

i春秋第二届春秋欢乐赛RSA256writeup

转载

[weixin_30588827](#) 于 2018-09-09 23:20:00 发布 87 收藏

文章标签: [python](#)

原文链接: <http://www.cnblogs.com/null/p/9615802.html>

版权

i春秋第二届春秋欢乐赛writeup

i春秋 第二届春秋欢乐赛

分值: 100分 类型: Crypto 题目名称: rsa256

已解答

题目内容: [Download](#)

Flag:

提交

解题排名: [1](#) icq7b64725h [2](#) pcat [3](#) <http://blog.csdn.net/xiangshangbashaonian>

下载之后进行解压 发现四个文件

名称	修改日期	类型	大小
encrypted.message1	2017/6/7 12:48	MESSAGE1 文件	1 KB
encrypted.message2	2017/6/7 12:48	MESSAGE2 文件	1 KB
encrypted.message3	2017/6/7 12:48	MESSAGE3 文件	1 KB
public.key	2017/6/7 11:08	KEY 文件	1 KB

0x01看到题目是RSA的 又看到public.key 所以直接用kali linux的openssl

```
root@kali:~# cd Desktop
root@kali:~/Desktop# 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
/0Uce0xV1VXrAgMBAAE=
-----END PUBLIC KEY-----
root@kali:~/Desktop#
```

0x02可以看到e就是Exponent的值

而n的十六进制为Modules 我们用python转成十进制

```
C:\WINDOWS\system32\cmd.exe - python
Microsoft Windows [版本 10.0.16299.125]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>python
Python 3.6.2 (v3.6.2:5fd33b5, Jul 8 2017, 04:57:36) [MSC v.1900 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> a = 0xD99E952296A6D960DFC2504ABA545B9442D60A7B9E930AFF451C78EC55D555EB
>>> a
98432079271513130981267919056149161631892822707167177858831841699521774310891
>>>
```

<http://blog.csdn.net/xiangshangbashaonian>

0x03 再将n进行因式分解来得到我们的p和q (推荐使用<http://factordb.com/>)

The screenshot shows the factordb.com website interface. The search bar contains the number 98432079271513130981267919056149161631892822707167177858831841699521774310891. The search results show the number is factored into two prime factors: 302825536744096741518546212761194311477 and 325045504186436346209877301320131277983. The website also provides options for more information and ECI.

factordb.com - 14 queries to generate this page (0.01 seconds) ([limits](#)) ([imprint](#))

<http://blog.csdn.net/xiangshangbashaonian>

0x04最后一步 我用的kali linux 的python2.7

贴上python2.7代码进行解密

```
1 #coding:utf-8
2 import gmpy
3 import rsa
4 p = 302825536744096741518546212761194311477
5 q = 325045504186436346209877301320131277983
6 n = 98432079271513130981267919056149161631892822707167177858831841699521774310891
7 e = 65537
8 d = int(gmpy.invert(e , (p-1) * (q-1)))
9 privatekey = rsa.PrivateKey(n , e , d , p , q)      #根据已知参数, 计算私钥
10 with open("encrypted.message1" , "rb") as f:
11     print(rsa.decrypt(f.read(), privatekey).decode())      #使用私钥对密文进行解密, 并打印
12 with open("encrypted.message2" , "rb") as f:
13     print(rsa.decrypt(f.read(), privatekey).decode())      #使用私钥对密文进行解密, 并打印
14 with open("encrypted.message3" , "rb") as f:
15     print(rsa.decrypt(f.read(), privatekey).decode())      #使用私钥对密文进行解密, 并打印
```

```
root@kali:~/Desktop/fujian# python 2.py  
flag{3b6d3806-4b2b  
-11e7-95a0-  
000c29d7e93d}  
/blog.csdn.net/xiangshangbashaonian
```

转载于:<https://www.cnblogs.com/nul1/p/9615802.html>