buuctf——rsa

原创

re3sry 于 2021-05-29 22:42:53 发布 287 收藏 3

1.得到两个文件一个flag.enc一个pub.key

根据题目可知这是rsa加密，用记事本打开key文件。

关于rsa加密：CTF ——crypto ——RSA原理及各种题型总结_小锤队长的博客-CSDN博客_ctf rsa

```
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFx
krkcYL2wch21CM2kQVFpY9+7+
/AvKr1rzQczdAgMBAAE=
-----END PUBLIC KEY-----
```

这是公匙用工具解析得到n，e。（CTF在线工具-CTF工具|CTF编码|CTF密码学|CTF加解密|程序员工具|在线编解码 (ssleye.com)）

密钥类型	RSA
密钥强度	256
PN(e)	65537
PN(n)	86934482296048119190666062003494800588905656017203025617216654058378322103517
DER格式	303c300d06092a864886f70d0101010500032b003028022100c0332c5c64ae47182f6c1c876d42336910545a58f7eefefc0bcaaf5af341ccdd0203010001

再把n分解得到p，q。

86934482296048119190666062003494800588905656017203025617216654058378322103517 Factorize!

Result:

status (?)	digits	number
FF	77 (show)	8693448229...17<77> = 285960468890451637935629440372639283459<39> · 304008741604601924494328155975272418463<39>

p=285960468890451637935629440372639283459

q=304008741604601924494328155975272418463

2.写脚本解密

```
import gmpy2
import rsa

n=869344822960481191906660620034948005889056560172030256172166540583783221035 17
e=65537
p=285960468890451637935629440372639283459
q=304008741604601924494328155975272418463

d = int(gmpy2.invert(e,(p-1)*(q-1)))
k=rsa.PrivateKey(n,e,d,p,q)
with open("C:/Users/BY/Desktop/rsa/flag.enc","rb") as f:
    f=f.read()
    print(rsa.decrypt(f,k))
```


3.get flag

flag{decrypt_256}