




攻防世界crypto部分Handicraft_RSA的writeup

原创

隐藏起来  于 2020-04-12 17:04:05 发布  801  收藏 2

分类专栏: [CTF # 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/dchua123/article/details/105471989>

版权



[CTF 同时被 2 个专栏收录](#)

20 篇文章 3 订阅

订阅专栏



[crypto](#)

15 篇文章 0 订阅

订阅专栏

有人正在他老房子的地下室里开发自己的RSA系统。证明他这个RSA系统只在他的地下室有效!

1、下载文件丢到kali里看看是啥文件:

```
root@kali:~/Desktop#  
root@kali:~/Desktop# file f5346507773f4b909479387d59a01710  
f5346507773f4b909479387d59a01710: XZ compressed data  
root@kali:~/Desktop#
```

提示是XZ文件, 解压得一个同名的文件, 用editplus打开, 发现是一个加密过程。里面有公钥和加密后的文本。

2、将公钥保存成pub.pem用rsactftool生成私钥:

```
python3 ~/RsaCtfTool/RsaCtfTool.py --publickey pub.pem --private
```

3、将私钥保存成private.pem, 然后进行多次RSA解密, 因为我也不知道加密了多少次, 所以用了100次循环来解密, 代码如下:

```
from Crypto.PublicKey import RSA  
import base64  
with open('private.pem') as f:  
    p = f.read()  
    rsakey = RSA.importKey(p)  
    private_key = RSA.construct((int(rsakey.n), int(rsakey.e), int(rsakey.d)))  
  
msg= base64.b64decode("eER0JNlcZYx/t+71nRvv8s8zyMw8dYspZ1ne0MQuatQncnDL/wnHtkAoNdCa1QkpcbnZeAz4qeMX5GBms0+B  
  
with open('decode.txt', 'w+') as f:  
    for s in range(1,100):  
        msg = private_key.decrypt(msg)  
        f.write(repr(msg) + '\n')
```

4、查看生成的decode.txt, 即可看见flag:

Warning, you are using the root account, you may harm your system.

b'` \xb9\xdd\xa8i}<H\xd46\x93P\xc3X\xc1\xcd\xbd\xd31\x8b\xd0P\xc3\x84\x9b
b" \x0c\x0f\x80\x81\xcd\x19\xdc\x18\x0cjq^\xa5z\xb1\x81?[\x92\xac\xc9\xbf
b' \x13~\xd5\xec\x91\xd3\xef\xdf\xaf\xdc\x17\xe3n\xda\xb4\x16\xdb\x04\xa4
b' \x88\x80Ly\x18\x14+X\xddQ\xb8\x06\xef\xc1D\xddz\xac\xad\xaf\xe9~"\xe4z
b' \xa8\xba\xbd\xe5\x17\xcb]3m\x97\xc4\xa3\xcf\$d\xe4\x7f\xcc\xfc3=\xc7#\x
b' \x02\xb8\tYQ\xca\x84\xff\x80\xd9p\xb1\x1a\xed\x91\x1d\xe0\xa9! \x08\x0e
b' \x81. \xe7[\xcd7qk\xc4\xab\xebz\xfd0x"\xfd\xda)-\xaf3\x12\xe8\x81\xe8\xa
b' p\xc4!B\xbdY\x0f\xa8\$\x7f\x1\x06\xbfh\xb5[h\xa0\xe6\xde\xe8\x1e0z\xe9
b' d#\xc8\x8ekYzIo?Pg\xee\xd0`s\xbaY\x9b\x06F\xd9\xc6\x8b8\xb9\xf6\xf4\x1
b' M\x90\x196\x93\xb5\xff\xe2P\xf7FcGY\x9e\xad6\xc5\xd6\xc4*\xfc\xeb2\x1f
b" c0c\x8c\xe1P\xa5f\xd2F\x8c\x94\xf0\oU\x98\xdd\xdd\xab\xc1\x12\x82\x1f
b' \x8b\xba1T\xbf\x930\x05\x11T\xec\xb8}\xae\xa3N6m\x9cU\x91\xf7\xa1xik.\x
b' (\xc5\xa6#\xfdq6n;\x0e\x12\x80P}\x91\xa4\x1d\xc7\xc0~\r\xe0\xd7\x1d\xcd
b" \x94\xb2*\x97\xf1\xcd\x06W\xc7\x85\xe3\x81\xb4\x9f\x15\x87\xb9\xf1Y\xcd
b' ?2. \x96\r\n\x05\xe62h\&Y_\x97\x85\xa4\x11\x98\xa4\xc7\xab0|P\xa5\xb4
b' 0s\xeb\x06\xbf\x97c\xd2\x14*t-\x8b\xda(!\xa4\\\x18\xe5v\x99\xdc\xcaA%
b' \x15\xbe8\xbb\x9e<\xdb\x0c\x80M\xde^}\xe0\x92\xd6\x9b\xb3\xde\xc6\x15a
b' =\xe9\x8bw\xa6\x8a\x1b\xf2\xb9\xea\xbe\xaa?\xfbi\xb8\xdc\xd1\xe5J\x85
b' b\x16\n\x0c.\x08r!\x05\xbc\x15\x84\xea\xaf\x1c\xb0\x1c\x93K\x86\xb7
b' the flag is: ASIS{n0t_50_e4sy__RSA__in_ASIS!!!}'
b' n\xfe\xf2AP\t.1\xe1;\x97H\xa0\x8f\xac\xa3<\x0e\x95\xd9Y\xb32\xad\x00
b" Z\xdc\x1f\xa6D=\xe3\x03w\xd8\x1b\xc2\xde}\xf8\x82sf\xeb%\xfe\xf0g\xcf8
b' \x93\x11\xd6\x98\xaa\x8b\xb8\xf4#\x12n\xeaU9\xa0\x7f\xfc(:\\\xbc\xc46

flag即是:

ASIS{n0t_50_e4sy__RSA__in_ASIS!!!}