攻防世界 Crypto高手进阶区 1分题 Broadcast

原创

思源湖的鱼 于 2020-12-01 13:51:16 发布 575 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 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/weixin_44604541/article/details/110380957

版权

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1分题

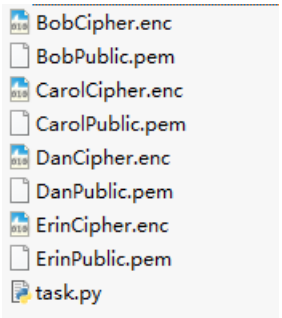
本篇是Broadcast的writeup

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

得到几个流量包和一个python代码



```python
#!/usr/bin/env python3
from Crypto.Util import number
from Crypto.PublicKey import RSA
from hashlib import sha256
import json

#from secret import msg
msg = 'Hahaha, Hastad\'s method don\'t work on this. Flag is flag{fa0f8335-ae80-448e-a329-6fb69048aae4}.'
assert len(msg) == 95

Usernames = ['Alice', 'Bob', 'Carol', 'Dan', 'Erin']
N = [ ( number.getPrime(1024) * number.getPrime(1024) ) for _ in range(4) ]
PKs = [ RSA.construct( (N[0], 3) ), RSA.construct( (N[1], 3) ), RSA.construct( (N[2], 5) ), RSA.construct( (N[3]
, 5) ) ]

for i in range(4):
    name = Usernames[i+1]
    open(name+'Public.pem', 'wb').write( PKs[i].exportKey('PEM') )

    data = {'from': sha256( b'Alice' ).hexdigest(),
            'to'  : sha256( name.encode() ).hexdigest(),
            'msg' : msg
            }
    data = json.dumps(data, sort_keys=True)
    m = number.bytes_to_long( data.encode() )

    cipher = pow(m, PKs[i].e, PKs[i].n)

    open(name+'Cipher.enc', 'wb').write( number.long_to_bytes(cipher) )
```

。。。。。。

这啥啊

直接把flag写在代码里什么鬼

结语

无语