buuctf Dangerous RSA

原创

m0_46607055 于 2021-10-22 09:34:37 发布 73 收藏
分类专栏： CTF密码学 文章标签： rsa

低加密指数攻击

rsa 的加密 为 c = m ^ e mod n

当e 很小，n很大 时，有两种情况

① m ^ e 有可能小于 n 。 此时， c = m ^ e 。 密文 m = c 开e次方

当 m ^ e > n 。 此时。 m ^ e = kn + c 。 k 是整数 。对 k 进行爆破，就能找到对应的m

脚本

```
#python3
## -*- coding: utf-8 -*-#
from gmpy2 import iroot
import libnum
e = 0x3
n = 0x52d483c27cd806550fbe0e37a61af2e7cf5e0efb723dfc81174c918a27627779b21fa3c851e9e94188eaee3d5cd6f752406a4
c = 0x10652cdfaa6b63f6d7bd1109da08181e500e5643f5b240a9024bfa84d5f2cac9310562978347bb232d63e7289283871efab83

k = 0
while 1:
    res = iroot(c+k*n,e)  #c+k*n 开3次方根 能开3次方即可
    #print(res)
    #res = (mpz(1304000448281971381981734052456302315991930504782460047879974048879771035557949448672899135
    if(res[1] == True):
        print(libnum.n2s(int(res[0]))) #转为字符串
        break
    k=k+1
#b'flag{25df8caf006ee5db94d48144c33b2c3b}'
```