

操作系统原理 实验

主讲：凌应标

isslyb@mail.sysu.edu.cn

教材与主要参考书

<http://sist.sysu.edu.cn/~isscwli>

教材：自编

参考文献

- 于渊 著. 《Orange's: 一个操作系统的实现》. 电子工业出版社, 2009年6月
- 李无言 著. 《一步步写嵌入式操作系统——ARM编程的方法与实践》. 电子工业出版社, 2011年1月
- 李忠著. 《x86汇编语言-从实模式到保护模式》. 电子工业出版社, 2013年1月

课程要求与成绩计算

■ 免考

- 条件：实验1~6全部评价AAAAB+B+或相当
- 最终成绩可能范围：75分以上

■ 非免考

- 平时项目评价占50%
- 期终上机考试占50%

实验项目要求

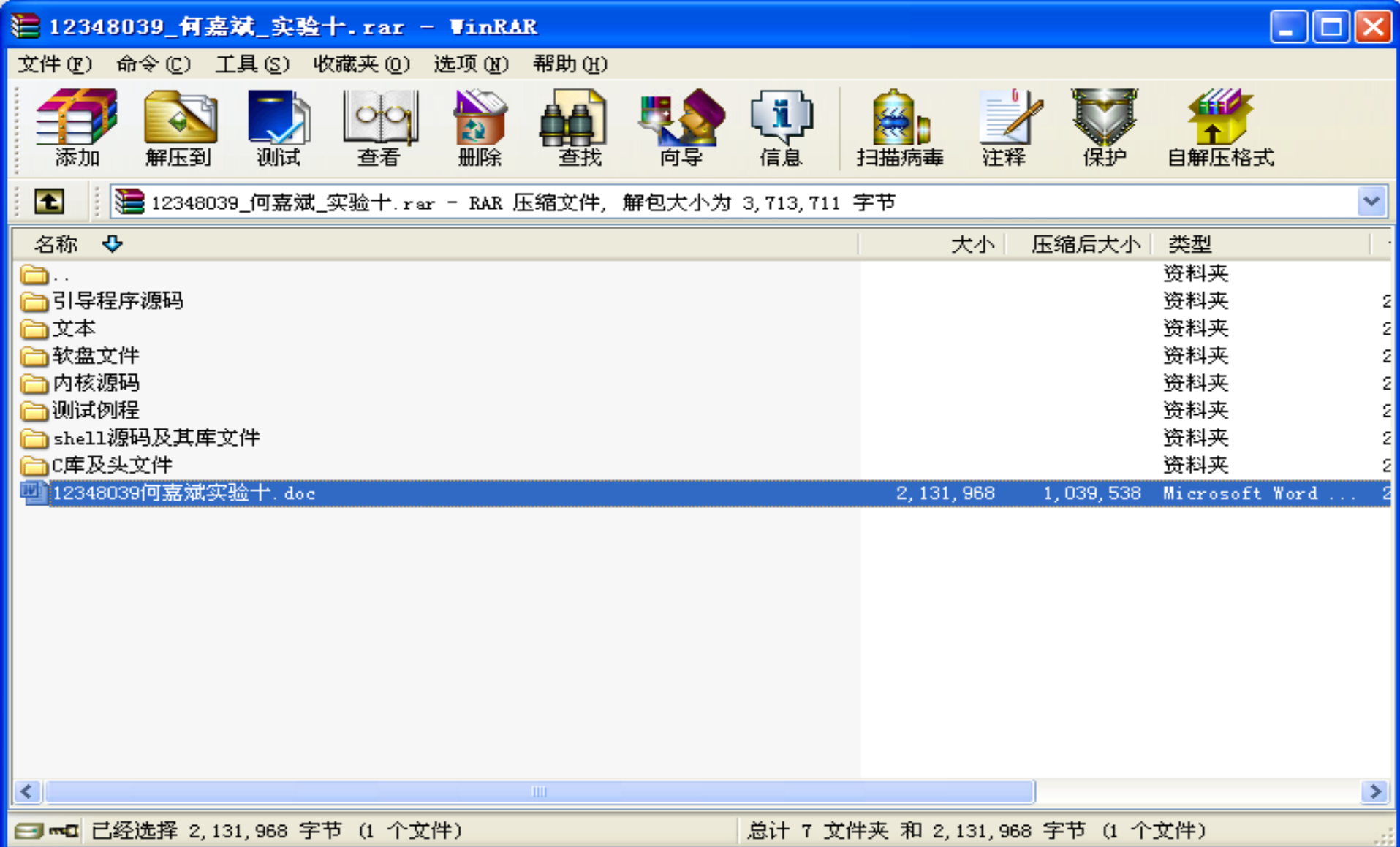
- 基础实验项目5个和扩展实验7个
- 实验项目，迟交影响成绩评价！
- 工具与环境可由选择，开发新型工具或优化一套开发环境都可**加分**！
- 一系列基础实验项目必须连续完成，**当前项目只能在前一个项目的基础上进行，体现出前后的进化关系，否则要被约谈，证明没有抄袭行为！**
- 一个项目可提交多个改进的版本，实现新功能和个性化特征都有利于提高相应项目的成绩。
- 实验项目提交内容用winrar工具整体压缩打包，统一格式命名为：
<学号>+<姓名>+<实验项目号>+<版本号>.rar



