CTF --第二届春秋欢乐赛-Crypto-Rsa256 writeup

原创

--Xc 于 2018-12-08 20:14:38 发布 1651 收藏 2
分类专栏： RSA 文章标签： crypto
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_41676901/article/details/84897686
版权


RSA 专栏收录该内容
2 篇文章 0 订阅
订阅专栏

打开文件看见：

老规矩，public.kep先扔给openssl解出n和e

给xshell写命令行：

openssl -pubin -text -modulus -in waimup -in public.key

```
root@VM-0-2-debian:/cll/fujian# openssl rsa -pubin -text -modulus -in warmup -in public.key
Public-Key: (256 bit)
Modulus:
    00:d9:9e:95:22:96:a6:d9:60:df:c2:50:4a:ba:54:
    5b:94:42:d6:0a:7b:9e:93:0a:ff:45:1c:78:ec:55:
    d5:55:eb
Exponent: 65537 (0x10001)
Modulus=D99E952296A6D960DFC2504ABA545B9442D60A7B9E930AFF451C78EC55D555EB
writing RSA key
-----BEGIN PUBLIC KEY-----
MDwwDQYJKoZIhvcNAQEBBQADKwAwKAIhANmelSKWptlg38JQSrpUW5RC1gp7npMK
/0UceOxV1VXrAgMBAAE=
-----END PUBLIC KEY-----
```
https://blog.csdn.net/weixin_41676901

然后将n转为十进制：

```
root@VM-0-2-debian:/cll/fujian# python
Python 2.7.13 (default, Nov 24 2017, 17:33:09)
[GCC 6.3.0 20170516] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> n='D99E952296A6D960DFC2504ABA545B9442D60A7B9E930AFF451C78EC55D555EB'
>>> int(n,16)
98432079271513130981267919056149161631892822707167177858831841699521774310891L
>>>
```

所以:

e=65537

n=98432079271513130981267919056149161631892822707167177858831841699521774310891

分解n:factordb.com

q=3028255367440967415185462127611943114 77

p=3250455041864363462098773013201312779 83

聚集了n,e,q,p就可以编写脚本解密了

```
#coding:utf-8
import gmpy
import rsa
p = 3028255367440967415185462127611943114 77
q = 3250455041864363462098773013201312779 83
n = 9843207927151313098126791905614916163189282270716717785883184169952177431089 1
e = 65537
d = int(gmpy.invert(e , (p-1) * (q-1)))
privatekey = rsa.PrivateKey(n , e , d , p , q)      #根据已知参数，计算私钥
with open("encrypted.message1" , "rb") as f:
    print(rsa.decrypt(f.read(), privatekey).decode())       #使用私钥对密文进行解密，并打印
with open("encrypted.message2" , "rb") as f:
    print(rsa.decrypt(f.read(), privatekey).decode())       #使用私钥对密文进行解密，并打印
with open("encrypted.message3" , "rb") as f:
    print(rsa.decrypt(f.read(), privatekey).decode())       #使用私钥对密文进行解密，并打印
```

保存好放到xshell运行，你要的旗出来了！！！！！

```
root@VM-0-2-debian:/cll/fujian# python test.py
flag{3b6d3806-4b2b

-11e7-95a0-

000c29d7e93d}

root@VM-0-2-debian:/cll/fujian#
```