攻防世界 Crypto高手进阶区 5分题 SM

原创

思源湖的鱼 于 2020-12-30 14:31:53 发布 674 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111967593

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的5分题

本篇是SM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

得到三个文件和一段python

```
from Crypto.Util.number import getPrime,long_to_bytes,bytes_to_long
from Crypto.Cipher import AES
import hashlib
from random import randint
def gen512num():
    order=[]
    while len(order)!=512:
        tmp=randint(1,512)
        if tmp not in order:
            order.append(tmp)
    ps=[]
    for i in range(512):
        p=getPrime(512-order[i]+10)
        pre=bin(p)[2:][0:(512-order[i])]+"1"
        ps.append(int(pre+"0"*(512-len(pre)),2))
    return ps

def run():
    choose=getPrime(512)
    ps=gen512num()
    print "gen over"
    bchoose=bin(choose)[2:]
    r=0
    bchoose = "0"*(512-len(bchoose))+bchoose
    for i in range(512):
        if bchoose[i]=='1':
            r=r^ps[i]
    flag=open("flag","r").read()

    key=long_to_bytes(int(hashlib.md5(long_to_bytes(choose)).hexdigest(),16))
    aes_obj = AES.new(key, AES.MODE_ECB)
    ef=aes_obj.encrypt(flag).encode("base64")

    open("r", "w").write(str(r))
    open("ef","w").write(ef)
    gg=""
    for p in ps:
        gg+=str(p)+"\n"
    open("ps","w").write(gg)

run()
```

- 生成ps
- 根据bchoose和ps生成r
- 用choose生成key对flag做AES加密得到ef

所以解题思路是

- 根据ps和r得到bchoose
- 通过bchoose得到choose
- 然后解flag

```
from base64 import b64decode
from hashlib import md5
from Crypto.Cipher import AES
from Crypto.Util.number import long_to_bytes

def cal_k():
    with open('ps','r') as f:
        ps=[long(x) for x in f.read().split('\n')[:-1]]
    with open('r','r') as f:
        r=long(f.read())
    pbits=[bin(x).rfind('1')-2 for x in ps]
    bc=['0']*512
    for le in range(512):
        ind=pbits.index(511-le)
        tt=bin(r)[2:].rjust(512,'0')[511-le]
        if tt=='1':
            bc[ind]='1'
            r^=ps[ind]
    return long(''.join(bc),2)

def solve():
    with open('ef','rb') as f:
        ef=b64decode(f.read())
    key=long_to_bytes(int(md5(long_to_bytes(cal_k())).hexdigest(),16))
    aes_obj = AES.new(key, AES.MODE_ECB)
    return aes_obj.decrypt(ef)

if __name__=='__main__':
    print solve()
```

得到flag：`flag{shemir_alotof_in_wctf_fun!}`

结语

好奇的是题目名是什么意思