# ISCC2024 WriteUp

AkyOI+李承达+3433778745@qq.com

### Misc+精装四合一

### 解题思路（必须包含文字说明+截图）

去除四张照片的照片部分的数据，剩下来的数据异或0xff之后用脚本拼在一起，

# sudo sysctl -w kernel.randomize\_va\_space=0

from pwn import\*

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

file1 = open('1.png','rb')

file2 = open('2.png','rb')

file3 = open('3.png','rb')

file4 = open('4.png','rb')

res = open('5.zip','wb')

for i in range(3176):

res.write(long\_to\_bytes(bytes\_to\_long(file1.read(1))^0xff))

res.write(long\_to\_bytes(bytes\_to\_long(file2.read(1))^0xff))

res.write(long\_to\_bytes(bytes\_to\_long(file3.read(1))^0xff))

res.write(long\_to\_bytes(bytes\_to\_long(file4.read(1))^0xff))

res.write(long\_to\_bytes(bytes\_to\_long(file1.read(1))^0xff))

发现是个zip，爆破密码是65537，之后里面的word用zip格式打开，media里的true\_flag.png。之后word里面有个大数字n = 16920251144570812336430166924811515273080382783829495988294341496740639931651

,分解之后p = 167722355418488286110758738271573756671

q = 100882503720822822072470797230485840381

之后解个rsa就出flag了

Rsa解密脚本

# sudo sysctl -w kernel.randomize\_va\_space=0

from pwn import\*

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

import gmpy2

e=65537

n=16920251144570812336430166924811515273080382783829495988294341496740639931651

p=167722355418488286110758738271573756671

q=100882503720822822072470797230485840381

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

d=gmpy2.invert(e,phi)

c=bytes\_to\_long(open('flag.jpeg','rb').read())

m=pow(c,d,n)

print(long\_to\_bytes(m))