

实验一

实验目的:

1. 了解原型操作系统设计实验教学方法与要求
2. 了解计算机硬件系统开机引导方法与过程
3. 掌握操作系统的引导程序设计方法与开发工具
4. 学习PC字符显示方法、复习加强汇编语言程序设计能力

实验要求:

1. 知道原型操作系统设计实验的两条线路和前6个实验项目的差别
2. 掌握PC电脑利用1.44MB软驱的开机引导方法与过程的步骤
3. 在自己的电脑上安装配置引导程序设计的开发工具与环境
4. 参考样版汇编程序，完成在PC虚拟机上设计一个1.44MB软驱的引导程序的完整工作。
5. 编写实验报告，描述实验工作的过程和必要的细节，如截屏或录屏，以证实实验工作的真实性，按时打包提交实验相关文档。

实验内容:

1. 在自己的电脑上安装一种虚拟机软件，在实验报告中记录主要的安装步骤和截屏。
2. 利用虚拟机软件，生成有1.44MB软驱的一个PC虚拟机，列出PC虚拟机的配置，并生成有1.44MB软盘映像文件3个。
3. 安装winHex等可视化编辑十六进制文件内容的工具，对第一个软盘映像文件的首扇区填满个人学号姓名拼音。
4. 安装一种x86汇编程序和一种编辑汇编/C源程序代码的工具或集成环境。
5. 用x86汇编语言编写一个程序，参考字符反弹运动示范程，修改或重写程序，直接对文本方式的显存进行操作，以某种运动轨迹或几何图像在屏幕一个区域显示字符或字符串，还可以有各种个性化变化效果，能看到个人学号或姓名拼音。
6. 程序汇编后满足引导扇区程序的要求，利用工具将其制作写入1.44mb软盘映像的引导扇区中，保证在虚拟机中能引导执行，观察到效果。
7. 建立自己的软件项目管理目录，管理实验项目相关文档

实验过程:

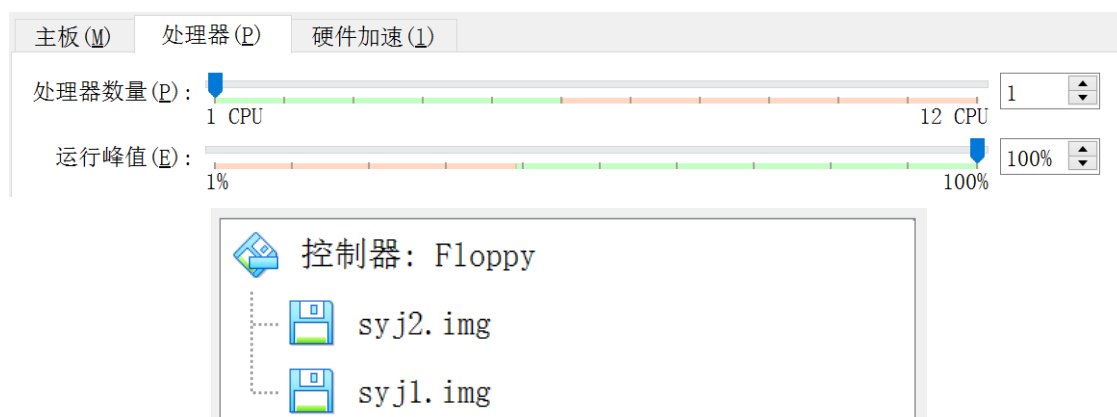
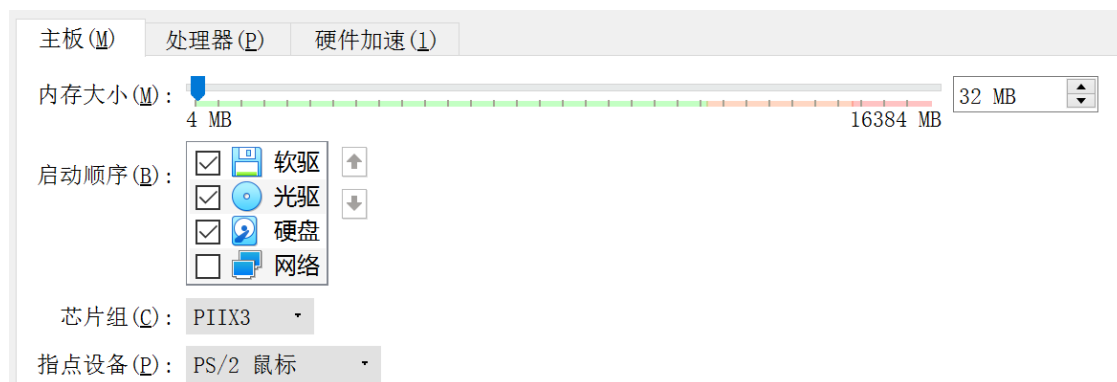
1. 我在自己的电脑上安装了两个虚拟机软件，分别为VirtualBox和VMware，本次实验主要用VirtualBox来实现；安装步骤其实只需要一直点确定即可



