强网杯部分Crypto题解

原创

Risker_GML 于 2018-03-26 12:10:10 发布 3312 收藏 3
文章标签： CTF 强网杯

周末打了两天强网杯，被大佬虐成狗，web狗做不出来去搞密码.... 爆出三道密码题，题解如下：

题目名称：streamgame1

操作：

分析下载的压缩包，给了一个python脚本和key，key值16进制打开是12个数，脚本里是用flag值和mask等进行一系列加密算法，最终得到12个key文件里的数，而且flag内容为19位的二进制数字，即2^19种可能。所以写脚本爆破，每次按照给出的算法计算出12个值，12个值与key值对应均相等即找到flag，python脚本如下：

```
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)

key=[85,56,247,66,193,13,178,199,237,224,36,58]
mask=0b10100011000100011100

for k in range(2**19):
    R=k;
    a=''
    judge=1
    for i in range(12):
        tmp = 0
        for j in range(8):
            (k, out) = lfsr(k, mask)
            tmp = (tmp << 1) ^ out
        if(key[i]!=tmp):
           judge=0
           break
    if(judge==1):
        print 'flag{'+bin(R)[2:]+'}'
        break
```

FLAG:

flag{11101011000011101011}

题目名称：streamgame2

操作：

和streamgame1思路一样，python脚本如下：

```
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)
key=[178,233,14,19,160,106,27,252,64,230,125,83]
mask=0x100002
for k in range(2**21):
    R=k;
    a=''
    judge=1
    for i in range(12):
        tmp = 0
        for j in range(8):
            (k, out) = lfsr(k, mask)
            tmp = (tmp << 1) ^ out
        if(key[i]!=tmp):
           judge=0
           break
    if(judge==1):
        print 'flag{'+bin(R)[2:]+'}'
        break
```

FLAG:

flag{11011110010100110100 1}

题目名称：streamgame4

操作：思路和streamgame1和streamgame2相同，只是这次key文件给了1024个数，对于没个尝试flag值进行1024次比较太费时间，所以取前5个比较即可(比较前3个或者4个可能出现重的情况)，python脚本如下

```
key=[209,217,64,67,147]
def nlfsr(R,mask):
    output = (R << 1) &0xffffff
    i=(R&mask)&0xffffff
    lastbit=0
    changesign=True
    while i!=0:
        if changesign:
            lastbit &= (i & 1)
            changesign=False
        else:
            lastbit^=(i&1)
        i=i>>1
    output^=lastbit
    return (output,lastbit)

mask=0b11011001101100110110

for k in range(2**21):
    R=k;
    a=''
    judge=1
    for i in range(5):
     tmp=0
     for j in range(8):
        (k,out)=nlfsr(k,mask)
        tmp=(tmp << 1)^out
     if (key[i] != tmp):
            judge = 0
            break
    if(judge==1):
        print 'flag{'+bin(R)[2:]+'}'
        break
```

FLAG:

flag{10010011101010110101 1}

总结：1,2纯靠直接爆破，4偷了一些，key里面那么多数据只有了5个(碰撞几率太小了)，但是streamgame3的题三个一起算，文件数据太多，一般电脑爆不出来...