

攻防世界Normal_RSA解析,长知识了

原创

该用户正摸鱼 于 2022-01-14 15:37:42 发布 966 收藏

分类专栏: [攻防世界crypto题目](#) 文章标签: [python rsa](#)

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/weixin_58111246/article/details/122492280

版权



[攻防世界crypto题目](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

下载打开此文件夹可以看到:

> 此电脑 > Data (D:) > 微软浏览器下载保存 > L

名称	修改日期	类型	大小
flag.enc	2016-04-29 17:56	ENC 文件	1 KB
pubkey.pem	2016-04-29 17:19	PEM 文件	1 KB

CSDN @该用户正摸鱼

flag.enc里面的即是密文

pubkey.pem里面的是n (模数) 和e (公钥)

思路: ***rsatool工具我py运行报错,就很无语,很离谱,只能用kali救命了

1. 网站[SSL在线工具-公钥解析 \(hiencode.com\)](#)解析pubkey.pem文件, 得到n和e (用openssl这些好像解析出的数据是十六进制的, 转为十进制即可)
2. 网站[factordb.com](#)进行质因数分解n, 得到p (质因数) 和q (质因数)
3. 由p、q计算出phi(n): $\phi = (p - 1) * (q - 1)$ (一般py写脚本)
4. 由e、phi(n)计算出d (私钥)
5. 并保存为xxx.pem格式
6. 命令解密:xxx xxx xxx out flag.txt

下面是解题过程。。。

过程:

公钥解析

获取公钥的加密类型、加密长度、其他参数，以及DER格式输出。

```
-----BEGIN PUBLIC KEY-----
MDw=DQYJKoZIhvcNAQEBBQADKwAwKAIhAMJjauND200/+5erCQRPGqxsC/bNFXDr
yigb+/L/vJdAgMBAAE=
-----END PUBLIC KEY-----
```

[解析](#)

详细信息

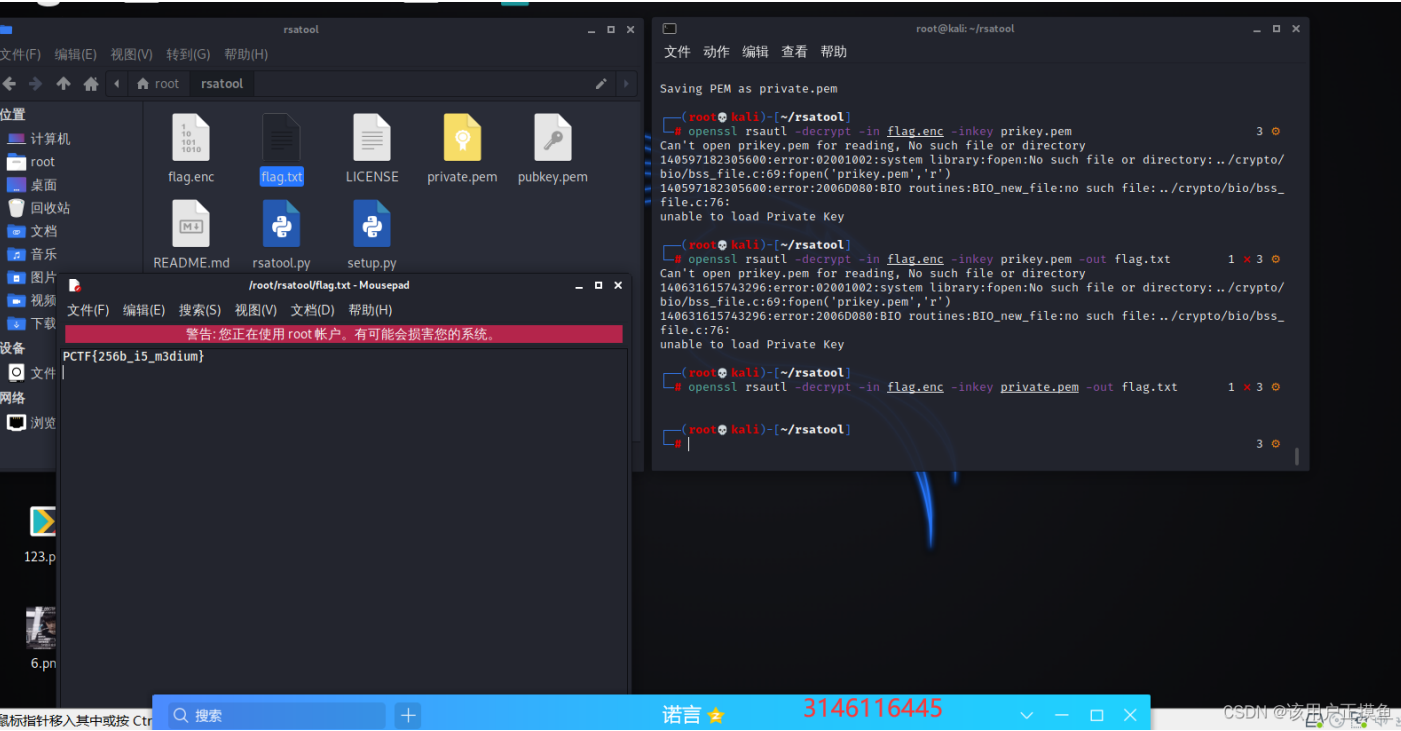
密钥类型	RSA
密钥强度	256
PN(e)	65537
PN(n)	87924348264132406875276140514499937145050893665602592992418171647042491658461

