高等院校实验课教材

信息系统安全与对抗技术实验教程

罗森林　高　平　编著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

信息系统安全与对抗技术
实 验 教 程

罗森林 高 平 编著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

图书在版编目(CIP)数据

信息系统安全与对抗技术实验教程/罗森林,高平编著. —北京:北京理工大学出版社,2005.1

ISBN 7-5640-0420-7

Ⅰ.信…　Ⅱ.①罗…②高…　Ⅲ.信息系统-安全技术-教材　Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2004)第 135745 号

出版发行/ 北京理工大学出版社
社　　址/ 北京市海淀区中关村南大街 5 号
邮　　编/ 100081
电　　话/ (010)68914775(办公室)　68944990(发行部)
网　　址/ http://www.bitpress.com.cn
电子邮箱/ chiefedit@bitpress.com.cn
经　　销/ 全国各地新华书店
印　　刷/ 北京圣瑞伦印刷厂
开　　本/ 787 毫米×1092 毫米　1/16
印　　张/ 17.5
字　　数/ 411 千字
版　　次/ 2005 年 1 月第 1 版　2005 年 1 月第 1 次印刷
印　　数/ 1~4000 册　　责任校对/ 陈玉梅
定　　价/ 27.00 元　　责任印制/ 李绍英

前　言

随着全球信息化进程的不断深入，信息技术的应用越来越广泛地渗透到社会发展的各个领域，在极大推动生产力发展的同时，人们对信息网络的依赖程度也日益提高，也因此使国家和社会面临着日益严重的信息安全威胁，国家政治、经济、文化、国防等各个领域面临非传统的安全挑战，国家安全和社会稳定受到新的安全威胁，并表现得更为尖锐复杂。信息安全对抗过程中，无论是从技术角度还是管理角度，人才是核心要素，因此，信息安全与对抗技术专业人才的培养尤为重要。

北京理工大学是国家教育部首批批准建立信息对抗技术专业的高校之一，其教学、科研、人才梯队的建设已初见成效，本书为针对本科生、研究生的教学实验教程，其实验设计充分考虑了“培养类”教学的特点，以便充分地发挥学生的主观能动性，培养学生的创新能力。本教学实验的主要内容涉及网络通信和数据的采集、传输、处理等基础性实验，计算机病毒实验、网络物理隔离实验、数据加密解密实验、数字水印和数字签名、无线网络安全实验、网络攻防综合性实验等典型技术性实验。同时针对不同的教学要求设计了基础型和提高型两类实验。实验安排建议：（1）将基础型实验学时数控制在每个实验 4 学时左右；（2）采用分组形式，每组人数控制在 2 至 3 人；（3）优秀学生应利用课余时间完成提高型实验；（4）利用多处形式（如小学期、教学实践等）安排综合性实验。

《信息系统与安全对抗导论》、《信息系统安全对抗理论与技术》以及《信息系统安全与对抗技术实验教程》三本教材，形成从理论到实验、由顶层至底层的互为延伸和贯通的信息对抗技术专业人材培养的系统性配套教材。

在本书的编写过程中，得到了王越院士、闫达远教授、李硕老师、苏京霞老师以及冯杨同学的多方面的帮助，在此一并表示衷心的感谢。同时，衷心感谢西安邮电学院范九伦教授对本书的认真评阅；衷心感谢北京理工大学出版社任世宏先生对本书的详细、认真的修改和热情帮助。最后，衷心感谢北京理工大学出版社多方面的支持和帮助。

本书的全部例程都经过认真的编制和调试，读者如果需要请与作者联系，电子邮件地址：bituosenlin@sina.com、gaoping@bit.edu.cn。

由于时间所限，加之笔者能力范围的限制，对于书中的不足和错误之处敬请广大师生批评指正，以便使其日臻完善。

作　者

2004 年 9 月于北京理工大学

目　录

第1章 绪 论

1.1 实验背景和目的

信息系统越发展到它的高级阶段，人们对其依赖性就越强，从某种程度上讲该信号系统就越容易遭受攻击，遭受攻击后的后果也就越严重。由于信息系统一般起着“催化剂”和“增强剂”的作用，其安全问题也是任何一个系统所不可忽视的问题。信息化进程在给人们带来诸多益处的同时，也给人们带来了新的安全问题，以网络环境为中心的信息系统的安全问题不同于传统意义上的安全，具有新的形式、特点。无论是信息安全管理方面，还是信息安全技术方面，人才是其中的核心要素，需要不同领域、不同层次的多方面人才，特别是高素质复合型人才尤为重要。因此，信息安全人才的培养势在必行。