实验项目提交内容

- 实验报告：电子版（Word2003的DOC格式或PDF格式）
- 原程序文件及可执行代码程序文件
- 测试输入数据文件和输出数据文件
- 虚拟机软盘映像文件





实验报告格式与内容

- 实验报告包括：实验目的、实验要求、实验方案、实验过程和结果、实验总结等
- 实验目的和实验要求由老师提供实验项目文档中获取
- 实验方案包括相关基础原理、实验工具和环境、程序流程和算法思想、数据结构与程序模块功能说明，代码文档组成说明等
- 实验过程测试输入数据文件和输出数据文件
- 虚拟机软盘映像文件



实验报告格式与内容

- 【个人信息】院系/专业、年级/姓名
- 【实验题目】
- 【实验目的】
- 【实验要求】
- 【实验方案】包括：硬件或虚拟机配置方法、软件工具与作用、方案的思想、相关原理、程序流程、算法和数据结构、程序关键模块，结合代码与程序中的位置位置进行解释。**不得抄袭，否则按作弊处理。**
- 【实验过程】包括：主要工具安装使用过程及截图结果、程序过程中的操作步骤、测试数据、输入及输出说明、遇到的问题及解决情况、关键功能或操作的截图结果。**不得抄袭，否则按作弊处理。**
- 【实验总结】每人必需写一段，文字不少于**500**字，可以写心得体会、问题讨论与思考、新的设想、感言总结或提出建议等等。**不得抄袭，否则按作弊处理。**
- 【参考文献】（如有要列出，包括网上资源）



实验评价参考标准

项目 分	评	C	B-	B	B+	A-	A			A+			A++					A+++							
态度	未交	●																							
	抄袭	●																							
	极差	●																							
	雷同		●	●		●																			
质量 达标	部分		●																						
	基本			●																					
	全部			●	●	●	●				●				●	●	●				●	●	●	●	
	超额							●		●	●			●				●	●	●	●				
	提前								●	●			●		●										
实验 报告	粗糙																								
	简略							●	●																
	完整						●				●		●												
	详实											●		●	●				●	●	●	●	●	●	●
	功能																	●				●			
创新	方法															●				●		●	●		
	技术																			●			●	●	
	工具																●						●	●	
	环境																	●				●			●
教学 贡献	项目																								
	教程																								
	环境																								

上机考试

- 平时实验项目评价达到免考条件的同学可免机考，名单将在第**13**周开始分批公布，总评成绩不会低于**75**分。
- 机考**2**小时内在实验室专用环境进行。
- 题目**4~5**题，全部要求编程完成，提交完整程序文档和软盘映像文件。
- 题目考前公布，电脑、软件工具和环境可自带。



操作系统实验教学方法

■ 原型进化

- 从最小的操作系统原型开始，在相同的起跑线上出发
- 增量式扩展原型系统的功能，难度可控制，学习效果好
- 进化目标丰富，具有灵活的进化线路，允许多种组合，方便实验项目编制和教学过程控制
- 学生可以个性化选择发展方向，优秀学生可以充分施展自己的能力

■ 嵌入式开发

- 开发工作在熟悉的Windows/Linux/Mac OS/其它上进行，可以充分利用现有强大的计算机系统和丰富好用的软件工具
- 产生的操作系统原型放到虚拟机中运行，方便快捷安全，还可以调试，也不怕死机，因为死的是虚拟机。



