第三届南宁市网络安全技术大赛部分wp

原创

Jdragon-.- 于 2018-12-16 20:51:00 发布 162 收藏

1、shamir重要数据损坏(Crypto)

题目描述:某集团总裁Shamir将自己使用的笔记本电脑上重要的秘密数据分割成5份子秘密数据，并分别存放在5个存储设备上，其中可以由至少3份子秘密数据联合参与运算，才能重构原来的秘密数据。分割方案使用的参数模数为5987。由于Shamir使用的笔记本电脑感染病毒致使该重要秘密数据损坏无法修复，于是Shamir让技术人员通过存放在编号为5、7、9的三个存储设备的子秘密数据进行重构重要秘密数据，其中编号5的存储设备存放的数据为（5,2258）、编号为7的存储设备存放的数据为（7,2424）、编号为9的存储设备存放的数据为（9,2630）。请问技术人员重构出来的重要秘密数据是多少?
（提示：多项式f(x),x=5,7,9）

题干

shamir典型门限秘密共享，要形成（3，5）门限，则产生一个二次多项式

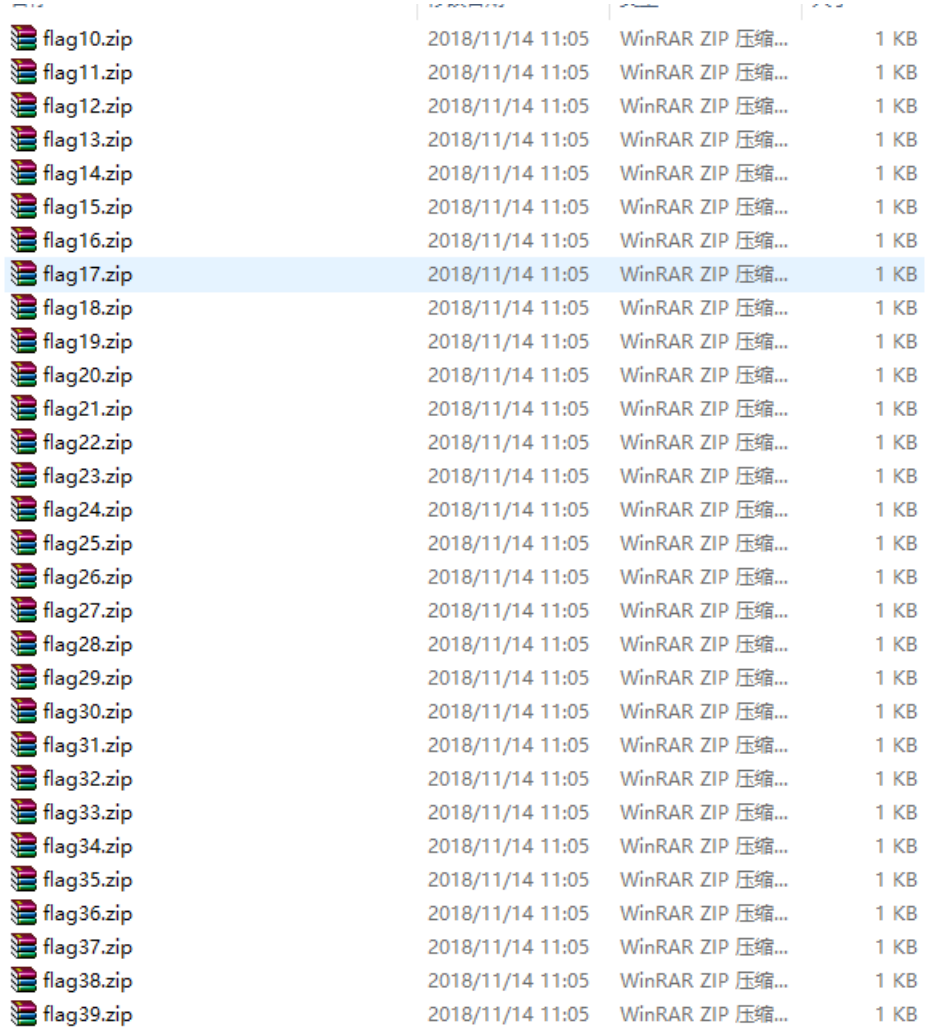
$$f(x)=(ax^2+bx+M) \bmod p$$

根据题目获得对应的三组（f(x)，x）轻易的解出方程。
a = 5，b = 23, M = 2018
而M就为加密的信息，flag为2018提交成功。

2、misc2(MISC)

题目描述:小明下载资源得时候发现变成了压缩包，而且他没有密码，你们能帮帮他吗?
(°—° 〃)

