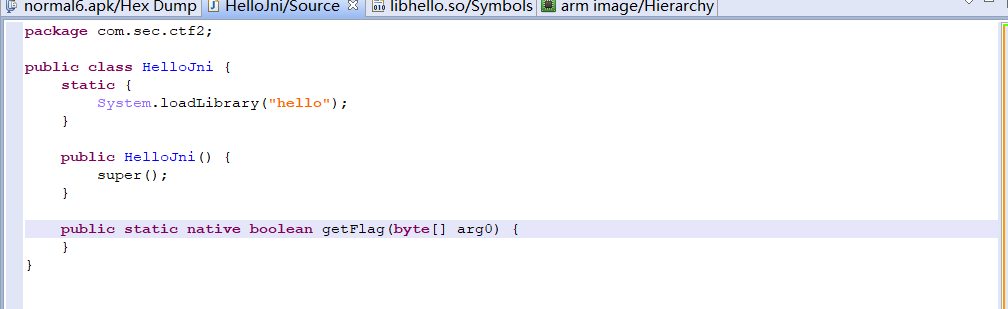
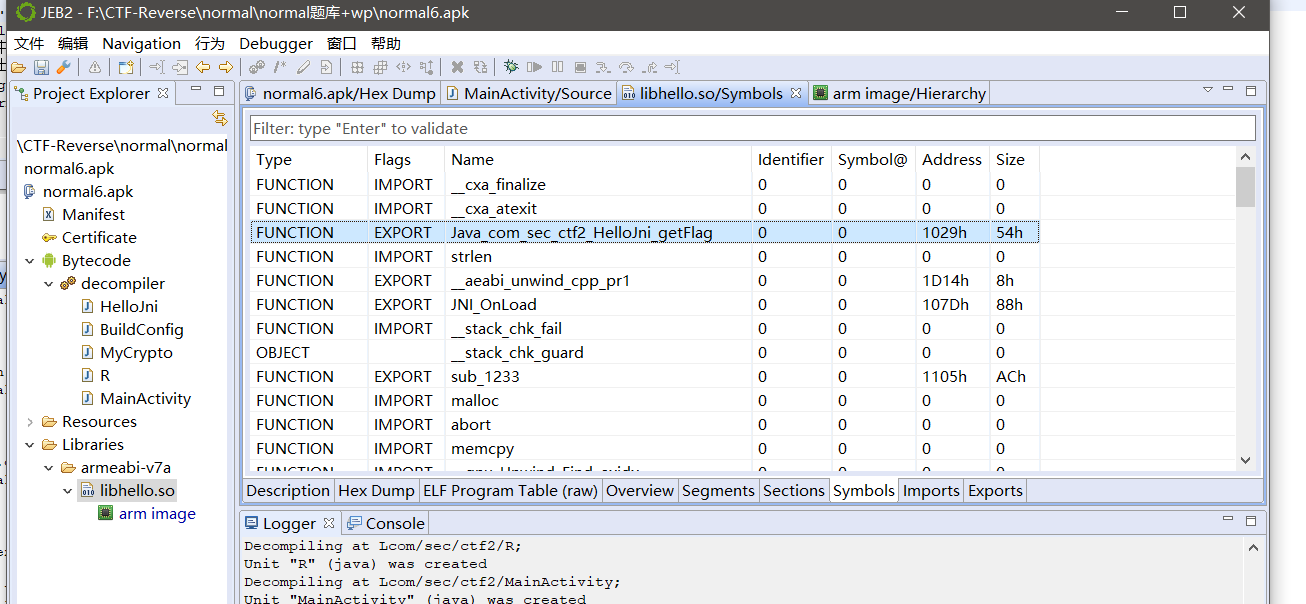
这次是安卓逆向，需要先搞一个jeb然后把normal6拖进去反编译



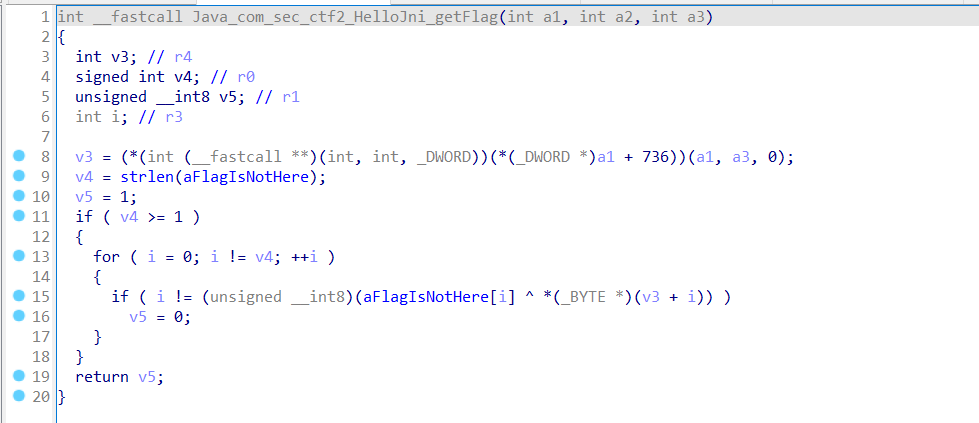
打开这个getFlag函数：



不知所云，上网查后看到说是因为“native关键字连接静态链接库hello，上面也能看到loadLibrary(“hello”)，所以check密码的代码在os文件（静态链接库）中”，然后打开发现确实有这个函数