操作系统实验工具与环境

■ 实验支撑环境

- 硬件：个人计算机
- 主机操作系统：Windows/Linux/Mac OS/其它
- 虚拟机软件：VMware/VirtualPC/Bochs/其它
 - PC虚拟机裸机/DOS虚拟机/其它

■ 实验开发工具

- 汇编语言工具：x86汇编语言
- 高级语言工具：标准C语言
- 磁盘映像文件浏览编辑工具
- 调试工具：Bochs



虚拟机软件

- 我们要开发30年前的PC上运行的操作系统原型。
 - 硬件：8086CPU/1M内存/1.44FDD/VGA/101键盘/
- 什么要虚拟PC机？
 - 实验室没有30年前的这种PC机了
 - 真有的话，在上面开发也不方便
 - 慢死了：开机5分钟，读写磁盘让人心烦
 - 开机关机多了，电脑易坏
 - 原型随时死机，而且没法调试
 - DOS不好用，软件工具缺乏，程序开发很不方便，不胜其烦
- 有虚拟机，真好而且都好用！
 - 各种操作系统上都有：Windows/Linux/Mac OS/其它
 - 虚拟机软件：VMware/VirtualPC/Bochs/其它，任君选择！
 - 嵌入式开发，开发工作在Windows/Linux/Mac OS/其它上进行，软件丰富好用
 - 原型放到虚拟机中运行，方便快捷安全



汇编程序工具与C语言工具

- 是最关键的工具与环境
- 怎么选择？
 - Obj:支持16位代码/32代码
 - 原型的执行代码格式:
 - 支持16位代码/32代码
 - BIN/COM/EXE/ELF
 - 有连接程序可连接汇编程序工具和C语言工具产生相同格式的obj文件
 - 16位代码确认函数调用/栈操作/返回/整数字节/变量命名规则兼容
- 常用组合
 - TCC+TASM: 实模式/16位代码/COM/EXE
 - GCC+NASM: 保护模式/32位代码BIN/ELF



TCC+TASM组合

- 特别适用：实模式/16位代码/COM
- 优点
 - 小巧，方便
 - 16位代码，恐龙绝种了。
 - 相容性较好
- 缺点：
 - 原型的执行代码格式只能COM或EXE格式
 - 不支持任意入口的BIN格式，因此制作不了引导扇区程序
 - 有Bug!C局部字符串变量初始化无效，已有补丁。

GCC+NASM组合

- 特别适用：保护模式/32位代码/BIN/ELF
- 优点
 - 小巧，方便
 - 32位代码，更通用、强大！
 - 相容性很好
 - 支持任意入口的BIN格式
- 缺点：
 - 16位代码支持有待全面检视，欢迎同学研究和尝试！
 - 汇编命令使用参数较多

裸机编程体验

- 场景：你面对一台尘封的**PC**机，单色显示器/没有硬盘/有一软驱/1M内存，通电，竟然还能工作，只是没有操作系统，屏幕停在一行英文提示信息处，敲打键盘没反应。
- 任务：随便你编写一个什么程序，只要它能执行就算你完成任务
- 没有真机，你虚拟一台吧！（操作）
- 编程什么程序？简单点，在屏幕什么地方显示一个'@'吧！



裸机编程体验

- 例1 在屏幕显示一个'@' （编辑操作）

```
mov ax,0xB800
```

```
mov es,ax
```

```
mov [es:0],'@'
```

```
mov [es:1],7
```

```
jmp $
```

你们也做一下！

- 裸机看不懂汇编语言程序，你想办法把汇编程序转换为机器语言程序吧！手工转换，肯定烦人。



裸机编程体验

- 算了，允许你用现在的电脑帮忙。（操作）
- 搞好了，机器语言程序如下框内：

1	00000000	B800B8
2	00000003	8EC0
3	00000005	26C606000040
4	0000000B	26C6060100F0
5	00000011	EBFE

```
mov ax,0xB800  
mov es,ax  
mov byte [es:00], '@'  
mov byte [es:01], 0F0h  
jmp $
```

