

攻防世界 crypto 入门题之Normal_RSA

原创

沐一·林 于 2021-08-08 23:34:17 发布 64 收藏

分类专栏: [CTF 密码学](#) 文章标签: [unctf](#)

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/119523319

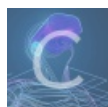
版权



[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

攻防世界 crypto 入门题之Normal_RSA

继续开启全栈梦想之逆向之旅~

这题是攻防世界crypto 入门题之Normal_RSA

Normal_RSA

👍 78 最佳Writeup由露思提供

WP

难度系数: ★★★★★ 5.0

题目来源: PCTF

题目描述: 你和小鱼走啊走走啊走, 走到下一个题目一看你又一愣, 怎么还是一个数学题啊 小鱼又一笑, hhhh数学在密码学里面很重要在知道吃亏了吧! 你哼一声不服气, 我知道数学 很重要了! 但是工具也很重要, 你看我拿工具把他解出来! 你打开电脑折腾了一会还真案 做了出来, 小鱼有些吃惊, 向你投过来一个赞叹的目光

题目场景: 暂无

题目附件: 附件1

https://blog.csdn.net/xiao__1bai

简单RSA的题目看我的另一篇博客, 介绍了工具的使用:

https://blog.csdn.net/xiao__1bai/article/details/119465149?spm=1001.2014.3001.5502

所以这题可以直接脚本秒杀了：

```
(wdnmd@kali)-[~/桌面/CTF-RSA-tool]
└─$ python2 solve.py -v -k /home/wdnmd/桌面/pubkey.pem --decrypt /home/wdnmd/桌面/flag.enc
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=879243482641324068752761405144999371
45050893665602592992418171647042491658461 HTTP/1.1" 200 998
DEBUG: http://www.factordb.com:80 "GET /index.php?id=1100000000836631227 HTTP/1.1" 200 874
DEBUG: http://www.factordb.com:80 "GET /index.php?id=1100000000836631226 HTTP/1.1" 200 873
DEBUG: d = @x1806799bd44ce649122b78b43060c786f8b77fb1593e0842da063ba0d8728bf1L
INFO: 000&[0PCTF{256b_i5_m3dium}]
```

https://blog.csdn.net/xiao__1bai

解毕：敬礼！