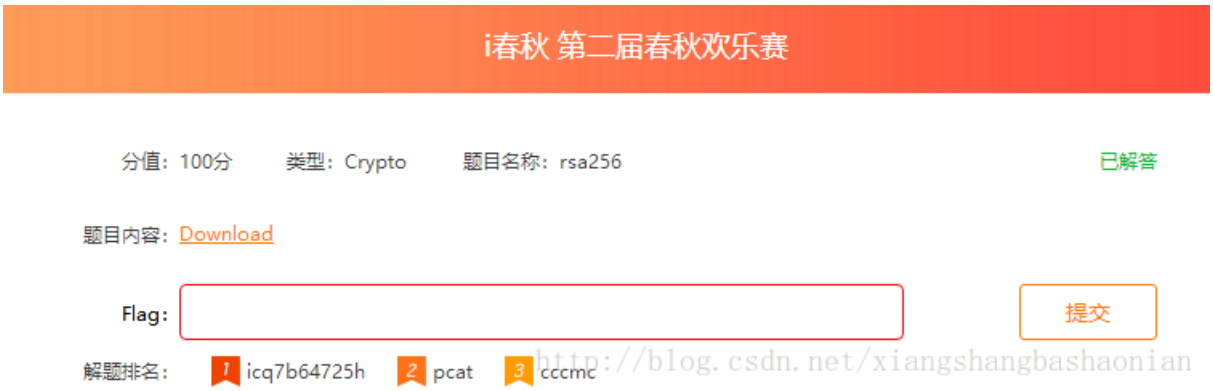
i春秋第二届春秋欢乐赛RSA256writeup

原创

iqiqiya 于 2018-03-15 22:39:31 发布 4792 收藏
分类专栏： ------i春秋第二届春秋欢乐赛 我的CTF进阶之路 文章标签： writeup Crypto RSA256 i春秋第二届春秋欢乐赛

本文链接：https://blog.csdn.net/xiangshangbashaonian/article/details/79575062


------i春秋第二届春秋欢乐赛 同时被 2 个专栏收录
3 篇文章 0 订阅
订阅专栏
我的CTF进阶之路
108 篇文章 18 订阅
订阅专栏



下载之后进行解压 发现四个文件

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
/0UceOxV1VXrAgMBAAE=
-----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
>>>
```


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/)

0x04最后一步 我用的kali linux 的python2.7

贴上python2.7代码进行解密

```
#coding:utf-8
import gmpy
import rsa
p = 302825536744096741518546212761194311477
q = 325045504186436346209877301320131277983
n = 98432079271513130981267919056149161631892822707167177858831841699521774310891
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
```