北京理工大学是国家教育部首批批准建立信息对抗技术专业的学校。其学科、教学、科研、实验、人才梯队的建设已初建成效。根据“培养类”教学的需求，针对教材、实验等建设进行了全方位的规划，形成了战略性的学科建设框架，开设了独具特色的《信息系统与安全对抗导论》、《信息系统安全对抗理论与技术》等专业课程，同时开设面向全校学生的开放系列信息对抗技术专业实验，通过实践和不断的完善，教学与实验的配套形成了自己的特色。为了便于交流和使用，将北京理工大学信息对抗技术专业的系列实验合成一册，形成配套性实验教程。

1.2 实验的总体目标

教学实验是学生实践活动中的一个重要环节，信息安全问题是跨学科问题，是复杂问题之一，本教学实验根据“培养类”教学的要求，通过合理配置和开设系统性系列实验，结合专业基础和专业课程，使学生对专业知识具有更为深刻的理解和掌握。同时根据不同层次的学生将实验分为基础型和提高型两类，便于对不同能力学生的培养，提高型实验主要是培养学生的独立思维和创新能力。

1.3 实验的设计原则

根据信息安全与对抗的规律和特点，学生实验的设计遵循如下原则：

- 加强复合型、创新型、研究型人才的培养，充分发挥学生的主观能动性，给学生提供更多的自主学习、独立思考的空间。
- 实验教学不仅仅为某专门课程服务，要充分发挥学生的综合知识运用能力。

- 实现教学、实验、科研等多个环节的有机融合，科研与教学相统一，实验与课程相呼应。
- 注重系统性、基础性、理论与实践相结合能力的培养。培养学生系统思维能力，得到从底层具体设计到顶层系统分析能力多方面的训练。
- 注重实验的开放性和可持续发展。实验面向全校学生开放，同时根据发展不断完善和调整，紧跟信号安全技术的最新发展。
- 结合中国优秀传统，自主发展具有中国特色的信息安全与对抗体系。

1.4 实验的平台结构

信息安全与对抗的实验建立于信息系统模型的平台之上，图 1.1 所示为信息系统模型平台框图。该平台具有可扩展性，可随时加入新的信源、信道（理想与非理想），构成各类实验、仿真平台。该平台可以实现不同层次的信息安全与对抗技术实验。

