i春秋第二届春秋欢乐赛RSA256writeup

原创

bingge15 于 2019-10-03 21:42:02 发布 414 收藏

分类专栏： CTF 文章标签： CTF i春秋 RSA

i春秋第二届春秋欢乐赛RSA256writeup

本文python代码引用如下：
本文链接：https://blog.csdn.net/xiangshangbashaonian/article/details/79575062

题目：RSA256

分值：100

第一步：查看题目及附件

根据题目和附件我们可以得到两个消息：

1. 题目是一道rsa的解密题目
2. 附件中给出了三个已经加密后的message和一个public.key

第二步：了解openssl

在很多关于RSA的CTF题目中，我们都会对**OpenSSL**有了一定的了解，下面是介绍（具体的介绍这里就不进行赘述，我挑重点讲）：
OpenSSL整个软件包大概可以分成三个主要的功能部分：密码算法库、SSL协议库以及应用程序。
具体的大家看这个介绍，比较详细：https://blog.csdn.net/funkri/article/details/17533887

这里我们主要是想要在linux中查看到public.key的一系列信息，因此我们用如下命令：

```
openssl rsa -pubin -text  -modulus -in warmup -in -'/home/giantbranch/Desktop/fujian/public.key'
```

当然，后面的是我的public.key在linux中的目录，大家自己改好自己的目录文件。

PS：这条命令我不是很理解，是在网上查到的，希望有大佬可以给我解释一下哈哈。

解析后可以看到public.key的信息：

```
root@ubuntu:/home/giantbranch# openssl rsa -pubin -text  -modulus -in warmup -in
 '/home/giantbranch/Desktop/fujian/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-----
```


将大质数modulus转换为10进制：
98432079271513130981267919056149161631892822707167177858831841699521774310891
这里推荐这个在线进制转换网站：https://tool.lu/hexconvert/

第三步：将modulus分解为p、q：

P = 302825536744096741518546212761194311477
Q = 325045504186436346209877301320131277983
这里推荐这个网站：http://factordb.com/

第四步：计算私钥并解密

```python
#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
```

第五步：解出flag

```
F:\CTF资料\CTF资料\CTF比赛常用工具\密码工具\RSA\proiect\Scripts\python.exe F:/CTF资料/CTF资料/CTF比赛常用工具/密码工具/RSA/rsajiemi.py
flag{3b6d3806-4b2b

-11e7-95a0-

000c29d7e93d}
```