

# 攻防世界crypto高手题之RSA256

原创

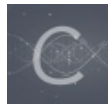
沐一·林 于 2021-09-17 20:39:59 发布 47 收藏 1

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/120356360](https://blog.csdn.net/xiao__1bai/article/details/120356360)

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高手题之RSA256

继续开启全栈梦想之逆向之旅~

这题是攻防世界crypto高手题的RSA256

### RSA256

最佳Writeup由 [系统战队](#) · admin 提供

WP 建议

难度系数: ★★★★ 3.0

题目来源: 暂无

**题目描述:** 被潘汉年按时来到上海百老汇大厦(今上海大厦), 叩开了袁殊临时下榻处的房门。袁殊说明自己当前身份和处境后, 突然话锋一转, 问潘汉年: “你到我这里来, 恐怕已经被日本特务注意到了。我应该怎么向他们解释呢?” 潘汉年说: “你就将计就计在敌伪内部站住脚, 取得合法地位。同时搜集敌伪情报向我提供。” “要是岩井要求我将你介绍给他怎么办?” “那我就用胡越明的化名同岩井见面, 就说我愿意和你在香港合作搞情报。” 时隔不久, 潘汉年接到袁殊通知, 通知内容为: RSA256.tar.gz, 要他在上海虹口区一家日本人开的餐馆里, 和岩井会见。请以暗号形式告知我方人员前往保护潘汉年的安全。(答案为flag{XXX}形式)

题目场景: 暂无

题目附件: [附件1](#)

CSDN @沐一一沐, 一沐沐一

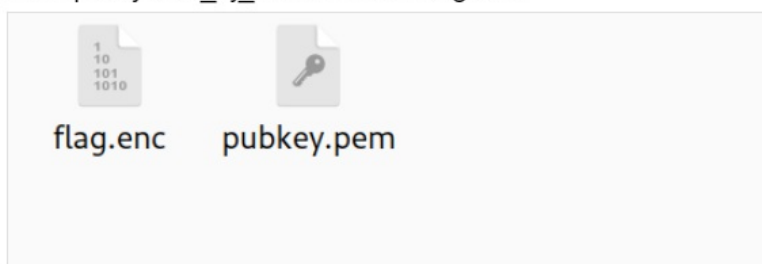
下载压缩包, 解压, 是两个附件, 一个没有后缀, 一个.txt文件, 打开查看内容, 感觉是RSA的密文密钥文件:

```
RSA256/ 0000755 0000000 0000000 000000000000 13446064553 ^
????绘?癯W Z闊?C?嗽偶野?
BLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhAKm9THp3YzcKBC/mvsfdyEFgLblCx6Ni
0bXTcqTQiRLZAgMBAAE=
-----END PUBLIC KEY-----
```

翻一下以前的笔记，这是对 `CTF-RSA-tool` 使用的示例，感觉题目类型就是这种密钥和密文的文件。

# factordb.com

```
python2 solve.py --verbose -k examples/jarvis_oj_mediumRSA/pubkey.pem --decrypt
examples/jarvis_oj_mediumRSA/flag.enc
```



```
L -----BEGIN PUBLIC KEY-----
? MDowDQYJKoZIhvcNAQEBBQADKQAwJgIhAMJjauXD20Q/+5erCQKPGqxsC/bNPXD r
} yigb/+l/vjDdAgEC
! -----END PUBLIC KEY-----
;
```

默认 (UTF-8, 部分)  其他:

```
n> · ß#îáÓ ¼ x e½= ImÚd A y
```

CSDN @沐一一沐, 一沐沐一

验证猜想，直接脚本跑一下：

```
$ python2 solve.py --verbose -k /home/wdnmd/桌面/gy.key --decrypt /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: Starting new HTTP connection (1): www.factordb.com:80
DEBUG: http://www.factordb.com:80 "GET /index.php?query=76775333402239611394270507078404178
11156978085146970312315886671546666259161 HTTP/1.1" 200 993
DEBUG: http://www.factordb.com:80 "GET /index.php?id=1100000001249442187 HTTP/1.1" 200 873
```

```
DEBUG: http://www.factordb.com:80 "GET /index.php?id=1100000001249442188 HTTP/1.1" 200 875
DEBUG: d = 0x6e1e3e007175af5e532b14628edda62d1d0f7561a926a10f29853bde0a5ed611L
INFO: c0L0u05flag{_2o!9_CTF_ECUN_}
```

CSDN @沐一一沐，一沐沐一

得到flag。

总结：

无

解毕！敬礼！