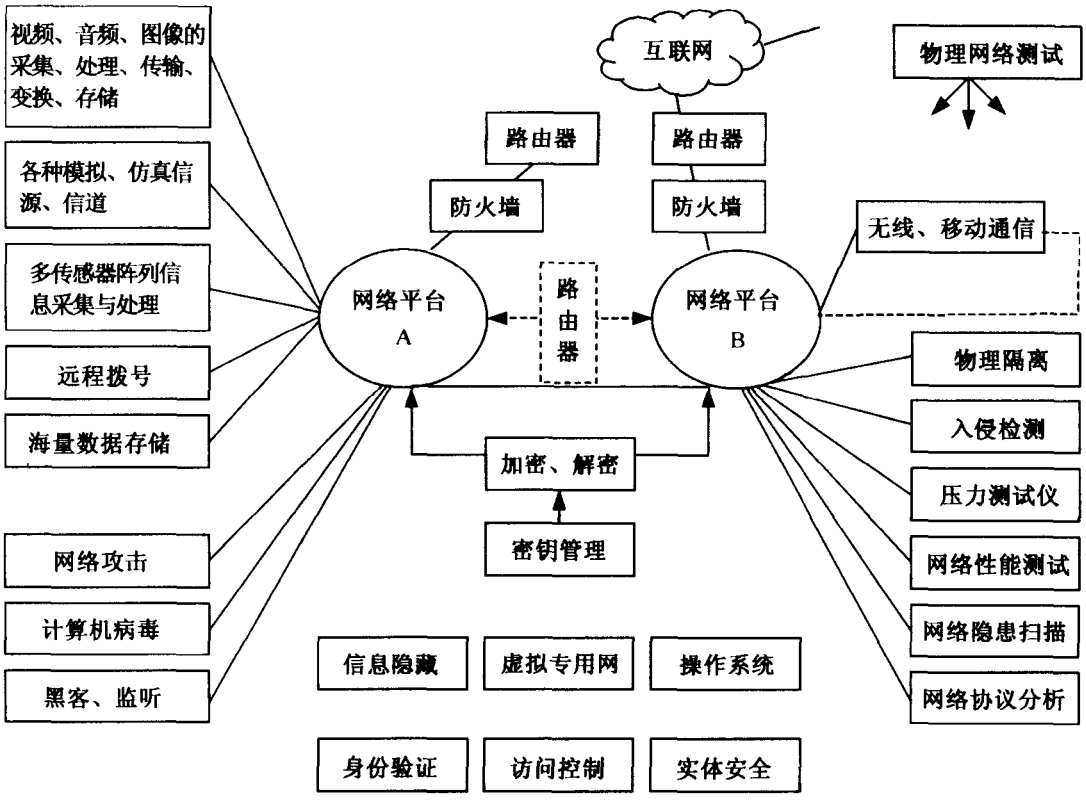

图 1.1 信息系统模型平台功能结构模型

1.5 实验的主要内容

本书针对信息安全与对抗相关理论与技术，面向本科生和研究生设计了七大类系列实验，分别对应于后面的各章，可根据不同情况选做其中部分实验。具体系列实验内容如下：

- 信息系统模型平台基础实验：基于物理链路层的通信实验；基于 TCP/IP 协议的通信实验；异构网络组建实验。
- 典型信息系统及其信息采集、传输、处理、交换、存储、管理与控制实验；语音数据采集、处理、传输、控制实验；图像数据采集、处理、传输、控制实验；网络流媒体的传输与控制实验。
- 信息系统病毒实验：文件型病毒分析与设计实验；宏病毒分析与设计实验；脚本病毒分析与设计实验。
- 信息系统安全物理隔离技术实验：信息网络的内、外网物理隔离。
- 信息隐藏技术实验：单密钥体制 DES 加解密算法实验；双密钥体制 RSA 加解密算法实验；图像数字水印实验。
- 信息系统攻防技术实验：网络信息收集与漏洞扫描实验；网络数据获取与分析实验；网络防火墙与入侵检测技术实验；网络攻击实验；网络防御实验；网络攻防综合实验系统设计与实验。
- 无线信息系统安全与对抗技术实验：无线网络建立与应用实验；无线网络安全与数字签名系统实验。

第 2 章　信息系统模型平台基础实验

2.1　引　　言

信息系统模型平台的基础实验主要涉及基于物理链路层，以及基于 TCP/IP 协议的网络数据通信，它是网络通信的基础，也是信息系统安全与对抗系列实验的基础。通过实验，让学生理解和掌握网络数据通信的基本概念、原理以及网络数据通信的程序设计、实现。

2.2　基于物理链路层的数据通信实验

一、实验目的

基于物理链路层的数据交换是网络通信的基础，实验中利用计算机的串行接口以三线制实现点到点的连接，设计用 C 语言或 8086 汇编语言实现计算机会话的基本通信程序。

