

这是一道rsa题目
已知公钥和密文，求解明文
rsa的题型已经很明显，网上有一堆总结rsa的
rsa原理网上也是一堆，可以去搜搜

根据公钥求e, n



<http://tool.chacuo.net/cryptrsakeyparse>

这个网站，把公钥输入即可

-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFxkrkcYL2wch21CM2kQVFpY9+7+
/AvKr1rzQczdAgMBAAE=
-----END PUBLIC KEY-----

↑ 将你电脑文件直接拖入试试 ^-^

解析RSA密钥指数、模数

公私钥 对应指数及模数如下:  

公钥指数及模数信息:

key长度:	256
模数:	C0332C5C64AE47182F6C1C876D42336910545A58F7EEFEFC0BCAAF5AF341CCDD
指数:	65537 (0x10001)

根据n求p, q

<http://factordb.com/index.php?query=365795385832997256016937740927632319393223250249226128280707612750643974854166569495946441349>

这个网站可以求解p, q

Result:		
status (2)	digits	number
77 (show)	8693448229...17<77>	= 285960468890451637935629440372639283459<39> · 304008741604601924494328155975272418463<39>

求明文

现在知道了e,n,p,q,c
可以求解明文了
代码如下：

```
import gmpy2
import rsa

e = 65537
n = 86934482296048119190666062003494800588905656017203025617216654058378322103517
p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463

phin = (q-1)*(p-1)
d = gmpy2.invert(e, phin)

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

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

得到flag

```
File Edit Shell Debug Options Window Help
Python 3.6.8 (tags/v3.6.8:3c6b436a57, Dec 24 2018, 00:16:47) [MSC v.1916 64 bit
(AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\wsxk\Desktop\ctf\BUUCTF\rsa\output\test.py =====
b'flag{decrypt_256}\n'
>>>
```