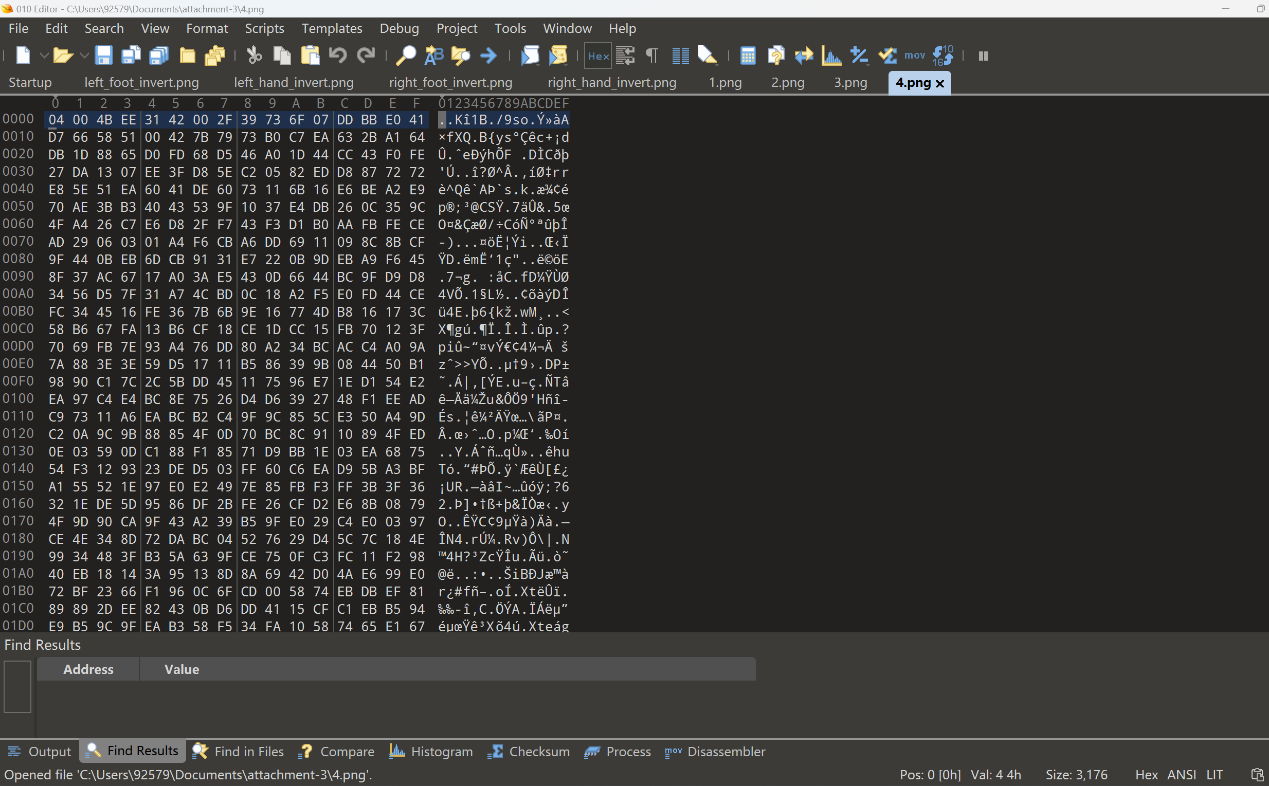
# ISCC2024 WriteUp

Whooops+李卓航+925798691@qq.com

### MISC+[精装四合一](https://iscc.isclab.org.cn/challenges#%E7%B2%BE%E8%A3%85%E5%9B%9B%E5%90%88%E4%B8%80)

### 解题思路

1. 下载，解压压缩包得到4个图片，使用010editor把正常显示图片的数据删去，得到冗余数据，对它们进行异或oxff操作：

使用如下脚本：

1. def xor\_with\_0xff(input\_file, output\_file):
2. with open(input\_file, 'rb') as f\_in:
3. with open(output\_file, 'wb') as f\_out:
4. while True:
5. byte = f\_in.read(1)  # 读取一个字节
6. if not byte:
7. break  # 如果已经读到文件末尾，退出循环
8. byte = bytes([ord(byte) ^ 0xFF])  # 对字节进行异或0xff的操作
9. f\_out.write(byte)  # 将结果写入输出文件
10. # 调用函数对文件进行异或0xff的操作
11. xor\_with\_0xff('C:/Users/92579/Documents/attachment-3/right\_hand\_invert.png', 'C:/Users/92579/Documents/attachment-3/4.png')

2. 再拼接到一起：

使用脚本如下：

fp1 = open('C:/Users/92579/Documents/attachment-3/1.png','rb')

fp2 = open('C:/Users/92579/Documents/attachment-3/2.png','rb')