二、实验所需条件和环境

硬件设备：局域网络、学生实验主机、符合 RS-232 标准的 DB-25 接头、通信导线若干和万用表。

系统软件：Windows 系列操作系统、DOS 6.22 操作系统。

实验环境配置如图 2.1 所示，通过串行接口，利用接收、发送、信号地三线制实现双机通信。

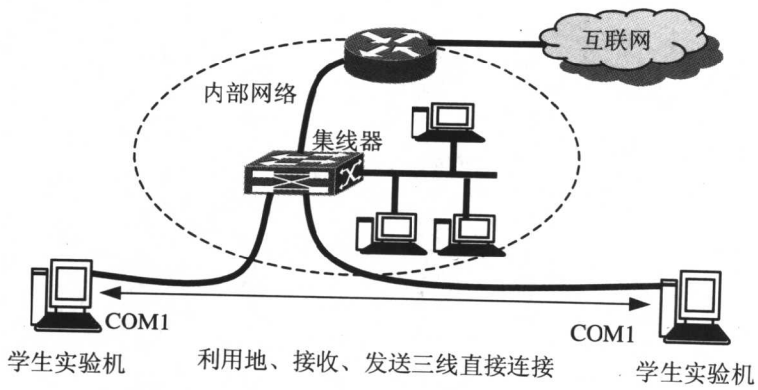

图 2.1　基于物理链路层的数据通信实验环境配置图

三、实验知识基础和方案

物理层（Physical Layer）是 OSI 参考模型的最底层，提供建立维护和拆除物理链路所需要的机械的、电气的、功能的接口。计算机遵循该接口定义，用物理介质相连实现面向比特（bit）流的数据传输。物理层采用的传输介质包括电缆、双绞线、光导纤维等。

为了使通信能顺利地进行，发送方和接收方都要共同遵守一些基本通信规则，即网络协议。在串行通信中，双方必须建立一致的概念和标准，包括：传输率、电气特性、信号名称和接口标准等。

（一）串行通信的方式

串行通信有三种连接方式：单工（Simplex）方式，半双工（Half-Duplex）和全双工（Full-Duplex）方式。

1. 单工方式

该方式仅允许数据按一个固定的方向传送。使用该方式时，必须已经确定了通信两端有一点为接收端，另一点为发送端，而且这种确定是不可逆转的。如图 2.2 所示，在参加通信的 A、B 两端中，A 只能为发送器，B 只能为接收器。

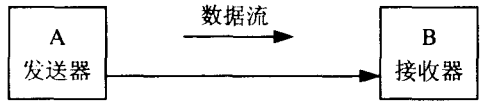

图 2.2　单工方式

2. 半双工方式

参加通信的两端均具备接收和发送数据的能力。由于 A、B 两端由一条信道相连，所以在某一特定时间内 A、B 两端传输方式是明确的，即 A 端发送时，B 端接收；反之，B 端发送时，A 端接收。绝不允许 A、B 两端同一时刻既发送又接收，如图 2.3 所示。

图 2.3　半双工方式

3. 全双工方式

全双工方式是由两条信道将 A、B 两端相连，A、B 两端可以实现同一时刻既发送又接收的功能，但要求 A、B 两端必须分别具备一套完全独立的接收器和发送器，如图 2.4 所示。

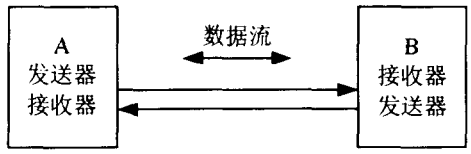

图 2.4　全双工方式

（二）微机串行通信接口

计算机系统一般配置两个异步串行通信端口，即 COM1 和 COM2，这些异步串行通信端口符合 RS-232 标准。

1. RS-232 接口标准

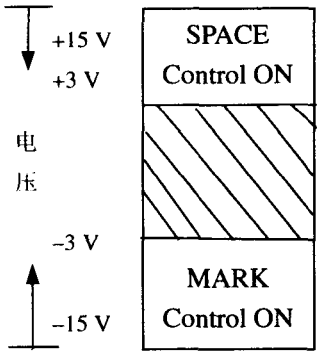

图 2.5 RS-232 的电平特性

EIA RS-232 是美国电子工业协会（EIA）公布的标准，用来实现数字信号与模拟信号之间的转换，即数据终端设备（DTE）与数据通信设备（DCE）进行串行二进制数据交换。

（1）机械特性

一般使用 25 针或 9 针连接器，根据 RS-232 标准规定设计。

（2）RS-232 电信号特性

为了保证能够正确地传输二进制数据以及控制设备能够正确地运行，RS-232 提供了数据信号和控制信号的电压范围以满足这种需要，如图 2.5 所示，+3 V～+15 V 表示正电压；-3 V～-15 V 表示负电压，在-3 V～+3 V 之间构成一个转换区域，但传输通常使用±12 V。

