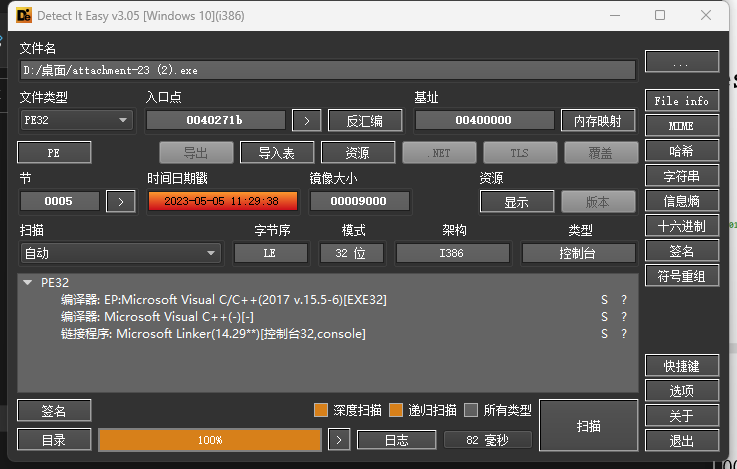
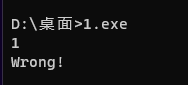
**Pull the Wool Over People's Eyes**

查壳 32位无壳PE文件



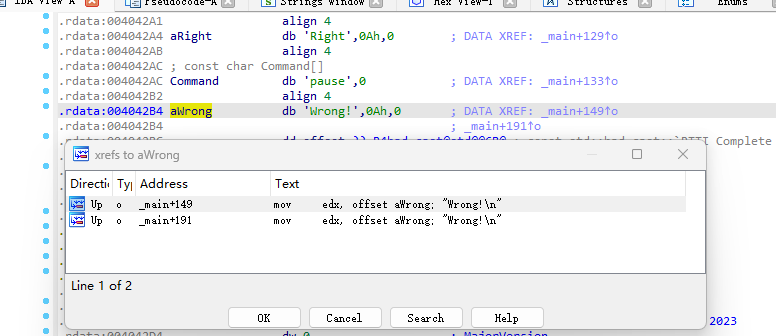
运行一下看看

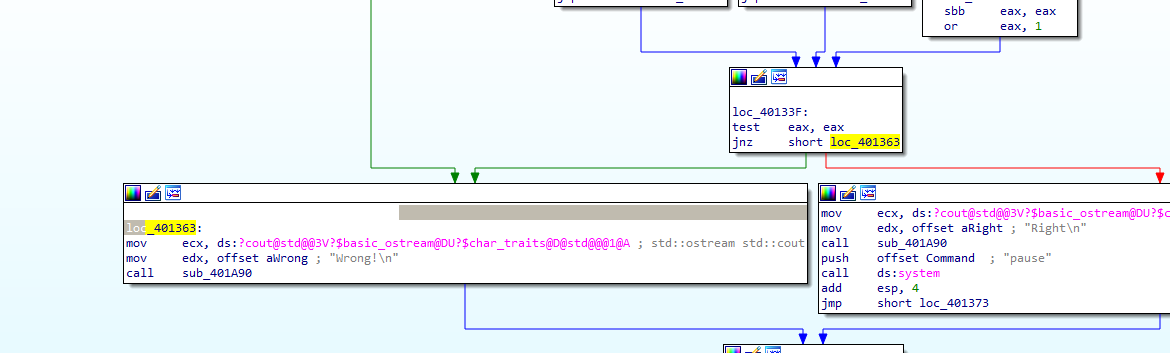


IDA打开

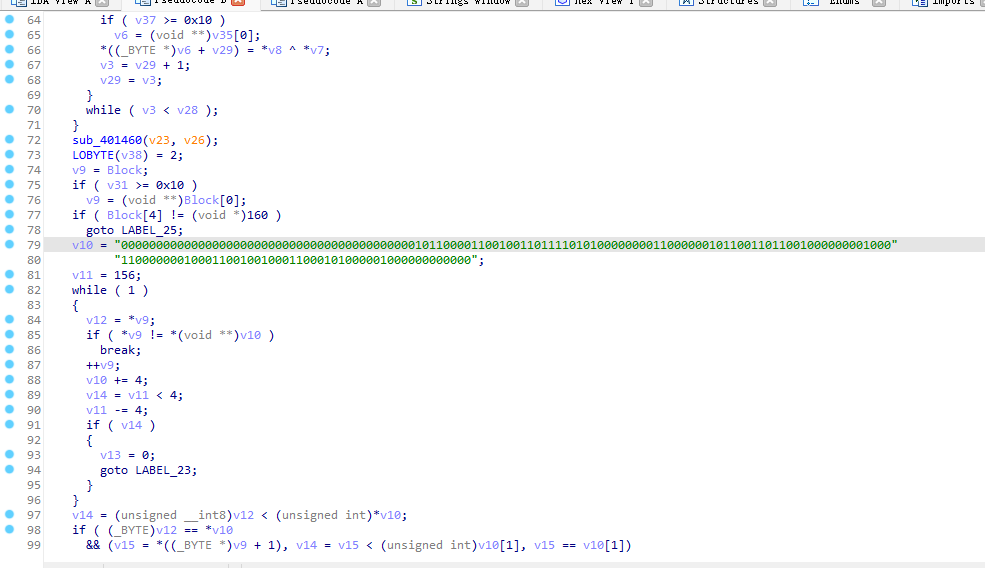
查看字符串列表

跟随 ‘Wrong’字符串





反编译查看main函数伪代码



简单分析一下

编写解密脚本如下

key = list(b'ISCC{ACYeeeloorrsuv}')

flag = "0000000000000000000000000000000000000000001011000011001001101111010100000000110000001011001101100100000000100011000000010001100100100011000101000001000000000000"

for i in range(len(flag)//8):

    print(chr(int(flag[i\*8:i\*8+8],2)^key[i]),end="")