buuctf Crypto RSA

原创

R-Mars 于 2021-03-17 19:00:13 发布 364 收藏 4

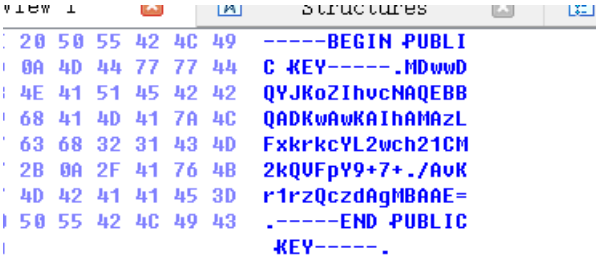
文章标签： 密码学

本文链接：https://blog.csdn.net/weixin_46244154/article/details/114943253

buuctf RSA

下载文件得到两个文件

pub.key即是公钥，用IDA打开




```
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAzLFxkrkcYL2wch21CM2kQVFpY9+7+/AvKr1rzQczdAgMBAAE=
```

提取出公钥中所含信息

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

模数转为十进制即是n

```
n=86934482296048119190666062003494800588905656017203025617216654058378322103517
```

分解n得到p q 因数分解网站.

```
285960468890451637935629440372639283459
304008741604601924494328155975272418463
```

运行脚本得到flag

```
import gmpy2
import rsa

p = 285960468890451637935629440372639283459
q = 304008741604601924494328155975272418463
e = 65537
n = 869344822960481191906660620034948005889056560172030256172166540583783221035l7

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

d = 81176168860169991027846870170527607562179635470395365333547868786951080991441

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

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

得到flag{decrypt_256}