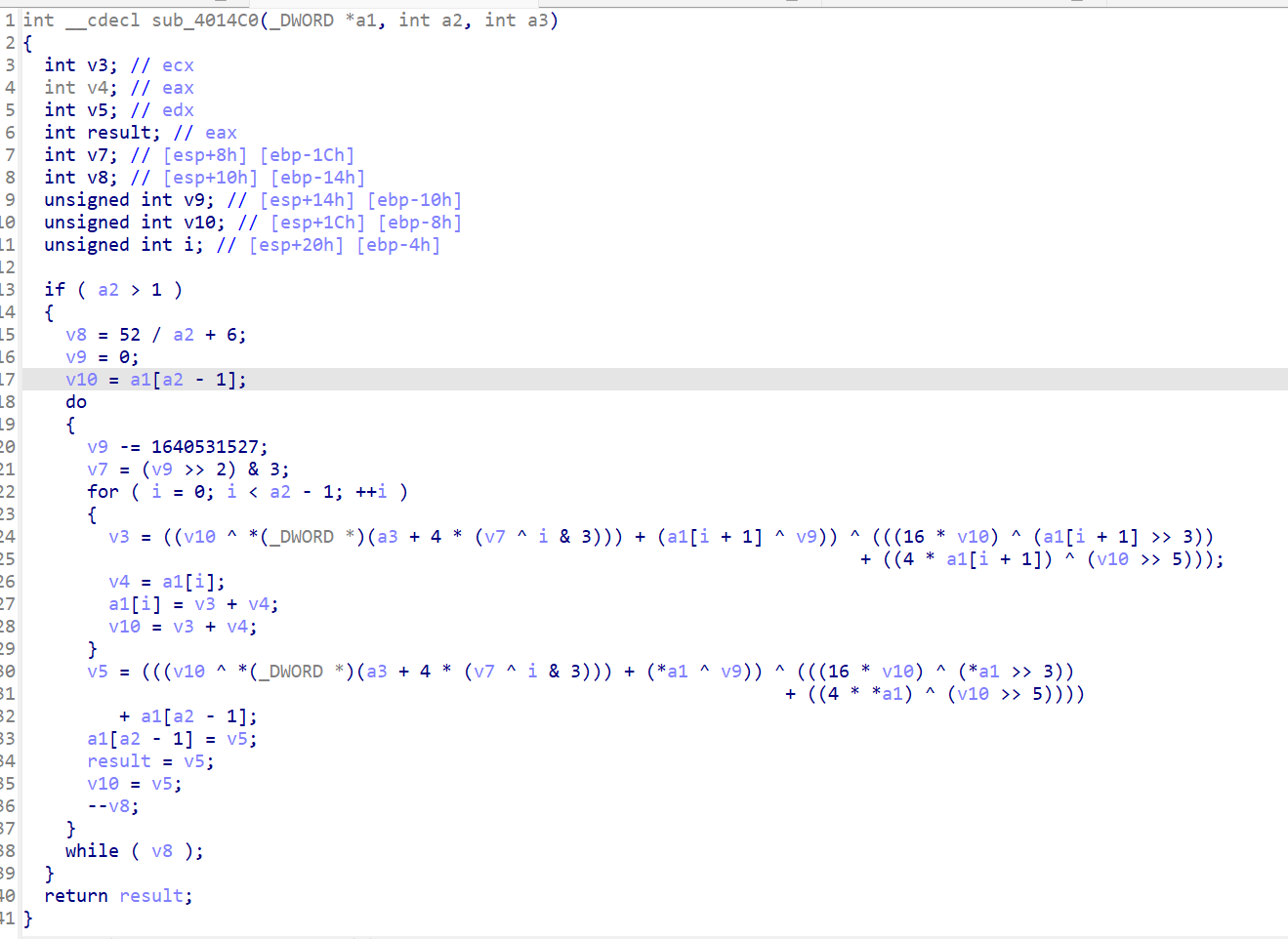
Nebu1ea 韩磊 [1504895348@qq.com](mailto:1504895348@qq.com)

Reverse:Badcode

解题思路：

用ida打开exe文件，发现这个函数：





是XXTEA，直接跟着程序的逻辑跑脚本就行了。

Exp:

from Crypto.Util.number import \*

def change(z, y, c, k, p, e):

    return ((((z >> 5) ^ (y << 2)) + ((y >> 3) ^ (z << 4))) ^ ((c ^ y) + (k[(p & 3) ^ e] ^ z)))

def function1(v, k):

    value = 0x61C88647

    a = len(v)

    b = 6 + 52 // a

    c = (0 - b \* value) & 0xFFFFFFFF

    y = v[0]

    for i in range(b):

        e = (c >> 2) & 3

        for p in range(a - 1, 0, -1):

            z = v[p - 1]

            v[p] = (v[p] - change(z, y, c, k, p, e)) & 0xFFFFFFFF

            y = v[p]

        p -= 1

        z = v[a - 1]

        v[0] = (v[0] - change(z, y, c, k, p, e)) & 0xFFFFFFFF

        y = v[0]

        c = (c + value) & 0xFFFFFFFF

    return v

p = [0XE9EA6C6D,0x2AA28790,0x19DBC6E,0XA1A2F6D5,0x84D19D24, 0xB17BB389]

k = [0x12345678, 0x9ABCDEF0, 0xFEDCBA98, 0x76543210]

d = function1(p, k)

flag=[]

v16='674094872038771148666737'

for i in range(len(p)):

    c=long\_to\_bytes(d[i])

    for j in range(3,-1,-1):

        flag.append(c[j])

for i in range(len(flag)):

    flag[i]^=ord(v16[i])-0x30

    if i%2:

        flag[i]-=2

    else:

        flag[i]+=3

print(bytes(flag))