- 有了机器语言程序，把它输入那旧电脑虚拟机中，才可以执行，怎么输入？是啊，现在敲什么它都没反应！



裸机编程体验

- 知不知电脑开机时会读磁盘，屏幕提示好象说请放进有系统的磁盘，虚拟机能读磁盘？

- 告诉你吧，能！而且能读虚拟的软盘！

- 虚拟的软盘是什么？怎么弄？（操作）
- 现在，你就把vFDD144这个文件当软盘吧！它与真盘容量一样。
- 现在还要搞清楚机器读软盘的什么位置，然后把程序放进这个位置才行！
 - 告诉你吧，机器开机自检后自动搜索磁盘是否存在，并读入首扇区，执行上面的程序。
- 那就把程序放到vFDD144这个文件的开头512字节这一区域，方法很多。（操作）
- 还要设置虚拟机把vFDD144这个文件当软盘用，然后开机试！（操作）
- 折腾！真折腾！总算看到了结果！



裸机编程体验

- 如果是真正裸机上完成这项工作，要几个小时才行！
- 裸机环境工作情况总结一下：
 - 机器代码编程或手工汇编，极困难费神。
 - 程序装入工作费时易错，机器利用率极低
 - 有错修改工作几乎推倒重来，从头开始！
 - 很难完成复杂的任务！
- 怎么办？这将引出我们一个学期的学习内容：**设计操作系统来解决这些问题。**



