: factoring 920139713
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits
div: primes less than 10000
fmt: 1000000 iterations
Total factoring time = 0.0070 seconds

***factors found***

P5 = 49891
P5 = 18443

ans = 1


D:\tools\toolssss\crypto\yafu-1.34
λ
```

编写脚本得到：


```
# coding:utf-8
import gmpy2
N,p,q,e=920139713,18443,49891,19
phi = (p-1)*(q-1)
d=gmpy2.invert(e,phi)
result=[]

with open("c.txt","r") as f:
    for c in f.readlines():
        c=c.strip('\n')#去掉列表中每一个元素的换行符
        result.append(chr(pow(int(c),d,N)))

flag = ''
for i in result:
    flag += i
    print flag
```

得到flag{13212je2ue28fy71w8u87y31r78eu1e2}