|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **年级、专业、班级** | | **2021信息安全02** | | | **姓名** | **于璐** |
| **实验题目** | X86指令系统 | | | | | |
| **实验时间** | **2023/10/21** | | **实验地点** | **DS3305** | | |
| **实验成绩** |  | | **实验性质** | **☑验证性 □设计性 □综合性** | | |
| 教师评价：  ☑算法/实验过程正确； ☑源程序/实验内容提交； ☑程序结构/实验步骤合理；  □实验结果正确； □语法、语义正确； ☑报告规范；  其他：  评价教师签名： 杨吉云 | | | | | | |
| 1. 实验目的 2. 验证X86移位指令 3. 验证X86运算指令 4. 验证X86分支及循环指令 | | | | | | |
| 1. 实验项目内容 2. 写程序在每条指令执行后，观察并记录CF、SF、ZF、OF的值   mov ax, 7FF0h  add al, 10h  add ah,1  add ax, 2   1. 编写程序实现表达式求值：((3450h+76h)\*1234h)/2345h，记录运行结果； 2. 定义数组A为：567Fh, 78FFh, 4C6Ah, 90A4h, 6ABCh, F56Ah，编写程序：    1. 将该数组数据复制到数组B中；    2. 将数组A中每个数据算术左移2位，数组B中每个数据循环右移两位；    3. 将两个数组对应数据进行异或运算，结果保存到A数组中； 3. 定义为“asdterDXRT345\*!@as4”字符串，编写程序：    1. 将其中字母大小写反转；    2. 将其中的数字转换为二进制存储到数组中； | | | | | | |
| 1. 实验过程或算法（源程序）   本节实验课我完成了环境的搭建,怎么使用软件RadASM和OnllyDBG,编写了四个汇编语言程序,并在OD中完成了调试,观测程序运行时的寄存器状态,以及用(F7)快捷键观察第三第四题指令执行的跳转情况  以下是我的代码:  第一题:  1  第二题:  2  第三题:  3132  第四题:  111222 | | | | | | |
| 1. 实验结果及分析和（或）源程序调试过程   **4.1以下是调试过程中第一题寄存器的变化情况**   |  |  |  |  |  | | --- | --- | --- | --- | --- | | 指令 | CF | SF | ZF | OF | | mov ax, 7FF0h | 0 | 0 | 1 | 0 | | add al, 10h | 1 | 0 | 1 | 0 | | add ah,1 | 0 | 1 | 0 | 1 | | add ax, 2 | 0 | 1 | 0 | 0 |   mov ax, 7FF0h  1  add al, 10h  2  add ah,1  3  add ax, 2  4  4.2以下是第二题每条指令执行过后寄存器的内容  mov eax,val1  1  add eax,val2 ;76+3450  2  mul val3 ;(eax)\*1234  3  div val4 ;(eax)\*1234  4  第二题最后的计算结果为双字,存储在eax寄存器中,然后将这个值赋值给定义的变量result即可  在寄存器中我们可以观察到结果为1B3C(存储在eax寄存器中)  余数为190C(存储在edx寄存器中)  内存中的结果:  **内存**  观察到我们的结果00001B3C(商)被写入到内存中,程序执行正确  第三题和第四题寄存器的变化比较复杂,我自己在OD调试并学习.  **4.3第三题编写三个循环分别实现**   * 将该数组数据复制到数组B中； * 将数组A中每个数据算术左移2位，数组B中每个数据循环右移两位； * 将两个数组对应数据进行异或运算，结果保存到A数组中；   其中每次都让esi寄存器存储地址,ecx存储数组A的长度,用edi寄存器寻址数组B;对于(1),循序1现将数组拷贝到寄存器eax中,然后在拷贝到[edi]中  对于(2),用算术移位指令sal,和sar来实现算术左移和算术右移  对于(3)用异或指令运算xor eax,ebx 并将eax的值拷贝到数组A中,即执行指令mov [esi],eax  **第三题内存中结果:**  程序执行前:  **1**  程序执行之后:  **2**  程序执行之后,数组B中值被依次写入内存,此时内存中402018开始为数组B的内容,及原数组右移两位之后的结果  **4.4**  第四题编写一个循环实现大写字母小写字幕的转换以及将数组转变成二进制存储到我定义的数组arrayB中,用以下代码来实现,同时我也学习到了助教的代码,可以用指令or al,00100000B 指令等来进行大小转换!  **第四题内存中结果:**  程序执行之前,内存中的内容  **执行前**  程序执行之后,内存中的结果被修改如下:  观察到字符串中的大小写字母全部发生了翻转,并且数字以二进制的形式存到了数组B中,在内存中的403013位置开始值为03,04,05,04  2  **遇到的问题及解决方案**  1.我在编写第三题的代码时不能编译成功,我将数组A中的f56ah变成0f56ah就可以通过编译了  A dd 567fh,78ffh,4c6ah,90a4h,6abch,0f56ah  2.不能观察除寄存器之外的值,通过询问老师可以到内存区域观察 | | | | | | |