Result:

> = 275127860351348928173285174381581152299<39> · 319576316814478949870590164193048041239<39>

More information [CSDN @该用户正摸鱼](#)

p,q,e,n都整出来了了，pycharm打开，编写脚本，前提要gmpy2,有的人要pycryptodome，这个用来算出n, 因为她们可能弄出来的不是十进制，还得去转，我直接用脚本，导入gmpy2,列出数据，输出数据phi.d



用到rsatool,github上找这个工具，然后在kali上命令安装，有些感觉用不到（卡了一会看其他师傅博客里面有的弄了这些）

```
python3 -m pip install gmpy, wget https://bootstrap.pypa.io/get-pip.py, wget
https://bootstrap.pypa.io/pip/2.7/get-pip.py,
sudo python get-pip.py,
sudo pip install setuptools, sudo apt-get install libgmp-dev,
```

pip install gmpy2,

wget https://www.mpfr.org/mpfr-current/mpfr-4.1.0.tar.bz2,

wget ftp://ftp.gnu.org/gnu/mpc/mpc-1.1.0.tar.gz,

tar -zxvf mpc-1.1.0.tar.gz && cd mpc-1.1.0

到这快成功了。。。图上几个命令安装一下，终止了就重试，就像你进GitHub可能也失败，翻墙就没问题了

```
11
10 x64 (root@kali)-[~]
└─# cd rsatool
cd: 没有那个文件或目录: rsatool

(root@kali)-[~]
└─# ~/mpc-1.1.0# make && make check && make install
zsh: 没有那个文件或目录: /root/mpc-1.1.0#

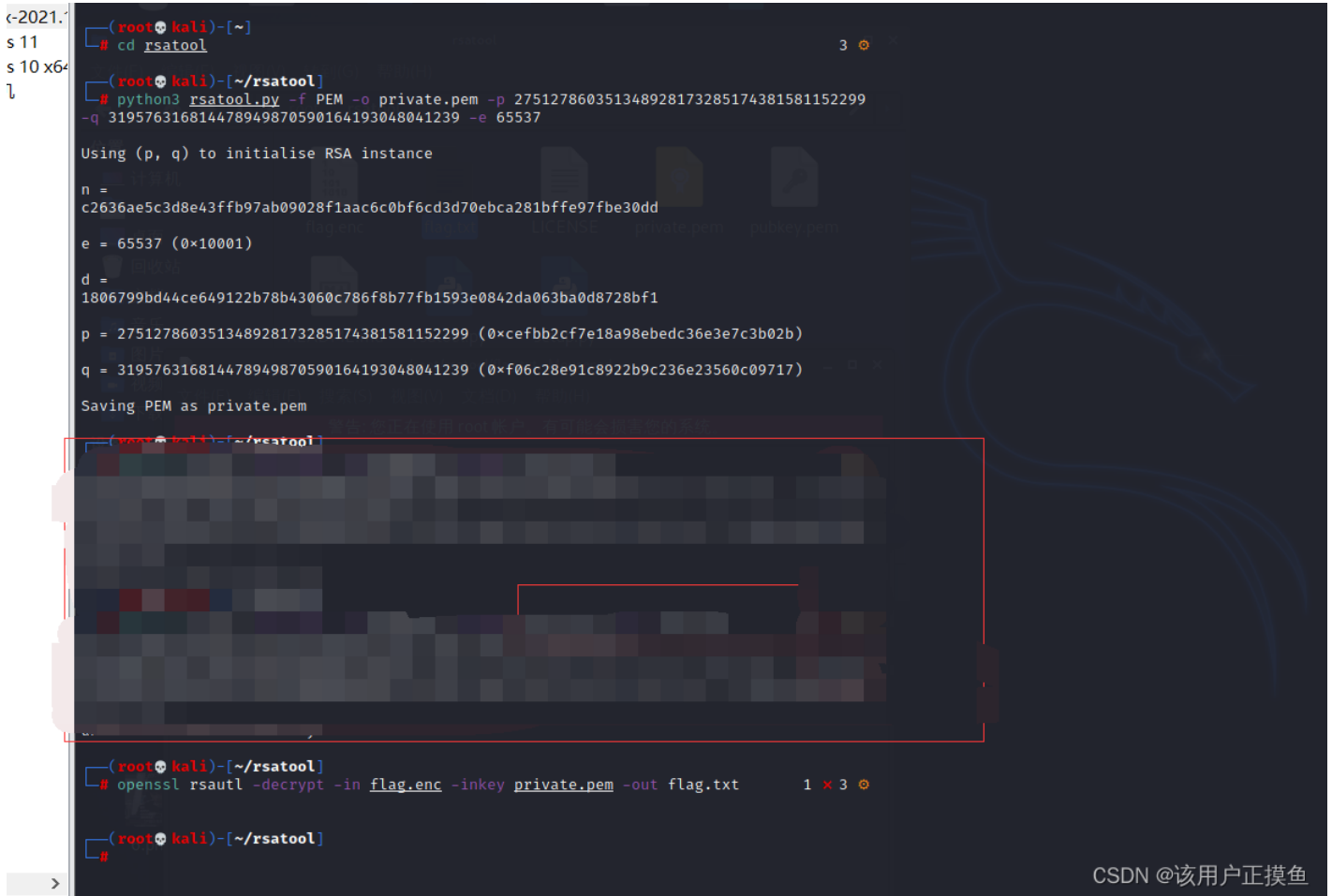
(root@kali)-[~]
└─# pip3 install gmpy2
Requirement already satisfied: gmpy2 in /usr/local/lib/python3.9/dist-packages (2.1.2)

(root@kali)-[~]
└─# openssl rsa -pubin -in pubkey.pem -text -modulus
Can't open pubkey.pem for reading, No such file or directory
140321878422848:error:02001002:system library:fopen:No such file or directory:../crypto/
bio/bss_file.c:69:fopen('pubkey.pem','r')