2. 利用VirtualBox生成一个有软驱的虚拟机的步骤如下：

1. 点击“新建”，名称和文件夹可以任意填，类型选择“other”，版本选择“other/unknown”
2. 内存大小选择32MB（或更多）
3. 虚拟硬盘选择“现在创建虚拟硬盘”
4. 虚拟硬盘文件类型选择“VDI”
5. 存储方式选择“动态分配”
6. 文件位置默认，大小选择2GB
7. 创建完成后，点击“设置”：在“系统”中将启动顺序将“软驱”调到最高，在“存储”中点击“添加软盘控制器”，再“添加虚拟软驱”，“选择磁盘”，“注册”，再选择你所创建的img文件，点击“选择”，最后点击“ok”即可保存设置

最后的各种配置数据以及3个软盘映像文件如下图（其中syj1.img为第三问所用img文件，syj2.img为第五第六问所用img文件，syj3.img根据老师要求仅为备用，无任何作用）



由于VirtualBox一个虚拟机最多链接两个软盘映像文件，因此只显示两个

3. 在这一步需要新建一个空img文件，步骤如下：

1. 使用记事本新建一个asm文件，输入代码如下：

```
times 510-($-$$) db 0
dw 0xaa55
```

2. 将上述文件放入nasm根目录，nasm使用命令 `nasm syj1.asm -o syj1.bin` 生成bin文件

3. 直接改后缀名生成img文件，即新建了一个基本不含数据的img文件

之后百度下载winHex，使用winHex打开该img文件，如图所示

syj1.img																																
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000064	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000384	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

使用winHex填满syj1.img文件的步骤如下

1. 将我的学号和拼音翻译成16进制：31 38 33 34 30 31 34 36 73 6f 6e 67 79 75 6a 69 65
2. 鼠标点击第一个0，输入上述16进制数据
3. 一直输入到510位，注意保留最后的55AA

填满效果如下图：学号为18340146，拼音为songyujie

syj1.img																																ANSI ASCII															
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31															
00000000	01	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	8B340146songyujiel3840146songyujiel														
00000032	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	ie18340146songyujiel3840146songyujiel3840146songyujiel3840146son													
00000064	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	gyujie18340146songyujiel3840146son													
00000096	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	gyujie18340146songyujiel3840146s														
00000128	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	ongyujiel3840146songyujiel3840146s														
00000160	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	146songyujiel3840146songyujiel3840146songyujiel3840146son														
00000192	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	146songyujiel3840146songyujiel383														
00000224	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	40146songyujiel3840146songyujiel3840146songyujiel3840146son														
00000256	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	8340146songyujiel3840146songyujiel3840146songyujiel3840146son														
00000288	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	ie18340146songyujiel3840146songyujiel3840146son														
00000320	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	ie18340146songyujiel3840146son													
00000352	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	67	yujiel3840146songyujiel3840146so													
00000384	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	ngyujiel3840146songyujiel3840146s														
00000416	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	sonyujiel3840146songyujiel3840146sonyujiel3840146sonyujiel3840146sonyujiel3840146son														
00000448	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	46songyujiel3840146songyujiel3834														
00000480	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	31	38	33	34	30	31	34	36	73	6F	6E	67	79	75	6A	69	65	55	AA	0146songyujiel3840146songyujiel3840146songyujiel3840146son														

4. 安装的x86汇编程序为nasm，编辑汇编程序代码的程序为记事本/Visual Studio，编辑C源程序的集成环境为devc++，安装方式均为直接百度软件名称，在官网下载安装包，安装即可。



5. 实现的效果如下：

- 显示学号姓名
- 字母顺序变化

- 新增：字母碰到边缘变化颜色
- 新增：学号姓名带有闪烁效果

老师代码纠错部分：

```
mov [es:bx],ax           ; 显示字符的ASCII码值

                        ; 原代码是mov es[bx],ax, 不符合x86编码规则, 无法通过编译
```

显示学号姓名（闪烁效果）关键代码：

```
code:
    org 7c00h           ; 程序加载到100h, 可用于生成COM/7c00h引导扇区程序
    mov ax,cs
    mov es,ax           ; ES = 0
    mov ds,ax           ; DS = CS
    mov ax,name         ; name为学号和姓名
    mov bp,ax
    mov cx,12
    mov ax,01301h
    mov bx,008ch        ; b1 = 8ch, 8代表闪烁效果+黑底色, c代表字母颜色为红色
    mov dl,0
    int 10h
```

字母顺序变化关键代码：

```
change2:
    mov byte[char],'A'   ; 重置字母
    jmp show2

show:
    ...
    inc byte[char]       ; 显示的字符ASCII码++
    mov dl,91
    mov cl,byte[char]    ; cl=显示的字符ASCII码
    sub dl,cl            ; dl-cl
    jz change2           ; 如果dl=0 (即cl=91), 跳转到change2重置字符
    ...
```

