读书笔记

一些问题的解答

屈庆磊

quqinglei@icloud.com

2013 年 *5* 月

目录

1 汇编语言，王爽著 **3**

1.1 page: 128, keyword: mov sp,30h question: why 30h? 3

1 汇编语言，王爽著

1.1 page: 128, keyword: mov sp,30h question: why 30h?

desc 我们将 *cs:10 cs:2F* 的内存空间当作栈来使用，初始状态下栈为空，所以 *ss:sp* 要指向栈底，则设置 *ss:sp* 指向 *cs:30*。如果对这点还有疑惑建议回头认真复习一下第三章。

ans 代码中最前面有 24 个字，也就是 48 个字节，转换成十六进制就是 0x30，则为空栈的栈顶地址。或者说，*cs:10 cs:2F* 栈顶为 $0x2F + 1 = 0x30$