BUUCTF RSA

转载

awxnutpgs545144602 于 2019-09-11 09:02:00 发布 4372 收藏 5
文章标签： 密码学
原文链接：http://www.cnblogs.com/harmonica11/p/11504291.html
版权
给的文件夹中有个pub.key，里面是公钥，

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

在线分解

公钥指数及模数信息:

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

得到n，e

用http://www.factordb.com

869344822960481191906660620034948005889056560172030256172166540583783221035 17 Factorize! (?)

Result:

number

8693448229...17$_{<77>}$ = 285960468890451637935629440372639283459$_{<39>}$ · 304008741604601924494328155975272418463$_{<39>}$

得到p和q，写脚本

```
import gmpy2
import rsa

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

phin = (p-1) * (q-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

转载于:https://www.cnblogs.com/harmonica11/p/11504291.html