140321878422848:error:2006D080:BIIO routines:BIIO_new_file:no such file:../crypto/bio/bss_
file.c:76:
unable to load Public Key

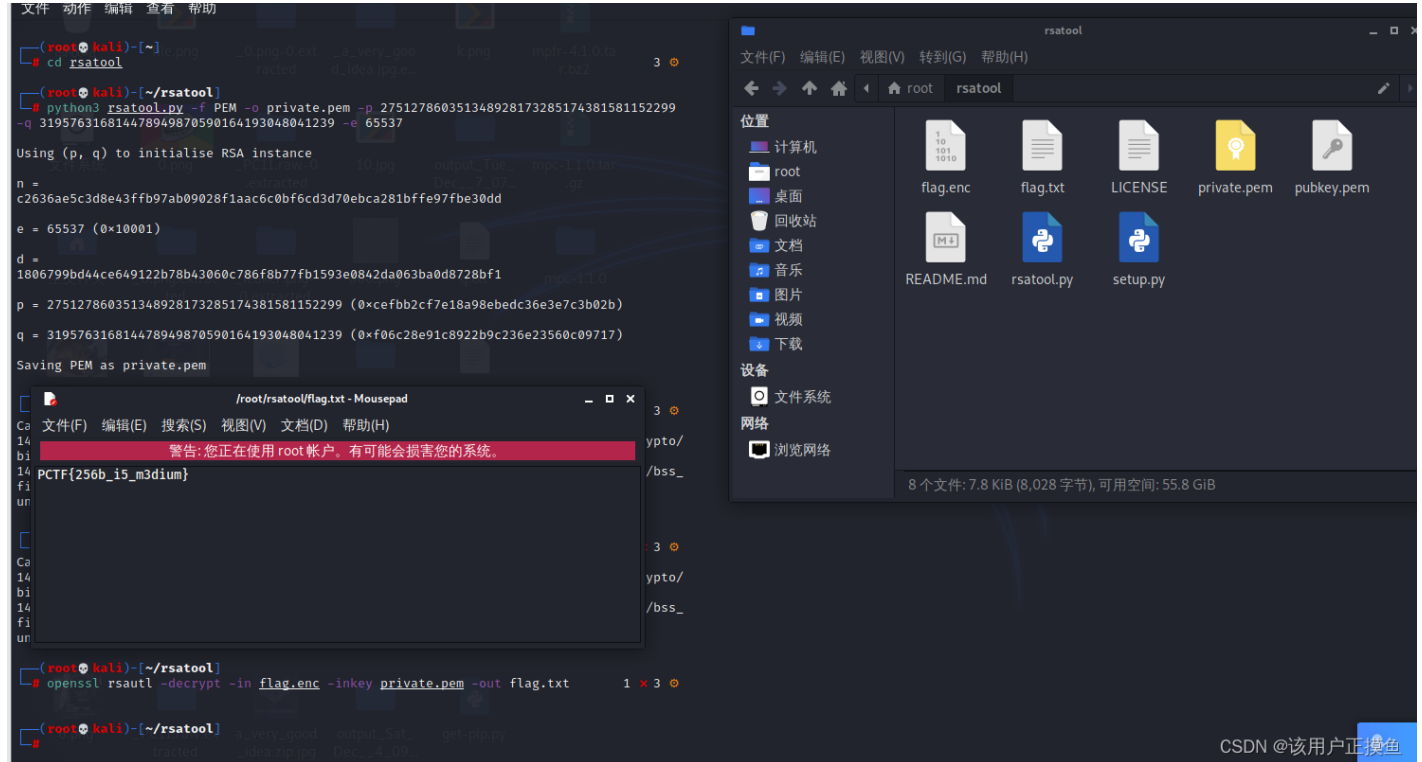
(root@kali)-[~]
└─# git clone https://github.com/ius/rsatool.git
正克隆到 'rsatool' ...
fatal: 无法访问 'https://github.com/ius/rsatool.git/': GnuTLS recv error (-110): TLS 链
接非正常地终止了。

(root@kali)-[~]
└─# git clone https://github.com/ius/rsatool.git
正克隆到 'rsatool' ...
remote: Enumerating objects: 62, done.
remote: Counting objects: 100% (13/13), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 62 (delta 6), reused 9 (delta 5), pack-reused 49
接收对象中: 100% (62/62), 13.34 KiB | 257.00 KiB/s, 完成.
处理 delta 中: 100% (27/27), 完成.
```

