Nebu1ea 韩磊 1504895347@qq.com

Misc :精装四合一

解题思路：

下载解压后得到4个图片，然后使用winhex把正常图片数据删去，因为图片的尾部标识是AE 42 60 82这一串十六进制符，找到他们，连着他们和前面的数据一起删了，就得到了四个不知名数据文件，依次打开，然后全都和0xff异或，异或后就该提取数据并放到一个文件下了，用的是脚本一。

接着就得到一个zip文件，因为没有提示信息，只能爆破，最终爆出来后得到一个docx文件，全选复制后粘贴出来了，得到了rsa加密的n值

接着把docx的后缀改成zip，能够在word\media下发现一个true\_flag.jpeg。接下来用脚本二。

exp:

脚本如下：

f1 = open('1.png','rb')

f2 = open('2.png','rb')

f3 = open('3.png','rb')

f4 = open('4.png','rb')

f5 = open('5.zip','wb')

for i in range(3176):

    f5.write(f1.read(1))

    f5.write(f2.read(1))

    f5.write(f3.read(1))

    f5.write(f4.read(1))

f5.write(f1.read(1))

脚本二：

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

import gmpy2

e = 65537

n = input("n=:")

p = input("p=:")

q = input("q=:")

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

b = gmpy2.invert(e,a)

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

m = pow(c,b,n)

print(long\_to\_bytes(m))