

# 暨南大学本科实验报告专用纸

课程名称 汇编语言实验 实验项目名称 安装新的 int9 中断例程 实验项目编号 14 实验项目类型 上机 实验地点 517 成绩评定 \_\_\_\_\_  
学生姓名 陈文笛 学号 2021103285 学院 网络空间安全 系 网络空间安全 专业 网络空间安全 实验时间 2023 年 5 月 22 日 下 午 ~    月    日    午  
温度    °C 湿度    指导教师 张银炎

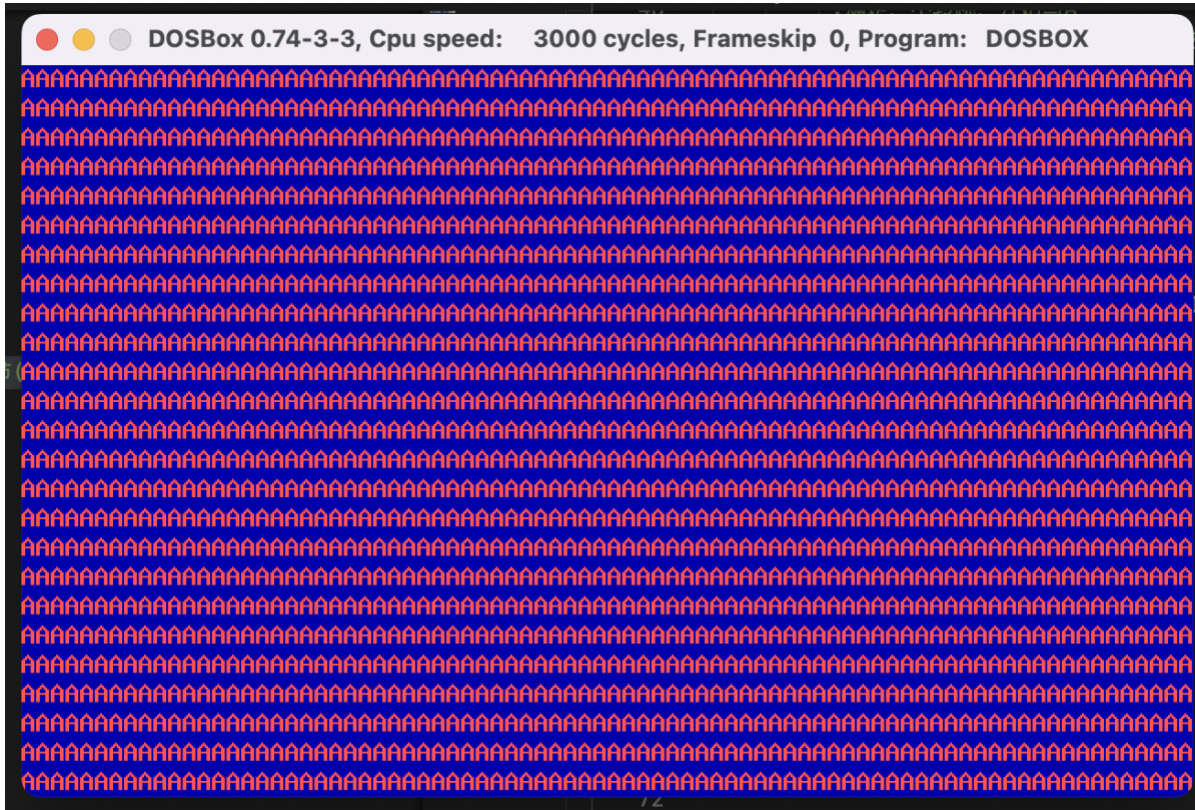
学生签名: 陈文笛

## 实验简介

安装一个新的 int 9 中断例程, 功能: 在 DOS 下, 按下 “A” 键后, 如果松开 则显示满屏幕的 “A” (字符显示属性为蓝底高亮红色), 其他键照常处理。

1. 实验报告中须提供源程序、测试结果截图、及源代码编写思路说明。

## 实验结果截图



## 实验结果分析

如图, 显示满屏幕的 “A” (蓝底高亮红色), 实验成功。不支持全屏, 所以高亮无法显示。

### 编写思路说明

首先从整体过程上来说要实现 3 个部分：1. 编写一个新的中断程序 2. 安装新的中断程序 3. 要保证旧的中断程序的执行

其中 1. 编写一个新的中断程序 的主要实现如下：

1. 从 60h 端口读取输入 2. 判断输入是否符合 3. 若符合，将“A”字符写满显示空间

其中 2. 安装新的中断程序 的主要实现如下：

1. 将新的中断程序复制到安全的空间 2. 将新的中断程序地址写到中断向量表

其中 3. 要保证旧的中断程序的执行 的主要实现如下：

1. 由中断向量表中读取旧的中断程序的地址 2. 保存好旧的中断程序的地址 3. 在新的中断程序执行前利用 call 和旧的中断程序的地址，执行旧的中断程序的地址

### 代码

```
assume cs:code

code segment

    start:

;将程序写入

    push cs

    pop ds;将 cx 赋值给 ds

    mov ax,0

    mov es,ax

    mov si,offset int9;ds:si 为源地址
```

```
mov di,204h;es,di 为目标地址，一段安全的空间 0:200，但前面[200]和[202]要存放原 int9 的 IP 和 CS
```

```
mov cx,offset int9end-offset int9
```

```
cld;传输方向为正
```

```
rep movsb
```

```
;记录下原始的中断程序地址,写入新程序前
```

```
push es:[9*4]
```

```
pop es:[200h]
```

```
push es:[9*4+2]
```

```
pop es:[202h]
```

```
;改变中断向量表
```

```
cli
```

```
mov word ptr es:[9*4],204h
```

```
mov word ptr es:[9*4+2],0
```

```
sti
```

```
mov ax,4c00h
```

```
int 21h
```

```
int9:
```

push ax

push bx

push cx

push es

in al,60h;接收输入

pushf;标志寄存器入栈

call dword ptr cs:[200h];执行旧程序

cmp al,9eh;A 的断码

jne int9ret

    ;满足，不转跳，开始写 A

    ;一般一屏的内容在显示缓冲区共占 4000 个字节(实验 8)

mov cx,2000

mov ax,0b800h

mov es,ax

mov bx,0

s: mov byte ptr es:[bx], 'A'

mov byte ptr es:[bx+1], 00011100B

add bx,2

```
    loop s

int9ret:

    pop es

    pop cx

    pop bx

    pop ax

    iret

int9end:

    nop

code ends

end start
```

