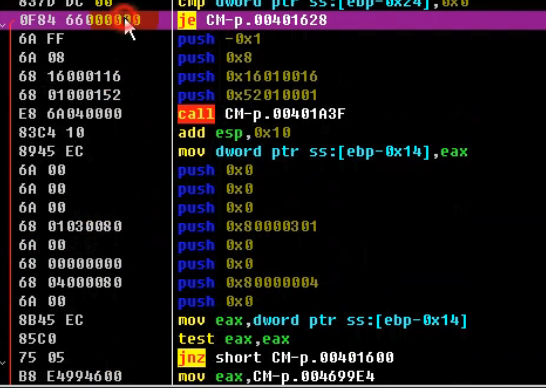
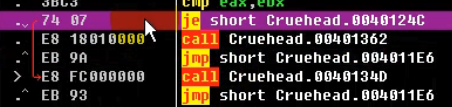
学习沐辰软件破解-逆向工程笔记

1. 如果是易语言编写的程序的话，push连续很多而且是push数值较大的数据的话和msgbox有关。也有的直接在BP按钮上对msgbox下断点。



1. 有的软件做了二次判断，第一层如果je什么的判断为假的话，就call进入一个函数（为注册失败的函数）再jmp回到别的代码退出或者执行别的功能，[这里学习到了F8一步步跟进去的时候，可以使用回车键进入函数，或者直接跟进去进入函数内部，直接执行到返回，再出来]。



1. 万能断点对于没有msgbox的，利用了操作系统的API对方框里面的内容进行获取

然后右键查找-->二进制字串

在HEX窗口输入 F3 A5 8B C8 83 E1 03 F3 A4 E8

然后执行到用户代码

然后寻找跳转，然后NOP什么的。

<理解>win98的API为hmemcpy和ECGetText在winXP上的API为ECGetText。然后GetDIgITemText和GetWindowText都是在输入框获取值的API。题目两个最终都会调用user32.ECGctText.hmemcpy这个API。