攻防世界 Crypto高手进阶区 7分题 SM1

原创

思源湖的鱼 于 2021-02-02 17:36:34 发布 336 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/113284261

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的7分题

本篇是SM1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

得到一段python和三个文件

```
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()
```

分析

- 要解flag，需要choose得到key
- choose的值与r和ps的^运算有关
- ps的值来自于order，而order每个值不同，因此读取ps最后一个1出现位置均不同，通过与r异或是否为0判断某一位是否为1，由此可以组成bchoose

先把值拿出来看看

```python
import os
import base64

r=open("r","r").read()
ef=open("ef","r").read()
ps=open("ps").readlines()

print(ef)
ef=base64.b64decode(ef)
print(ef)

for k in ps:
    if(bin(int(k,10))[-3]=='1'):
        print(bin(int(k,10)))
print(bin(int(r,10)))
```

得到

```
5eFo3ANg2fu9LRrFktWCJmVvx6RgBFzd0R8GXQ8JD78=
b'\xe5\xe1h\xdc\x03`\xd9\xfb\xbd-\x1a\xc5\x92\xd5\x82&eo\xc7\xa4`\x04\\\xdd\xd1\x1f\x06]\x0f\t\x0f\xbf'
0b11001100000101001010010100000101001010001011011100011001011011011010001011010001100110101100000101111111101101
11111011111001000111010010010010101101110110110000111101100110101111100110010011000001100110000000100111111001001
0101101011100010010011110101111000010001001100011111010100100111010101110011000110100001101000001001111101100110
1010111001111010011101110100100100111000100000011111111101101010110011100110110010001011001111010010011001010100
110001001111010100000111010110010101111110101111001001000101100100
0b101111010111110010000110100010000001010101111110001001111110100000111011010001111101010100101110001100110101110
100000101000100101010010110000111010000001110100110110101010101110101001110011001000100101011110001010101111010110
1111110000110011001000110010000001111010101111001110110111111110101101010000100111010001011111100011111011100111000
0100010011001101110100110011001000011001110011100000000100110100110110011100011011001000011001100100000110110110
110110010111001100011111001100001001000100001010111011010010111111
0b110101111110111011100111010000000000110001011100111011111010110111000001111001000000010110010001010101000001111
10100001010101111111110111001100000000010010111011000110111100111100010001001100111010001100110011110000111010111
01001100000000100111000001101101010010001010100001011100101011101011110001101001100010100000100011011000100011001
01110100011000110101111001111100000010000011001010111011011011100011000111010010100101110000010000001100111111000
111011001010010010110001100110001101001010101101010110011100110110
0b100000001111001111010000110101110001111110000110101100000000001011001101011000001000101110001010010010110000001
0101001010101011100110111000110001010100010011110011011010101010101101100100101000000111001101111010101100111011
0001111110100001101110001010011101010010000110010000001100100100110101110000100000001100110111110111111010110101101
100101101000000000101000011011100000001001100000000001010010101100000111110100100110111100000110111011010000111010
01011101110101100000010001110111111101111111000110110101101010100010
```

获取choose

```
psre=[]
for k in ps:
    t=bin(int(k,10))
    psre.append(t)

l=[]
for i in psre:
    if i.rfind('1') not in l:
        l.append(i.rfind('1'))
    else:
        print('error')
        print(i.rfind('1'))

bchoose=[0 for _ in range(512)]
print(bchoose)

r2=int(r,10)
for i in range(512):
    rre=bin(r2)
    rre='0'*(512-len(rre))+rre
    ii = rre[-i-1]
    if(ii=='1' or ii==1):
        sub='1'+'0'*i
        for z in range(512):
            if psre[z][-i-1:]==sub:
                bchoose[z]=1
                r2=r2^int(ps[z],10)
                break
print(bchoose)
i=0
for k in range(512):
    if bchoose[k] ==1:
        i=i^int(ps[k],10)
print(i==int(r,10))
print(bin(i))
print(bin(int(r,10)))
choose=0
for i in range(512):
    choose=choose*2+bchoose[i]
print(choose)
```

得到`114005994730283104806205910741126903187995016424256664495198881524977654754093462012487447348643756901127984345410637679447559582585584284370883728128446 57`

用choose解flag

```
from Crypto.Util.number import getPrime,long_to_bytes,bytes_to_long
from Crypto.Cipher import AES
import hashlib
from random import randint
key=long_to_bytes(int(hashlib.md5(long_to_bytes(choose)).hexdigest(),16))
aes_obj = AES.new(key, AES.MODE_ECB)
flag = aes_obj.decrypt(ef)
print(flag)
```

得到flag：`flag{shemir_alotof_in_wctf_fun!}`

结语

到后面都是阅读源码和找突破点