

实验三

C/ 汇编混合编写操作系统

C 代码生成汇编代码样例

```
int callee(int, int, int);  
int caller(void)  
{  
    int ret;  
    ret = callee(1, 2, 3);  
    ret += 5;  
    return ret;  
}
```



```
caller:  
    push ebp  
    mov ebp, esp  
    push 3  
    push 2  
    push 1  
    call callee  
    add esp, 12  
    add eax, 5  
    pop  
    ret
```

练习

任务 1：汇编中实现简单的按键检测函数 key_detect_simple

其中 c 中调用代码在 main.c 中给出， utils.asm 文件中实现 key_detect_simple

```
key_detect_simple:
    push    esp
    mov     ebp, esp

    xor     eax, eax
    int     0x16
    ;the result will return in eax

    mov     esp, ebp
    pop     ebp
    ret

print_char:
    push    esp
    mov     ebp, esp
    mov     eax, [ebp+0x08]    ;get 1st param

    ;do something here
    mov     ah, 0x0e
    mov     bl, 0x00
    int     0x10

    mov     esp, ebp
    pop     ebp
    ret
```

练习

任务 2： c 中实现简单 print_str ，并在 entry.asm 调用 print_str 显示“ Success.”

编译及镜像生成指令

编译链接：

```
nasm -o boot.bin boot.asm  
nasm -f elf32 -o entry.o entry.asm  
nasm -f elf32 -o utils.o utils.asm  
gcc -c -m16 -o main.o main.c  
ld -static -nostdlib -m elf_i386 -T kernel.lds -o kernel.bin entry.o utils.o main.o
```

镜像生成：

```
dd if=/dev/zero of=os.img bs=512 count=2880  
dd if=boot.bin of=os.img bs=512 conv=notrunc  
dd if=kernel.bin of=os.img seek=1 bs=512 conv=notrunc
```

课后实验

任务 1：实现 utils.asm 文件中以下函数（必做）：

- clr_screen：清除屏幕功能
- key_detect：按键检测功能，可以通过参数指定是否回显检测的按键以及调用时是否阻塞
- read_floppy：读软盘功能，可以通过参数指定起始扇区和扇区大小
- c 中实现简单 print_str_uppercase，实现将字符串转换为大写输出。在 entry.asm 定义字符串 "success"，调用 print_str_uppercase 显示大写字符 "SUCCESS."

课后实验

任务 2：结合之前加载程序实验完成综合实验：

- 在软盘上建立一个表，记录用户程序的名称 / 软盘中的位置 / 字节数 / 内存中的加载地址；
- 设计一组控制台命令，来控制程序的执行和查询程序信息；
- 显示用户程序在软盘中位置、大小以及在内存中的加载地址等相关信息