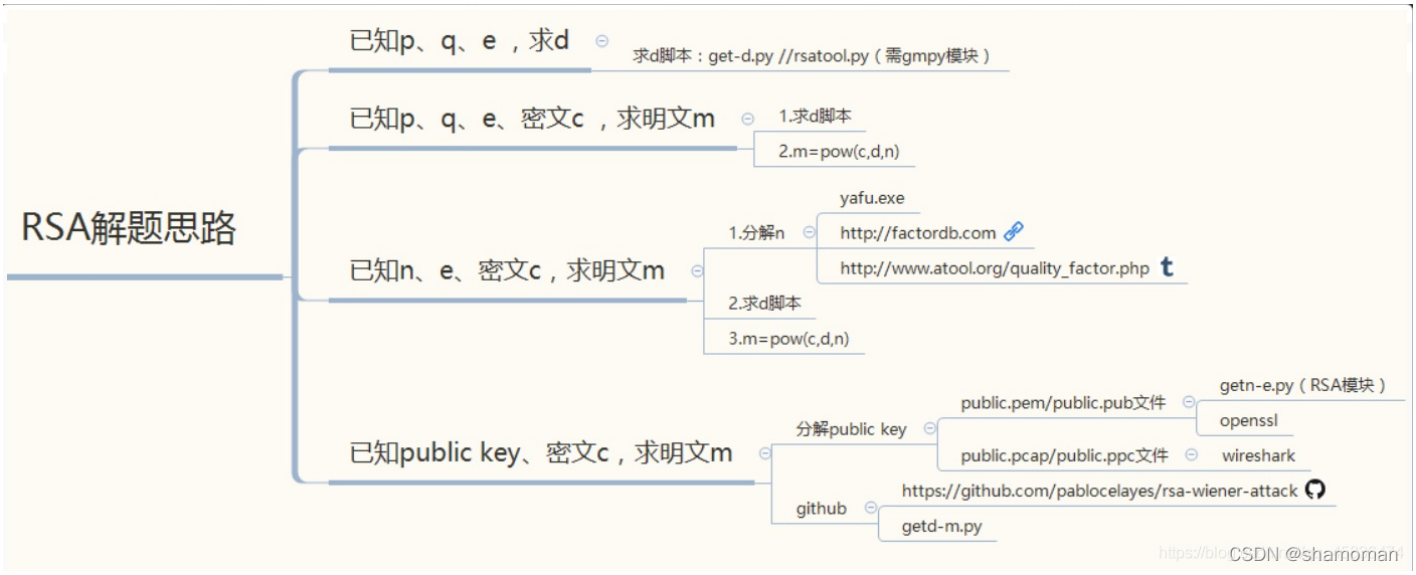
rsa入门ctf

原创

shamoman 于 2021-12-09 16:44:21 发布 26 收藏
分类专栏： 后台 文章标签： 安全 web安全 hdfs
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/jishamo/article/details/121830737
版权


后台 专栏收录该内容
9 篇文章 0 订阅
订阅专栏



已知p q e ctfshow crypto4

```
from Crypto.Util.number import *

p=447685307
q=2037
e=17

phi = (p-1)*(q-1)
d = inverse(e, phi)
print(d)
```

已知q p e c ctfshow crypto5 求m即可，根据公式m=pow（c,d,n）；

```
from Crypto.Util.number import *

def Decrypt(c,e,p,q):
    L=(p-1)*(q-1)
    d = inverse(e,L)
    n=p*q
    m=pow(c,d,n)
    flag=str(m)
    print(flag)



p=447685307
q=2037
e=17
c=704796792
Decrypt(c,e,p,q)
```

参考：

RSA密码的原理及做题总结-python黑洞网