攻防世界 Crypto高手进阶区 4分题 streamgame2

原创

思源湖的鱼 于 2020-12-18 14:04:42 发布 485 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/111357774

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的4分题

本篇是streamgame2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

得到一个key文件和一段python

key

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCI
00000000	B2	E9	0E	13	A0	6A	1B	FC	40	E6	7D	53					²é j ü@æ}S

```
from flag import flag
assert flag.startswith("flag{")
assert flag.endswith("}")
assert len(flag)==27

def lfsr(R,mask):
    output = (R << 1) & 0xffffff
    i=(R&mask)&0xffffff
    lastbit=0
    while i!=0:
        lastbit^=(i&1)
        i=i>>1
    output^=lastbit
    return (output,lastbit)



R=int(flag[5:-1],2)
mask=0x100002

f=open("key","ab")
for i in range(12):
    tmp=0
    for j in range(8):
        (R,out)=lfsr(R,mask)
        tmp=(tmp << 1)^out
    f.write(chr(tmp))
f.close()
```

和攻防世界 Crypto高手进阶区 3分题 streamgame1

一脉相承

爆破就完事了

```
def check(list1, list2):
    for i in range(12):
        if list1[i] != list2[i]:
            return False
    return True


def lfsr(R ,mask):
    output = (R << 1) & 0xffffff    #将R向左移动1位，bin(0xffffff)='0b111111111111111111111111'=0xffffff的二进制补
码
    i=(R&mask)&0xffffff             #按位与运算符&：参与运算的两个值,如果两个相应位都为1,则该位的结果为1,否则为0
    lastbit=0
    while i!=0:
        lastbit^=(i&1)    #按位异或运算符：当两对应的二进位相异时，结果为1
        i=i>>1
    output^=lastbit
    return (output,lastbit)


if __name__ == '__main__':
    f = open('key','rb')
    content = f.read()
    s_list = []
    for c in content:
        s_list.append(c)

    print(s_list)

    mask = 0x100002

    for i in range(1 << 21):
        print(i)
        tmp_list = []
        R = i
        for j in range(12):
            tmp = 0
            for k in range(8):
                (R, out) = lfsr(R, mask)
                tmp = (tmp << 1) ^ out  # 按位异或运算符：当两对应的二进位相异时，结果为1
            tmp_list.append(tmp)

        if (check(s_list, tmp_list)):
            print(bin(i))
```

得到flag：`flag{110111100101001101001}`

结语

2018强网杯里streamgame是个系列