然后cd进rsatool目录，弄错了文件夹名字找半天才发现出问题哪里c,妈了个巴子



如图，找到刚刚安装好的rsatool文件夹目录（很好找，前提安装好了），把flag.enc,publickey.pem放进去~



rsatool目录下python3 rsatool.py -f PEM -o private.pem -p 275127860351348928173285174381581152299 -q 319576316814478949870590164193048041239 -e 65537

```
python3 rsatool.py -f PEM -o private.pem -p 275127860351348928173285174381581152299
-q 319576316814478949870590164193048041239 -e 65537

Using (p, q) to initialise RSA instance
n =
c2636ae5c3d8e43ffb97ab09028f1aac6c0bf6cd3d70ebca281bffe97fbe30dd

e = 65537 (0x10001)

d =
1806799bd44ce649122b78b43060c786f8b77fb1593e0842da063ba0d8728bf1

p = 275127860351348928173285174381581152299 (0xcefb2cf7e18a98ebcd36e3e7c3b02b)

q = 319576316814478949870590164193048041239 (0xf06c28e91c8922b9c236e23560c09717)

Saving PEM as private.pem
```

CSDN @该用户正摸鱼

私钥会生成在当前目录下（即rsatool目录）

saving PEM as peivate.pem知道意思就好，所以解密命令那，openssl rsautl -decrypt -in flag.enc -inkey private.pem -out flag.txt，，是有关联的，红色部分应该也知道，就是让rsatool输出一个flag.txt的文本文件，

不用这g就可以直接.pem结尾了， 脑部吧~~~ 

flag.txt里面就是你想要的答案，溜了溜了,我反正整了快5个小时(包括摸鱼聊天)

瞎扯：

gmpy2模块那里可能会有人出错,我觉得大概率是python文件夹那里的问题,在xxx文件夹里有个模块的名称对不上,得改,我以前也是找到一个师傅得博客,上面说把那个模块名字改了就好了,真的就好了,或者pycharm里面安装模块,没试过,python很多模块,前路漫漫

rsatool:

ghub网站下载下来的工具,

名字,版本,说明,作者,作者邮箱,网址,安装所需,脚本文件

我这些都装了,还报错,报错,btm

```
from setuptools import setup

setup(name='rsatool',
      version='1.0',
      description='rsatool can be used to calculate RSA and RSA-CRT parameters',
      author='Joerie de Gram',
      author_email='j.de.gram@gmail.com',
      url='https://github.com/ius/rsatool',
      install_requires=['gmpy2', 'pyasn1'],
      scripts=['rsatool.py']
)
```

CSDN @该用户正摸鱼

```
1 ▶ #!/usr/bin/env python3
2 import base64
3 import fractions
4 import argparse
5 import random
6 import sys
7 import gmpy2
8
9 if sys.version_info >= (3, 5):|
10     from math import gcd
11 else:
12     from fractions import gcd
13
14 from pyasn1.codec.der import encoder
15 from pyasn1.type.univ import Sequence, Integer
16
17 PEM_TEMPLATE = b'-----BEGIN RSA PRIVATE KEY-----\n%s-----END RSA PRIVATE KEY-----\n'
18 DEFAULT_EXP = 65537
19
20 def factor_modulus(n, d, e):
21     if sys.version_info >= (3, 5)
```

```
rsatool x
D:\python386\python.exe D:/迅雷下载/rsatool-master/rsatool.py
usage: rsatool.py [-h] [-n N] [-p P] [-q Q] [-d D] [-e E] [-o OUTPUT]
                [-f {DER,PEM}] [-v]
rsatool.py: error: Either (p, q) or (n, d) needs to be specified
usage: rsatool.py [-h] [-n N] [-p P] [-q Q] [-d D] [-e E] [-o OUTPUT]
                [-f {DER,PEM}] [-v]
```

CSDN @该用户正摸鱼

error: EITHER (p,q).....需要被指定,我搞不来

友情链接: [rsatool工具安装有问题看看这个师傅的](#)

[Linux运用openssl以及rsatool解决一点点rsa的问题 python2.7 \(新手向_Gm1y's Blog-CSDN博客\)](#)
https://blog.csdn.net/jcbx_/article/details/97250664