

2022年HGAME中CRYPTO的RSA Attack3

原创

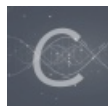
沐一·林 于 2022-04-04 16:20:29 发布 15 收藏

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/122779284

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 Attack3

RSA Attack 3[已完成]

描述

题目地址 <https://cmfj-1308188104.cos.ap-shanghai.myqcloud.com/Week3/RSA%20Attack%203.zip>

基准分数 250

当前分数 250

完成人数 51

CSDN @沐一·林

照例下载附件, 照例先 CTF-RSA-tool 工具先行:

```
└─$ python2 solve.py --verbose -i /home/wdnmd/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: d = 0xb5b9684e701c894fL
INFO: hgame{d0|YOU:kN0w!tHE*PRINcIpIe*bEhInd%WInNEr#aTTacK}
```

解毕!

敬礼!