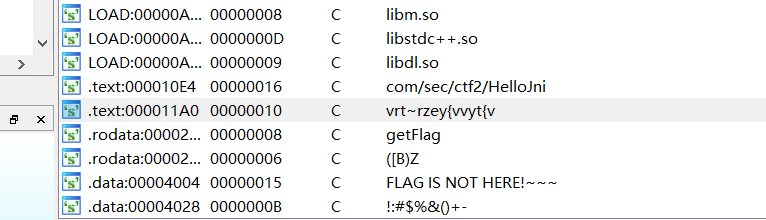


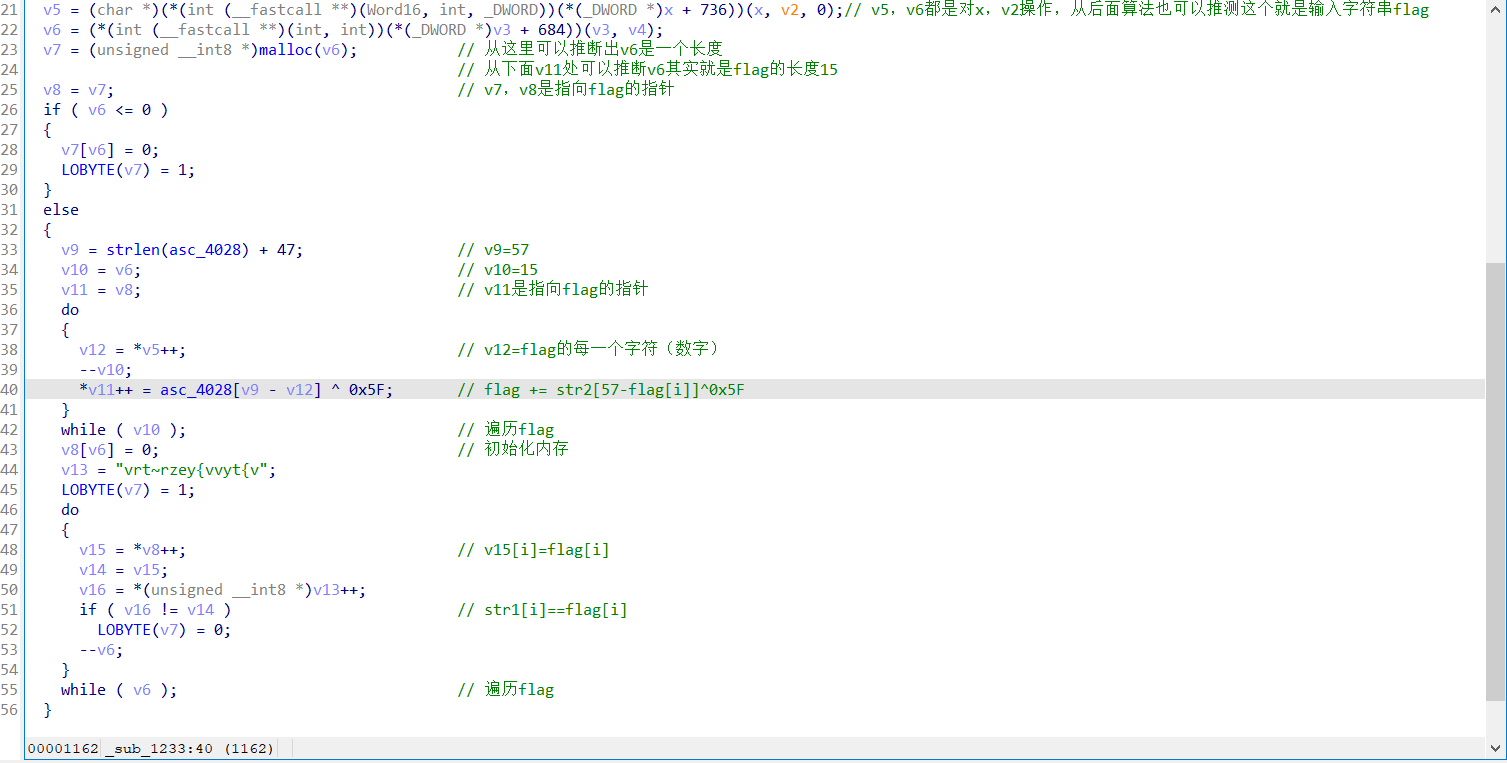
然后压缩这道题，再解压，再把libhello.so文件丢到ida



然后发现提示aFlagNotHere，这是因为真正的函数在启动时候在JNI\_onLoad函数里被替换掉了。

在字符串里找到可疑字符串

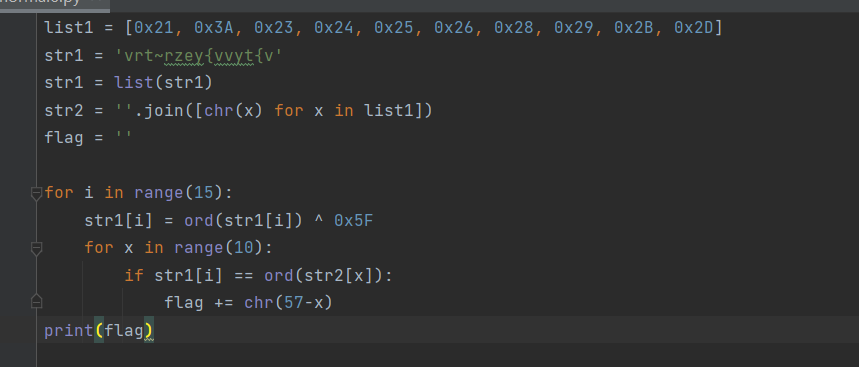






可以总结为str1[i] = str2[57-flag[i]] ^ 0x5F

然后开始写脚本：



Flag:

