2022年HGAME中CRYPTO的RSA Attack

原创

沐一 · 林 于 2022-04-04 16:20:48 发布 164 收藏

分类专栏： CTF 密码学 文章标签： ctf

本文链接：https://blog.csdn.net/xiao__1bai/article/details/122774938

2022年HGAME中CRYPTO的RSA Attack

RSA Attack[已完成]

描述

这就是传说中的暴力美学么

题目地址 https://cmfj-1308188104.cos.ap-shanghai.myqcloud.com/Week2/RSA%20Attack.zip

基准分数 150

当前分数 150

完成人数 230

CSDN @沐一 · 林

.

.

照例下载附件，一个task.py和output.txt：

```
rom Crypto.Util.number import getPrime
from libnum import s2n

from secret import flag

m = s2n(flag)
e = 65537
p = getPrime(80)
q = getPrime(80)
n = p * q
c = pow(m, e, n)
print("e =", e)
print("n =", n)
print("c =", c)
```

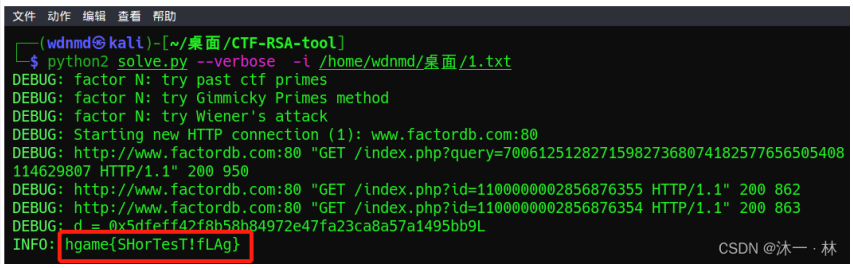
```
e = 65537
n = 700612512827159827368074182577656505408114629807
c = 122622425510870177715177368049049966519567512708
```

.

.

看着就简单，直接CTF-RSA-tool工具求解：

```
1 e = 65537
2 n = 700612512827159827368074182577656505408114629807
3 c = 122622425510870177715177368049049966519567512708
4
```



.

.

解毕！

敬礼！