字母碰到边缘变化颜色关键代码：

```
d12dr:
    mov word[y],1
    mov byte[rdu1],Dn_Rt
    jmp change

d12ul:
    mov word[x],23
    mov byte[rdu1],Up_Lt
    jmp change           ; 一共有8个转向部分代码, 此处以两个为例
                        ; 修改方式为jmp show改为jmp change
                        ; 新增change代码如下

change:
    inc ch               ; ch++
    mov dh,16
```

```

sub dh,ch          ; dh-ch
jz change1         ; 如果dh=0（即ch=16），跳转到change1重置颜色
jmp show

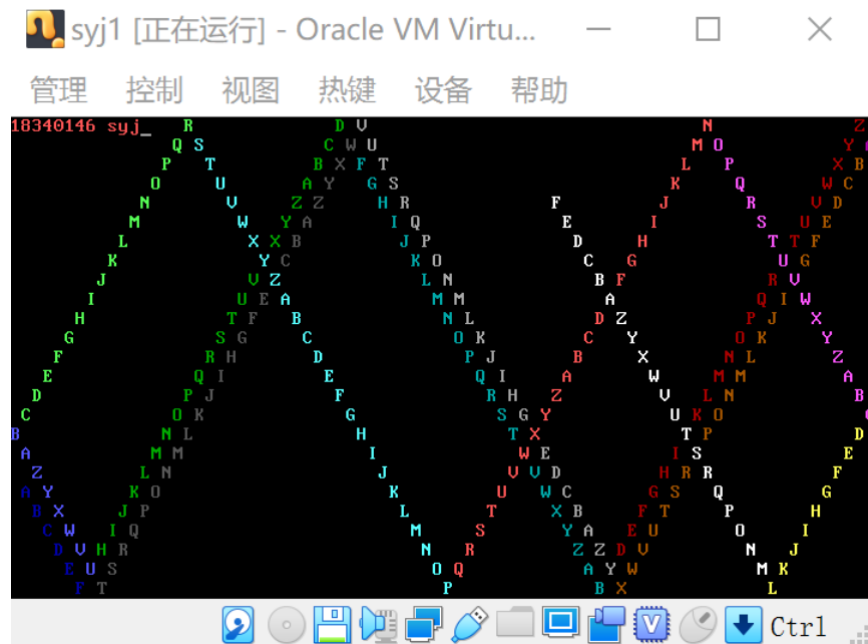
change1:
mov ch,1           ; 重置颜色
jmp show

```

6. 生成img文件步骤:

1. 上述代码保存为asm文件，放入nasm根目录下
2. nasm使用命令 `nasm syj2.asm -o syj2.bin` 生成bin文件
3. 直接改后缀名生成img文件

生成后将img文件导入虚拟机中，启动虚拟机，结果如下图：



闪烁效果截图无法体现，请打开syj2.img文件查看

7. 建立自己的软件项目管理目录如下图

电脑 > 桌面 > S & W > 操作系统 > 18340146_宋渝杰_实验一_v1 >

名称	修改日期	类型	大小
src	6/5/2020 下午 8:04	文件夹	
report.pdf	28/4/2020 下午 8:52	PDF 文件	980 KB

电脑 > 桌面 > S & W > 操作系统 > 18340146_宋渝杰_实验一_v1 > src

名称	修改日期	类型	大小
syj.asm	6/5/2020 下午 7:14	Assembler Source	4 KB
syj1.img	28/4/2020 下午 4:25	光盘映像文件	1 KB
syj2.img	6/5/2020 下午 7:14	光盘映像文件	1 KB
syj3.img	28/4/2020 下午 7:45	光盘映像文件	1 KB

实验心得:

遇到的问题和实验过程:

1. 最初在把老师的代码拿去nasm编译的时候，编译器直接报错：error: 161行“es无法识别”
2. 修改完代码之后，添加55AA后缀，并稍微修改顶部代码，通过上述生成img步骤生成img，放入虚拟机运行后，可以成功显示反弹程序，此时字符和颜色还未能变化

3. 修改顶部代码，加入上述显示学号姓名代码（当时bx = 000ch），同样生成img后运行，可以显示红色的学号姓名于左上角
4. 修改show：后的代码，同时添加ch和cl用于记录字母和颜色的变化，实现字母的变化功能（当时同时实现字母变化的同时，颜色和底色也变化），此时得到v0版本
5. 删除v0的颜色和底色变化（感觉丑陋），分析程序找到转换方向部分的代码，修改成上述“字母碰到边缘变化颜色关键代码”所示，实现字母碰到边缘变化颜色的功能
6. 学习 int 10h 的各项数据，思考如何添加闪烁效果：了解到 ah = 13h 时为显示字符串功能，而 bl 为控制显示字符串的颜色、底色和特效，经过多次赋值尝试后，得到：当 bl >= 80h 时，具有闪烁效果，第一个数为8时，为闪烁加黑底色效果，第二个数控制字母颜色，为c时是红色字体效果，于是将 bx = 008ch时，实现显示字符串带闪烁效果

总的来说，虽然我在本次实验遇到的问题不大，但是搜索知识、修改代码和测试研究还是有不少工作量的，大致花费了约完整的3天时间。在这次实验当中，也收获了不少汇编代码的一些细节知识，BIOS的中断知识等等，印象深刻的是我更加熟悉了x86的跳转判断，也能比较好的进行运用了。

参考资料：

<https://blog.csdn.net/hua19880705/article/details/8125706>