（3）RS-232 引脚分配

图 2.6 是符合 RS-232 标准的 DB-25 连接器的引脚分配示意图，引脚分为四组：地、数据、控制和定时。

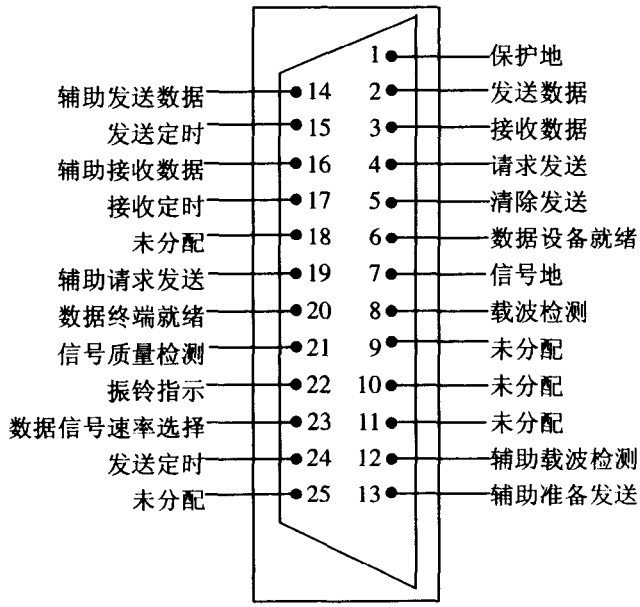

图 2.6 RS-232 引脚分配示意图

引脚功能说明如表 2.1 所示。

表 2.1　RS-232 标准引脚信号说明

引脚	含　义	引脚	含　义
1	PG：保护地	14	SBA：辅助发送数据
2	TD：发送数据	15	TC：发送定时
3	RD：接收数据	16	SBB：辅助接收数据
4	RTS：请求发送	17	RC：接收定时
5	CTS：清除发送	18	未分配
6	DSR：数据准备就绪	19	SCA：辅助请求发送
7	SG：信号地	20	DTR：数据终端就绪
8	CD：载波检测	21	CG：信号质量检测
9	未分配	22	CE：振铃指示
10	未分配	23	CH/CI：数据信号速率选择
11	未分配	24	DA：发送定时
12	SCF：辅助载波检测	25	未分配
13	SCB：辅助准备发送		

2. UART 概念

通用异步接收发送器 UART(Universal Asynchronous Receiver/Transimitter)主要由可编程集成通信芯片 Intel 8250、8251 组成，通过计算机标准配置 COM1 和 COM2 串行通信口进行异步串行通信，可以利用编程实现基于 RS-232 标准的异步串行通信设计，其特点如下：

- 传输速率可在 50～9 600 bps 的范围内选择；
- 可以分别控制发送、接收、传输线路状态和数据设备中断；
- 调制解调器控制功能。

UART 与外部设备的连接通过标准 RS-232 接口实现，采用标准 DB-25 或 DB-9 插头作为连接器，接口中 SIN、SOUT 是接受和发送信号线，RTS、DTR、DSR、CTS、RLSD（即 CD 信号）、CE 是外部设备控制信号线。

计算机与 UART 间的连接是由地址线、数据线、中断、读/写控制和复位控制线所构成，计算机数据线与 UART 数据线通过数据缓冲器来连接，该缓冲器由计算机 IOR/IOW 来控制，用于计算机和 UART 之间数据交换。地址线的使用是为了使 UART 在计算机 I/O 地址中占有一个位置。当计算机使用 UART 规定的 I/O 地址后，该 UART 就被选中。

由图 2.7 可以看出，8250 芯片将外部设备通过 RS-232 接口的串行数据接收进来并转换成并行的 8 位数据送往计算机，或者将计算机内的并行的 8 位数据转换成串行数据送往外部设备，在整个数据传输过程中，8250 检测数据传输状态，计算机随时读取 8250 状态信息或响应 8250 发出的中断请求，这样可以控制数据传输的过程和处理奇偶校验、溢出等。

