

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_46244154/article/details/114943253](https://blog.csdn.net/weixin_46244154/article/details/114943253)

版权

## buuctf RSA

下载文件得到两个文件

pub.key即是公钥, 用IDA打开

```
view 1 STRUCTURES
00000200 50 55 42 4C 49  ----BEGIN PUBLIC
0000020A 0A 4D 44 77 77 44  C KEY-----MDwwD
00000214 E 41 51 45 42 42  QYJKoZIhvcNAQEBB
00000218 68 41 4D 41 7A 4C  QADKwAwKAIhAMAZL
00000222 63 68 32 31 43 4D  FxkrkcYL2wch21CM
00000226 2B 0A 2F 41 76 4B  2kQUFpY9+7+./AvK
00000230 4D 42 41 41 45 3D  r1rzQczdAgMBAAE=
00000234 50 55 42 4C 49 43  .-----END PUBLIC
                                KEY-----.
```

```
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAMAZLFxkrkcYL2wch21CM2kQUFpY9+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 = 86934482296048119190666062003494800588905656017203025617216654058378322103517

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}