**2022级《汇编语言》**

**作业三答案**

**一、算法题**

1、【10分】

|  |  |  |
| --- | --- | --- |
| 原EBP | <----------ESP | 低地址  高地址 |
| 返回地址 |  |
| 30 |  |
| 20 |  |
| 10 |  |

2、【20分】

AddThree PROC

push ebp

mov ebp,esp

mov eax,[ebp + 16] ; 10h

add eax,[ebp + 12] ; 20h

add eax,[ebp + 8] ; 30h

pop ebp

ret 12

AddThree ENDP

二、简答题

1、【10分】

Stdcall：传参的方式是堆栈传参、传参的顺序是从右到左、堆栈平衡（清理）工作由子函数（被调用者）来完成；

Cdecl：传参的方式是堆栈传参、传参的顺序是从右到左、堆栈平衡（清理）工作由父函数（调用者）来完成；

2、【20分】

Offset：在汇编阶段获取偏移地址、只能取到全局变量的偏移地址；

Addr：在汇编阶段获取偏移地址、只能配合invoke使用，取到传入全局变量参数的偏移地址；

Lea：在执行阶段获取偏移地址，可以获取全局变量、局部变量等采用直接寻址、间接寻址和变址寻址的操作的地址；

3、【40分】

Uses：保存子函数用到的寄存器的值，相当于 push和pop两条指令的功能

Enter：可以简化堆栈帧的建立过程，带有两个参数，相当于 push ebp、mov ebp、esp和sub esp、imm等3条指令的功能；

Leave：可以简化堆栈帧的销毁过程，相当于mov esp、ebp和pop ebp等2条指令的功能；

Invoke：调用函数的另外一种方式，通过该指令调用的函数在调用之前必须进行声明，其本质相当于 push 和 call 的组合。