上海大学计算机学院

《汇编语言程序设计》报告

姓名 周鹏飞 学号 20121333 指导教师 _____

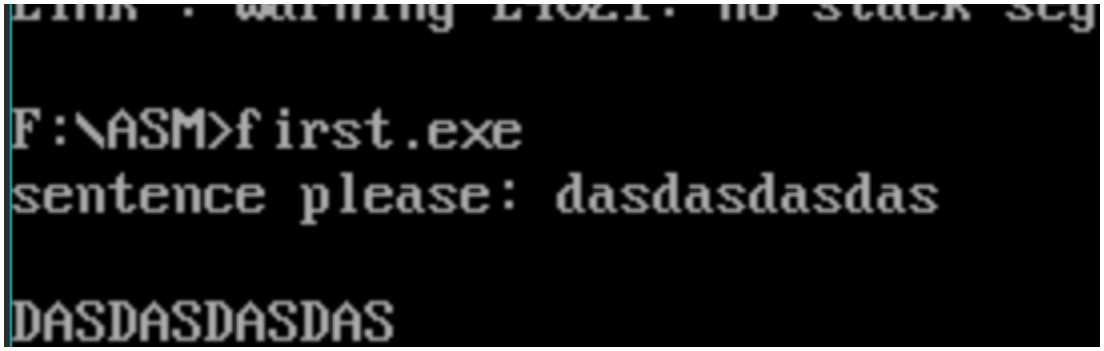
实验名称：小写转大写程序简单改进

一、实验任务

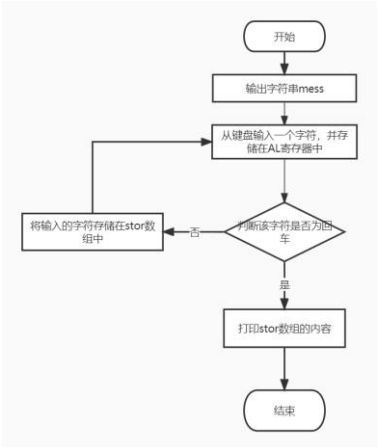
1.生成前述代码的可执行文件，并正确运行；
2.画出代码的流程图；
3.找出前代码的漏洞，并阐述其原因；
4．修改前述代码，消除漏洞；

二、实验内容

1．生成前述代码的可执行文件，并正确运行

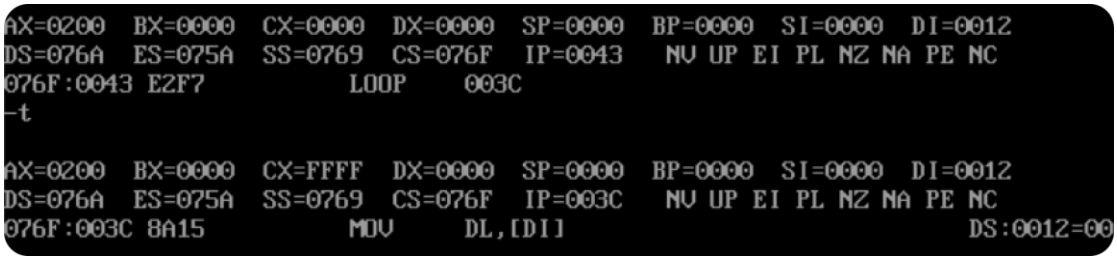


2.画出代码的流程图



3.找出前述代码的漏洞，并阐述原因

1）第一个漏洞就是可能会发生数组越界情况，因为我们最开始定义的数组的长度是 50，如果我们输入的字符串超过 50 之后，程序不会报错，会继续输入，从而导致数组越界的情况。
2）第二个漏洞就是如果我们一开始的时候什么也不输入，直接输入一个回车，程序会输出一大段乱码，原因如下：
程序中，如果我们直接输入回车，程序会跳转到打印 stor 数组流程，我们会用到计数器 cx 但是 CX 寄存器此时的值为 0，所以在进行完第一次 loop 循环之后，CX 寄存器的值会变成最大 FFFFH，那么程序就会将 stor[0]之后的 65535 个内存单元给打印出来，自然就会变成程序显示的那样，输出一大段乱码。



4. 修改前述代码，消除漏洞

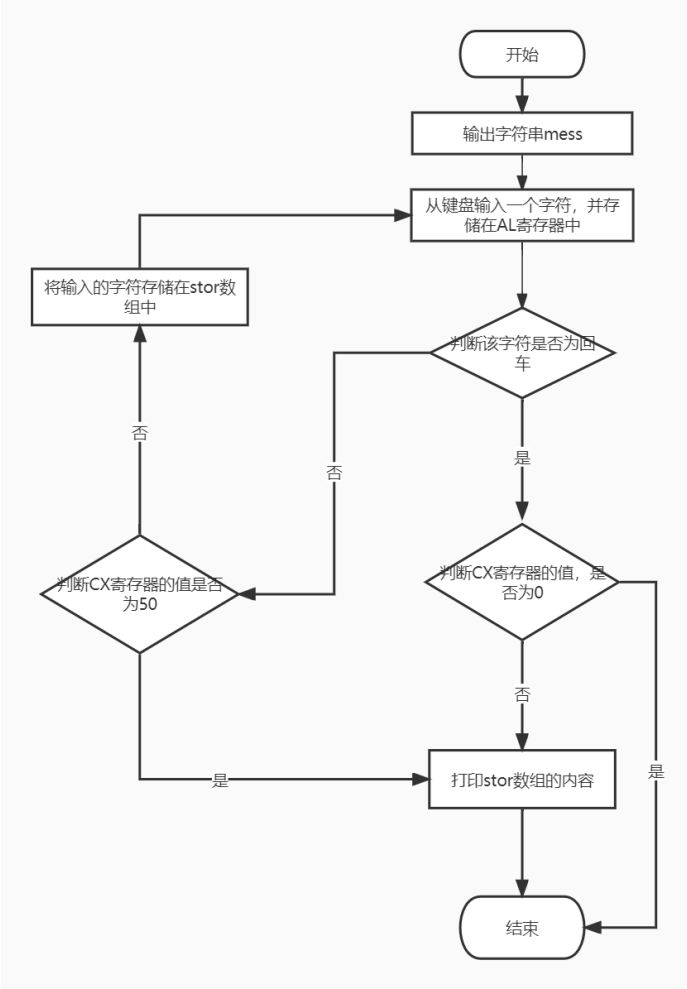
我们可以在输入字符之后添加判断条件，如果 cx 寄存器的值达到 50 的话，就跳转到 output 输出程序：

```
rotate: mov ah,1h
        int 21h
        cmp al,0dh
        jz output
        cmp cx,50
        jz output
```

在 output 程序对 cx 计数器进行判断，如果 cx 的值为 0，说明此时没有输入任何一个字符，直接结束程序：

```
output:
        cmp cx,0
        jz finish
        mov dl,0dh
        mov ah,2
        int 21h
```

5. 修改后代码的流程图如下：


开始
输出字符串mess
从键盘输入一个字符，并存储在AL寄存器中
将输入的字符存储在stor数组中
判断该字符是否为回车
否
是
否
判断CX寄存器的值是否为50
判断CX寄存器的值，是否为0
否
是
是
打印stor数组的内容
结束