Buuctf RSA 详细题解

原创

偷一个月亮 于 2020-08-31 21:06:57 发布 2891 收藏

分类专栏： CTF Python 文章标签： ctf rsa

本文链接：https://blog.csdn.net/yiqiushi4748/article/details/108329500

CTF 同时被 2 个专栏收录

43 篇文章 5 订阅

订阅专栏

Python

32 篇文章 0 订阅

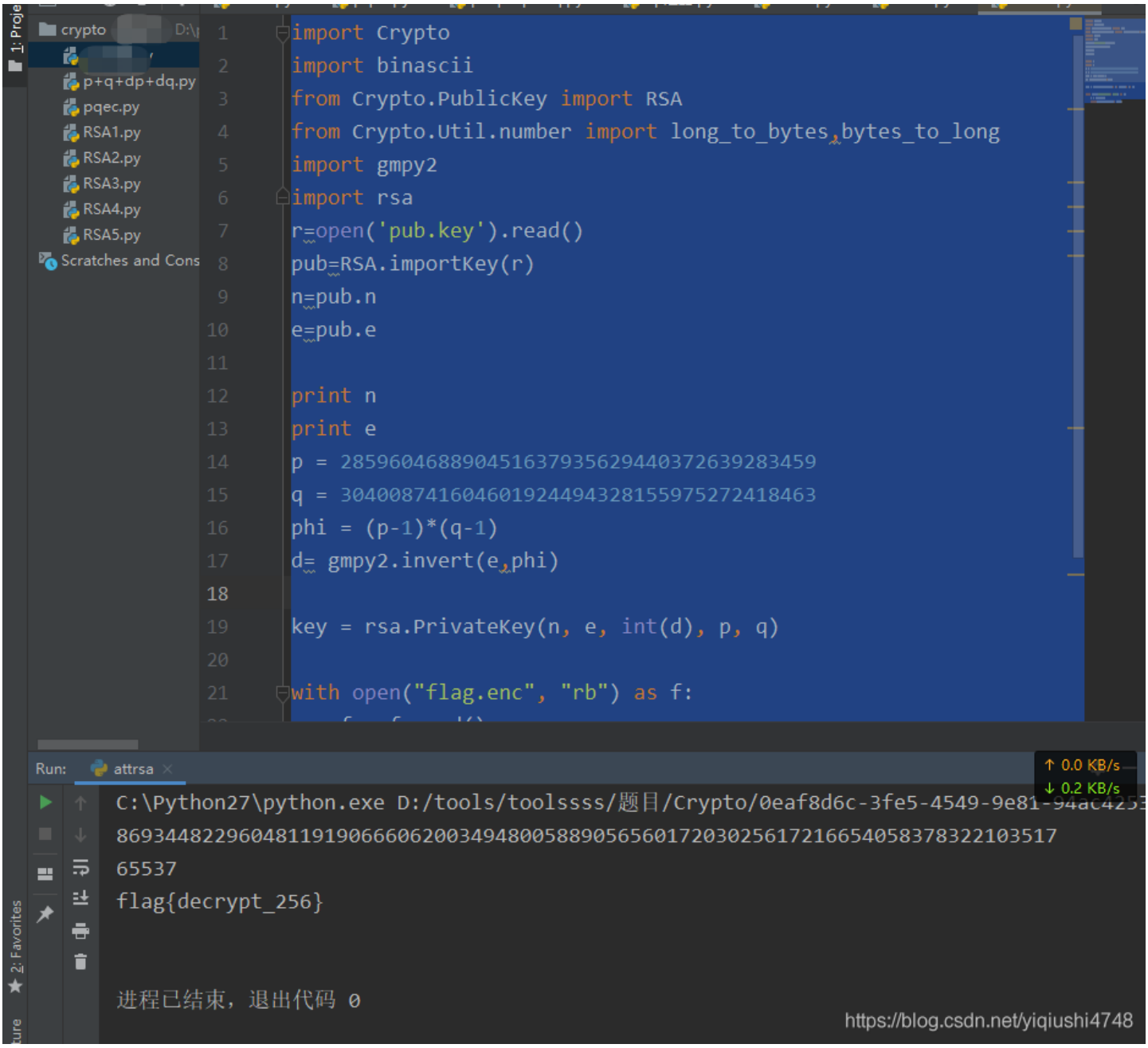
订阅专栏

```
import Crypto
import binascii
from Crypto.PublicKey import RSA
from Crypto.Util.number import long_to_bytes,bytes_to_long
import gmpy2
import rsa
r=open('pub.key').read()
pub=RSA.importKey(r)
n=pub.n
e=pub.e

print n
print e
p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
phi = (p-1)*(q-1)
d= gmpy2.invert(e,phi)

key = rsa.PrivateKey(n, e, int(d), p, q)

with open("flag.enc", "rb") as f:
    f = f.read()
    print(rsa.decrypt(f, key))
```


crypto
p+q+dp+dq.py
pqec.py
RSA1.py
RSA2.py
RSA3.py
RSA4.py
RSA5.py
Scratches and Cons
import Crypto
import binascii
from Crypto.PublicKey import RSA
from Crypto.Util.number import long_to_bytes,bytes_to_long
import gmpy2
import rsa
r=open('pub.key').read()
pub=RSA.importKey(r)
n=pub.n
e=pub.e
print n
print e
p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
phi = (p-1)*(q-1)
d= gmpy2.invert(e,phi)
key = rsa.PrivateKey(n, e, int(d), p, q)
with open("flag.enc", "rb") as f:
Run:
attrsa
↑ 0.0 KB/s
↓ 0.2 KB/s
C:\Python27\python.exe D:/tools/toolssss/题目/Crypto/0eaf8d6c-3fe5-4549-9e81-94ac4253
869344822960481191906660620034948005889056560172030256172166540583783221035 17
65537
flag{decrypt_256}
进程已结束，退出代码 0
https://blog.csdn.net/yiqiushi4748