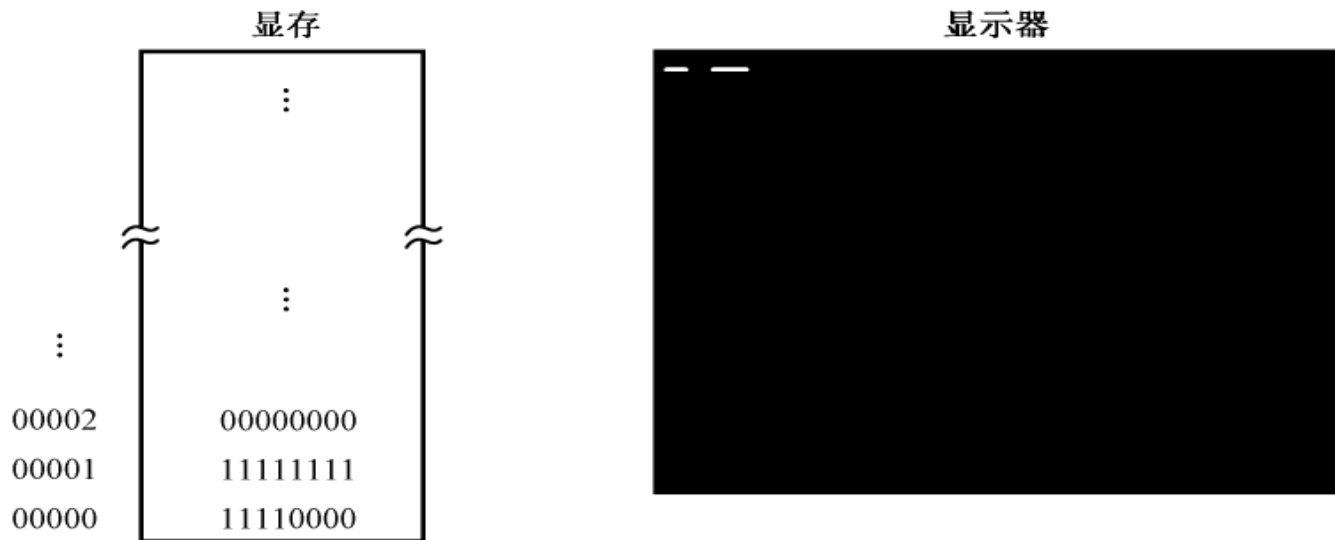
在屏幕上显示文字

■ 显示器

- 将那些内容以视觉可见的方式呈现在屏幕上。

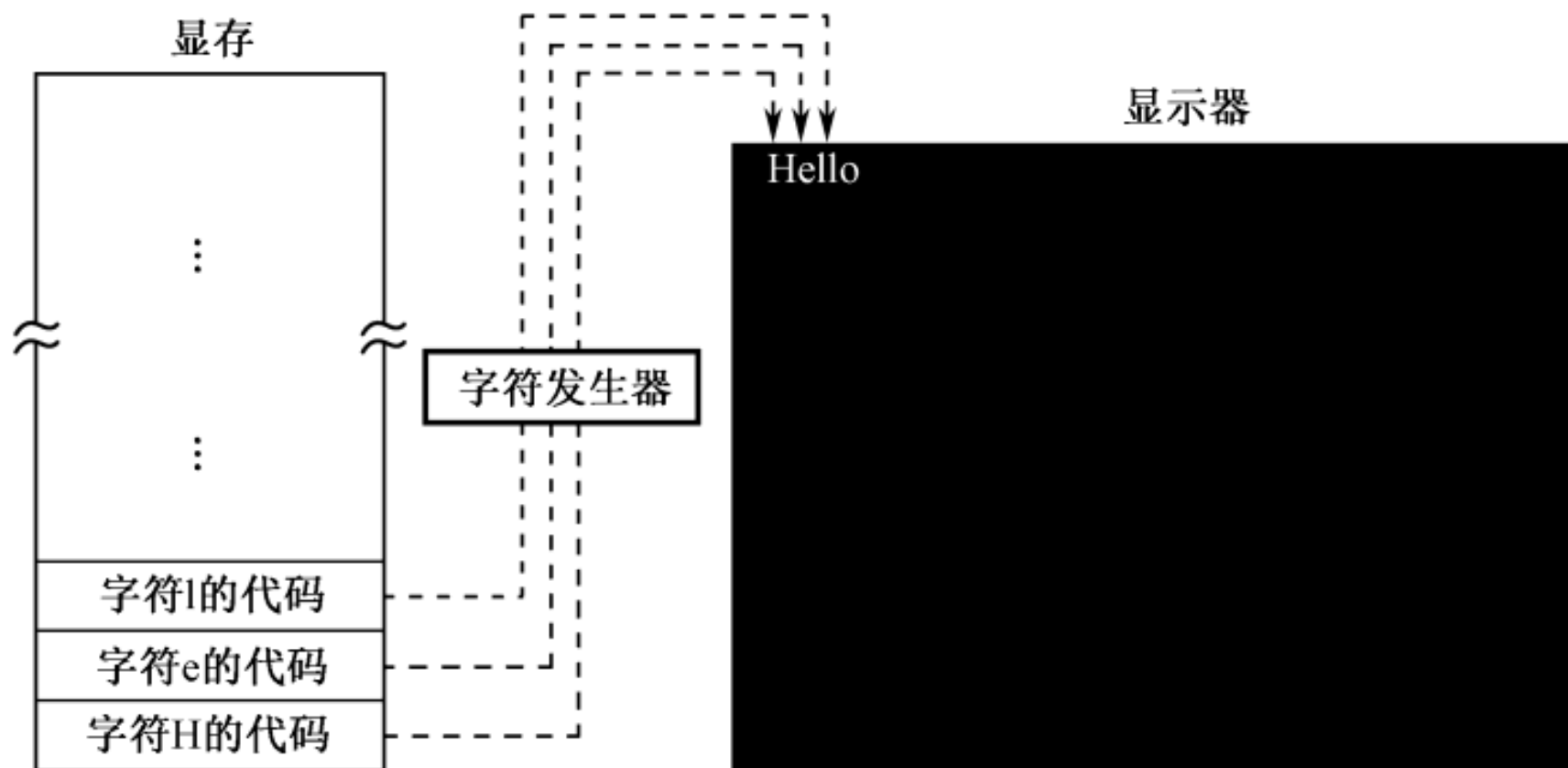
■ 显示卡

- 为显示器提供内容，并控制显示器的显示模式和状态
 - 图形方式：最小可控制单位为像素，VGA：640X400
 - 文本方式：最小可控制单位为字符，VGA：25X80
- 显示卡内存：存放像素或文字及相关属性



