攻防世界 Crypto高手进阶区 6分题 Handicraft_RSA

原创

思源湖的鱼 于 2021-01-18 22:36:49 发布 227 收藏

分类专栏： ctf 文章标签： rsa ctf 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112795826

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的6分题

本篇是Handicraft_RSA的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

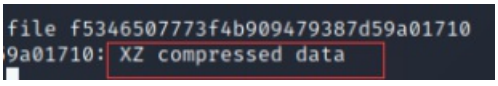
题目描述

得到一个无后缀文件

扔进winhex

没看出来是什么

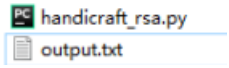
用file命令



XZ文件

- 加上`.xz`后缀
- 命令`xz -d f5346507773f4b909479387d59a01710.xz`解压
- 得到tar文件，`tar -xvf f5346507773f4b909479387d59a01710`

得到一个密文和一段python



内容分别如下

```python
#!/usr/bin/python

from Crypto.Util.number import *
from Crypto.PublicKey import RSA
from secret import s, FLAG

def gen_prime(s):
    while True:
        r = getPrime(s) #生成一个素数r
        R = [r] #将r转换为列表
        t = int(5 * s / 2) + 1
        for i in range(0, t):
            R.append(r + getRandomRange(0, 4 * s ** 2))
            #生成一个0~(4 * s ** 2)的随机数加上r的值并加到列表R里面
        p = reduce(lambda a, b: a * b, R, 2) + 1
        #reduce()函数会对参数序列中元素进行累积。
        if isPrime(p):
            if len(bin(p)[2:]) == 1024:  #[2:]会截掉前面的'0b'
                return p

while True:
    p = gen_prime(s)
    q = gen_prime(s)
    n = p * q
    e = 65537
    d = inverse(e, (p-1)*(q-1))
    if len(bin(n)[2:]) == 2048:
        break

msg = FLAG
key = RSA.construct((long(n), long(e), long(d), long(p), long(q)))
for _ in xrange(s):  #循环加密s次
    enc = key.encrypt(msg, 0)[0]
    msg = enc

print key.publickey().exportKey()
print '-' * 76
print enc.encode('base64')
print '-' * 76
```

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAq+m7iHurBa9G8ujEiTpZ
71aHOVNhQXpd6jCQNhwMN3hD6JHkv0HSxmJwfGe0EnXDtjRraWmS6OYzT4+LSrXs
z9IkWGzRlJ4lC7WHS8D3NWIWYHCP4TRt2N0TlWXWm9nFCrEXqQ3IWgYQpQvKzsds
etnIZJL1tf1wQzGE6rbkbvURlUBbzBSuidkmi0kY5Qxp2Jfb6OUI647zx2dPxJpD
ffSCNffVIDUYOvrgYxIhs5HmCF3XECC3VfaKtRceL5JM8R0qz5nVU2Ns8hPvSVP+
7/i7G447cjW151si0joB7RpBplu44Vk8TXXDAk0JZdW6KwJn7ITaX04AAAAAAAAA
AQIDAQAB
-----END PUBLIC KEY-----
-----------------------------------------------------------------------------
eER0JNIcZYx/t+7lnRvv8s8zyMw8dYspZlne0MQUatQNcnDL/wnHtkAoNdCalQkpcbnZeAz4qeMX
5GBmsO+BXyAKDueMA4uy3fw2k/dqFSsZFiB7I9M0oEkqUja52IMpkGDJ2eXGj9WHe4mqkniIayS4
2o4p9b0Qlz754qqRgkuaKzPWkZPKynULAtFXF39zm6dPI/jUA2BEo5WBoPzsCzwRmdr6QmJXTsau
5BAQC5qdIkmCNq7+NLY1fjOmSEF/W+mdQvcwYPbe2zezroCiLiPNZnoABfmPbWAcASVU6M0YxvnX
sh2YjkyLFf4cJSgroM3Aw4fVz3PPSsAQyCFKBA==
-----------------------------------------------------------------------------
```

把公钥信息保存为`pub.pem`
然后用RsaCtfTool.py获取私钥

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

然后解密

```
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("eER0JNIcZYx/t+7lnRvv8s8zyMw8dYspZlne0MQUatQNcnDL/wnHtkAoNdCalQkpcbnZeAz4qeMX5GBmsO+BXyAKD
ueMA4uy3fw2k/dqFSsZFiB7I9M0oEkqUja52IMpkGDJ2eXGj9WHe4mqkniIayS42o4p9b0Qlz754qqRgkuaKzPWkZPKynULAtFXF39zm6dPI/jUA
2BEo5WBoPzsCzwRmdr6QmJXTsau5BAQC5qdIkmCNq7+NLY1fjOmSEF/W+mdQvcwYPbe2zezroCiLiPNZnoABfmPbWAcASVU6M0YxvnXsh2YjkyLF
f4cJSgroM3Aw4fVz3PPSsAQyCFKBA==")

with open('decode.txt', 'w+') as f:
    for s in range(1,100):
        msg = private_key.decrypt(msg)
        f.write(repr(msg) + '\n')
```

得到flag

```
b'the flag is: ASIS{n0t_5O_e4sy___RSA___in_ASIS!!!}'
```

结语

多次RSA加密