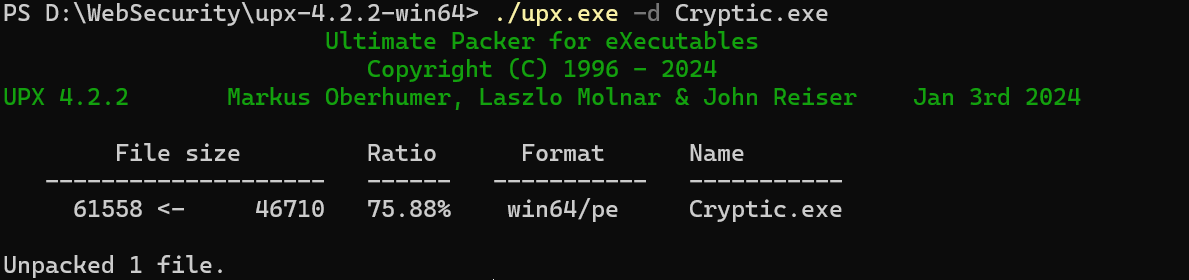
Nebu1ea 韩磊 [1504895347@qq.com](mailto:1504895347@qq.com)

Reverse: CrypticConundrum

解题思路：

Exe文件有upx壳，反编译之前去个壳



接着反编译



其中v8[0],v8[1],v9[0]以及它下面那个，是我们需要利用的，接着跟着程序的思路跑脚本就行了

Exp:

from Crypto.Util.number import \*

def change(a,b):

    tmp=a

    a=b

    b=tmp

    return 0

# 原始加密结果

encrypted\_flag = 0x00000034F088C0F12940C509384AD8F54B32188D7F360D9AB2A56FE836

# 解密原始加密结果得到明文

flag = long\_to\_bytes(encrypted\_flag)[::-1]

# 将明文转换为列表方便处理

flag = list(flag)

result = 'ISCC'

# 第一轮解密

for i in range(len(flag)):

    flag[i] =flag[i]-10

    flag[i] =flag[i]&0xff

# 第二轮解密

for i in range(len(flag) - 1):

    flag[i] = flag[i]+flag[i+1]

    flag[i] = flag[i]&0xff

# 第三轮解密

for i in range(len(flag) - 1):

    flag[i] = flag[i]^ord(result[2])

# 第四轮解密

for i in range(0, len(flag), 2):

    flag[i] = flag[i]^ord(result[i % 4])

# 翻转列表的前半部分

for i in range(len(flag) // 2):

    change(flag[i],flag[26 - i - 1])

# 再次翻转列表的前半部分

for i in range(len(flag) // 2):

    change(flag[i],flag[26 - i - 1])

# 第五轮解密

for i in range(len(flag)):

    flag[i] = flag[i]+ord(result[i % 4])

    flag[i] = flag[i]&0xff

print("Mohtherfuckflag:", bytes(flag))