字符显示原理

- 字符发生器和控制电路
- 用代码来控制屏幕上的像素，使它们或明或暗以构成字符的轮廓

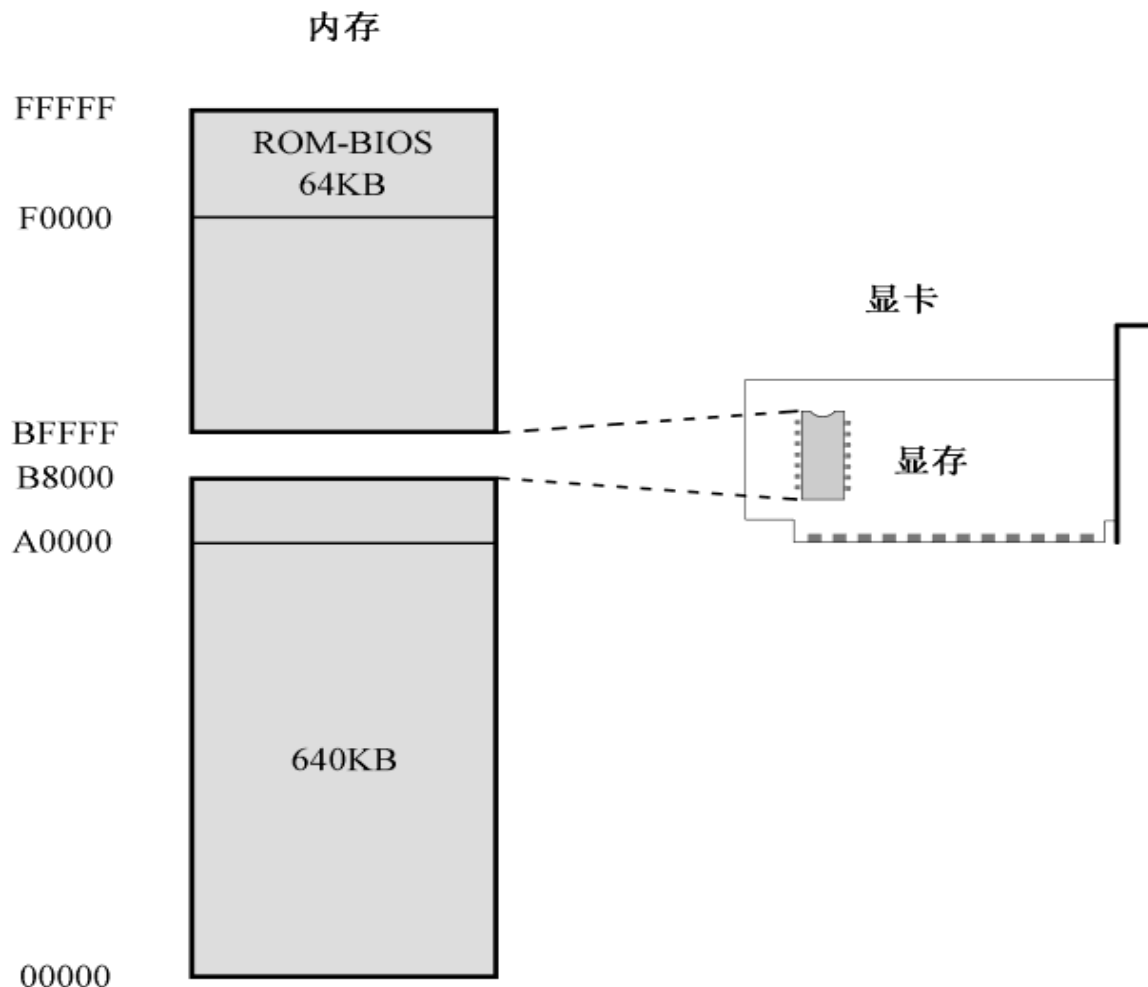


字符方式显存地址空间

■ 8086可访问的内在1MB

■ 地址空间

B8000~BFFFF
共32KB



初始化段寄存器

■ 访问显存使用逻辑地址

- 采用“段地址：偏移地址”的形式
- 显存段地址B800

■ 初始化段寄存器

```
mov ax,0xb800 ;ES指向文本模式的显示缓冲区
```

```
mov es,ax
```

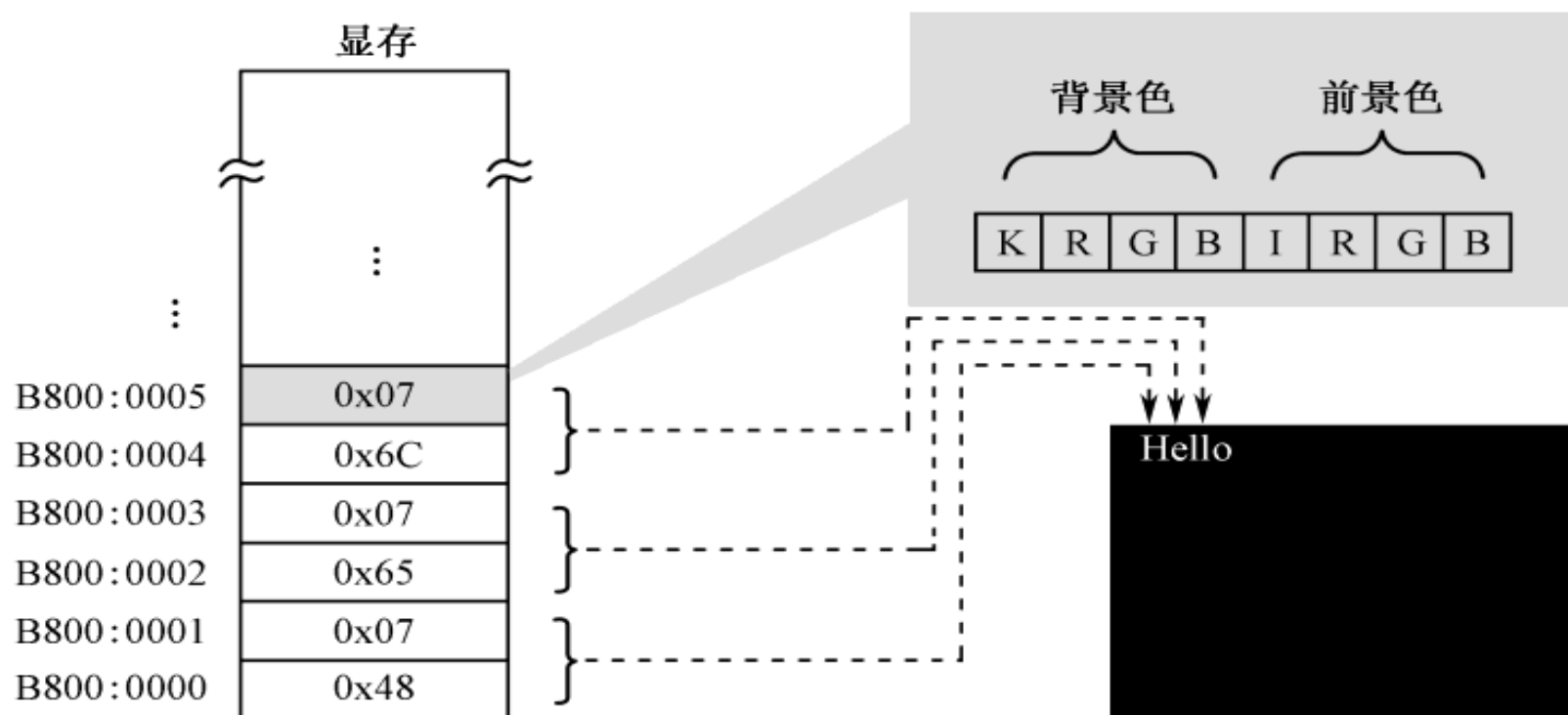
■ 规定

- 不能将立即数直接传送到段寄存器
- 防止误操作

```
mov es,0xb800 ;非法指令
```



显存与屏幕上字符的对应



屏幕上字符的显示属性

■ 字符属性0x07

- 解释为黑底白字，无闪烁，无加亮

R	G	B	背景色	前景色	
			K=0 时不闪烁，K=1 时闪烁	I=0	I=1
0	0	0	黑	黑	灰
0	0	1	蓝	蓝	浅蓝
0	1	0	绿	绿	浅绿
0	1	1	青	青	浅青
1	0	0	红	红	浅红
1	0	1	品（洋）红	品（洋）红	浅品（洋）红
1	1	0	棕	棕	黄
1	1	1	白	白	亮白

- 白底黑字，无闪烁，无加亮的属性是什么？
- 黑底红字，有闪烁，无加亮的属性是什么？
- 黑底白字，无闪烁，有加亮的属性是什么？



显示字符

- 把字符的**ASC**码和属性编码送到对应的显存中

```
mov byte [es:0x00], 'L'
```

```
mov byte [es:0x01], 0x07
```

- 或在屏幕中央显示一个 “@”

```
mov byte [es:(12X80+39)X2], '@'; 12行39列显示@
```

```
mov byte [es: (12X80+39)X2+1], 0x07
```