fp3 = open('C:/Users/92579/Documents/attachment-3/3.png','rb')

fp4 = open('C:/Users/92579/Documents/attachment-3/4.png','rb')

fp5 = open('C:/Users/92579/Documents/attachment-3/5.zip','wb')

for i in range(3176):

    fp5.write(fp1.read(1))

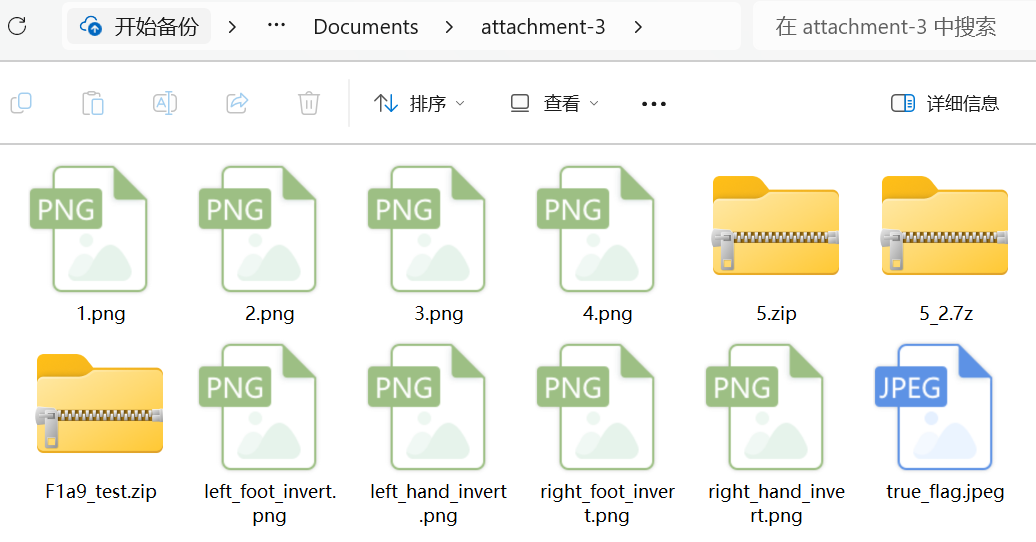
    fp5.write(fp2.read(1))

    fp5.write(fp3.read(1))

    fp5.write(fp4.read(1))

fp5.write(fp1.read(1))

得到一个zip文件，暴力破解得到密码：65537

后续得到的文件截图：

最后解码脚本为：

from Crypto.Util.number import long\_to\_bytes,bytes\_to\_long

import gmpy2

e = 65537

n = 16920251144570812336430166924811515273080382783829495988294341496740639931651

p = 167722355418488286110758738271573756671

q = 100882503720822822072470797230485840381

phi = (p-1)\* (q-1)

d = gmpy2.invert(e,phi)

c = bytes\_to\_long(open('C:/Users/92579/Documents/attachment-3/true\_flag.jpeg','rb').read())

m = pow(c,d,n)

print(long\_to\_bytes(m))