




# 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](#)

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/xiao\\_\\_1bai/article/details/122774938](https://blog.csdn.net/xiao__1bai/article/details/122774938)

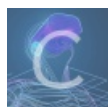
版权



[CTF 同时被 2 个专栏收录](#)

167 篇文章 6 订阅

订阅专栏



[密码学](#)

51 篇文章 1 订阅

订阅专栏

## 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:

```
from 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
```

```
文件 动作 编辑 查看 帮助
(wdmd@kali) - [~/桌面/CTF-RSA-tool]
└─$ python2 solve.py --verbose -i /home/wdmd/桌面/1.txt
DEBUG: factor N: try past ctf primes
DEBUG: factor N: try Gimmicky Primes method
DEBUG: factor N: try Wiener's attack
DEBUG: Starting new HTTP connection (1): www.factordb.com:80
DEBUG: http://www.factordb.com:80 "GET /index.php?query=700612512827159827368074182577656505408
114629807 HTTP/1.1" 200 950
DEBUG: http://www.factordb.com:80 "GET /index.php?id=110000002856876355 HTTP/1.1" 200 862
DEBUG: http://www.factordb.com:80 "GET /index.php?id=110000002856876354 HTTP/1.1" 200 863
DEBUG: d = 0x5dfeff42f8b58b84972e47fa23ca8a57a1495bb9L
INFO: hgame{SHorTesT!fLAg}
```

解毕！  
敬礼！