题干



压缩包，崩溃吧

下载文件后，面对密密麻麻的压缩包真的慌的一批，所以一开始并没有认真的看这道题。

CRC32值获得处

后来观测到压缩包全部为大小为3字节的文件，可以统一通过3位CRC32爆破来获取文件内容。

手上并没有能运行这么多crc碰撞的脚本，只能自己写了。

自己手动获取了40个压缩包的CRC32的值（崩溃中）放到TXT跑脚本

0xf3778194	0xe4b738e7
0x28c5fe0e	0x5fc2ce98
0x241A94F3	0xd4620087
0xa408f408	0x3f05477d
0xfdac09a6	0x632f2428
0x5aabe84e	0xe4b738e7
0x632f2428	0x0462d1f9
0x480277eb	0xcd7931c6
0xf3778194	0x7365e16f
0x3a6c61ab	0xff4f5344
0x4a069524	0x6df4ac1a
0x664602fe	0x0d3325ff
0x6d131437	0xf3778194
0x030f15e0	0x7a341569
0x9d8c386e	0x6df4ac1a
0xcd7931c6	0xa408f408
0x9d6b8043	0x142814be
0x28c5fe0e	0xe4b738e7
0x6a996803	0x480277eb
0xca14f5df	0x03e8adcd

所有压缩包CRC32

脚本代码如下

```
import datetime
import binascii
import sys
def showTime():
    print datetime.datetime.now().strftime("%H:%M:%S")
def crack():
    number = 0
    f = open("crc.txt","r")
    lines = f.readlines()
    str1 = ''
    for line in lines:
        crc = int(line,16)
        r = xrange(32, 127)
        for a in r:
            for b in r:
                for c in r:
                    txt = chr(a)+chr(b)+chr(c)
                    crcx = binascii.crc32(txt)
                    if (crcx & 0xFFFFFFFF) == crc:
                        # print hex(crc)
                        # sys.stdout.write(chr(int(txt)))
                        str1 = str1 + chr(int(txt))
        number += 1
        print "find crc "+str(number)
    print str1
if __name__ == "__main__":
    showTime()
    crack()
    showTime()
```

耗时40秒跑出字符串“Z3hubmN0ZnsyaVBfQ3JjX2p1NXRfSzFEZDFuOX0=
”

后带等于号，放进BASE64解码尝试。
得到gxnnctf{2iP_Crc_ju5t_K1Dd1n9}

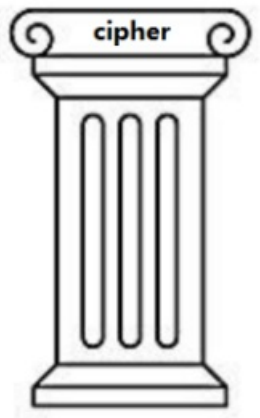
3、这是啥(MISC)

题目描述:666666(题目文件已更新)

附件:下载

题干

下载文件后，有一张图片



GFE-YLCERCNSNLA-AIX{N-PYNET-TSTMYRA}

在图中提取字符串就得到了
GFE-YLCERCNSNLA-AIX{N-PYNET-TSTMYRA}
按图片内容猜测就是栅栏，当时也没认真看题目
只根据之前的经验，和结合这次比赛flag的格式GXNNCTF{*******}对这段字符拆分
尝试拆分代码

```
str1 = 'gfe-ylcercnsnla-aix{n-pynet-tstmyra}'
g,x,n,c,t,f, = [],[],[],[],[],[]
for i in range(0,35):
    if str1[i]=='g':
        g.append((i+1))
    elif str1[i]=='x':
        x.append((i+1))
    elif str1[i]=='n':
        n.append((i+1))
    elif str1[i]=='c':
        c.append((i+1))
    elif str1[i]=='t':
        t.append((i+1))
    elif str1[i]=='f':
        f.append((i+1))
print('g:'+str(g))
print('x:'+str(x))
print('n:'+str(n))
print('c:'+str(c))
print('t:'+str(t))
print('f:'+str(f))
```

```
g:[1]
x:[19]
n:[11, 13, 21, 25]
c:[7, 10]
t:[27, 29, 31]
f:[2]
```

运行结果

可以看到对g,x,f固定位可以得出

```
g x  n n c t f
1 19       2
```

我认为f就是栅栏密码的第二行，而如果将gxnnct这六个字符任意排序能变成等差数列的话，这题就解出来了。
所以最后结果
[图片上传中...(image.png-cd856d-1545043361871-0)]

```
g x  n n c  t f
1 19 13 25 32 7 2
```

恰好形成等差为6的6个数据，这个时候，我恍然大悟，原来题目的66666是这个意思。（汗！）

代码

```
a,b,c,d,e,f=1 ,19 ,13 ,25 ,7 ,31
for i in range(-1,5):
    print (str1[a+i],end='')
    print(str1[b+i],end='')
    print(str1[c+i],end='')
    print(str1[d+i],end='')
    print(str1[e+i],end='')
    print(str1[f+i],end='')
```

```
PS D:\toget> python zl.py
gxnnctf{leemenatry----crypatnalyiss}
```

gxnnctf{leemenatry----crypatnalyiss}提交成功

4、伊丽莎白二世

伊丽莎白今年92岁，直接把标题丢进BASE92得到flag