- 技巧：指令中的常量可于用表达式



实验项目1：接管裸机的控制权

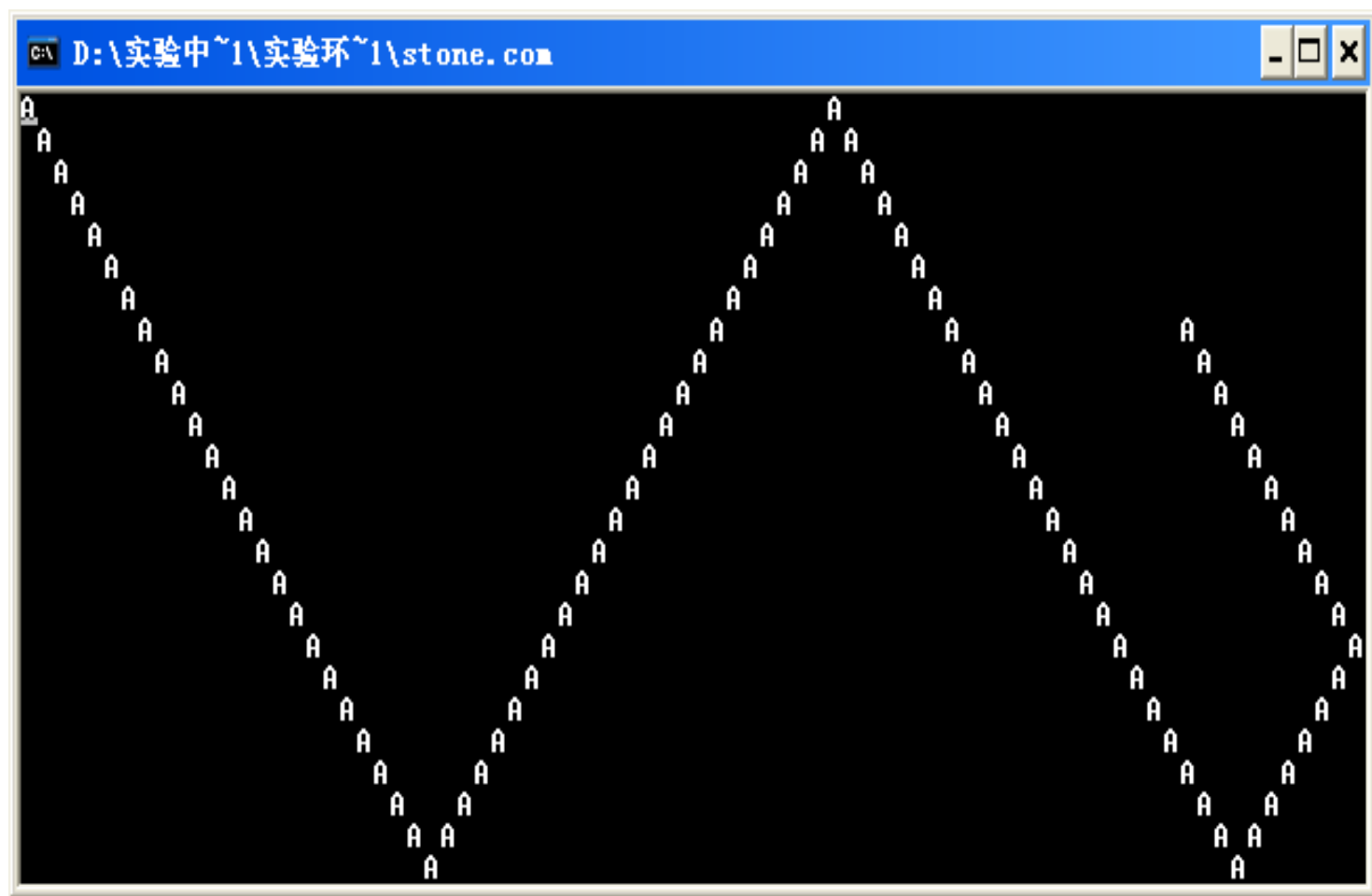
■ 搭建和应用实验环境

虚拟机安装，生成一个基本配置的虚拟机XXXPC和多个1.44MB容量的虚拟软盘，将其中一个虚拟软盘用DOS格式化为DOS引导盘，用WinHex工具将其中一个虚拟软盘的首扇区填满你的个人信息。

■ 接管裸机的控制权

设计IBM_PC的一个引导扇区程序，程序功能是：用字符‘A’从屏幕左边某行位置45度角下斜射出，保持一个可观察的适当速度直线运动，碰到屏幕的边后产生反射，改变方向运动，如此类推，不断运动；在此基础上，增加你的个性扩展，如同时控制两个运动的轨迹，或炫酷动态变色，个性画面，如此等等，自由不限。还要在屏幕某个区域特别的方式显示你的学号姓名等个人信息。将这个程序的机器码放进放进第三张虚拟软盘的首扇区，并用此软盘引导你的XXXPC，直到成功。





实验项目1参考程序

■ 参考程序stone.asm