同时，8250 还包含一个可编程波特率发生器，晶振频率可选 1.843 2 MHz 或 3.072 MHz，通过对其编程控制 UART 的传输速率。

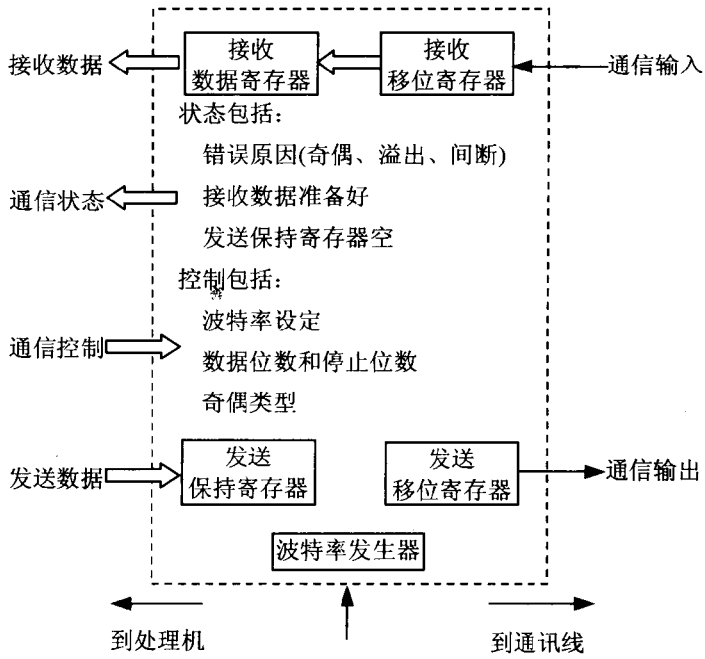

图 2.7 UART 功能框图

3. 8250 控制字说明

系统支持两个串行通信端口，COM1 使用的地址范围是 0x3F8H~0x3FEH，COM2 使用的地址范围是 0x2F8H～0x2FEH，均符合 RS-232 标准，每个通信端口各有 10 个可编程寄存器，需要通过相应的 I/O 地址访问。以 COM1 为例，寄存器的名称和地址列表如表 2.2 所示。

表 2.2 COM1 寄存器的名称与地址列表

地址	寄存器名称	备注说明
0x3F8	发送保持寄存器（THR）	DLAB=0
0x3F8	接收缓存寄存器（RBR）	DLAB=0
0x3F8	波特率因子寄存器［低］（DLL）	DLAB=1
0x3F9	波特率因子寄存器［高］（DLM）	DLAB=1
0x3F9	中断允许寄存器（IER）	DLAB=0
0x3FA	中断识别寄存器（IIR）	
0x3FB	线路控制寄存器（LCR）	
0x3FC	MODEM 控制寄存器（MCR）	*
0x3FD	线路状态寄存器（LSR）	
0x3FE	MODEM 状态寄存器（MSR）	*

注：因为 10 个寄存器要通过 7 个不同 I/O 地址进行访问，所以某些地址要重复使用，可通过 DLAB 位控制，对应线路控制寄存器（LCR）的最高位。5 个重复地址的寄存器在备注中表明 DLAB 的置位状态；此外，与 MODEM 相关的 MCR、MSR 的备注中“*”表示在本书程序中不起作用，不予考虑。

这里，规定每个寄存器的 8 位从高到低用 b7～b0 表示。

（1）线路控制寄存器（LCR，只写）

用来设置通信参数，初始化时必须设置，I/O 端口地址为 3FBh 或 2FBh。

b7：DLAB 位。置 0 为常态，置 1 访问 DLL、DLM 寄存器；

b6：中断控制位。置 0 禁止，置 1 允许；

b5、b4、b3：奇偶校验。具体设置及含义如下：

表 2.3　线路控制寄存器控制字

b5	b4	b3	含义
X	X	0	不校验
0	0	1	奇校验
0	1	1	偶校验

b2：停止位数。置 0 使用 1 位停止位，置 1 时，如果字符长度为 5，使用 1.5 停止位，如果字符长度为 6、7、8，使用 2 位停止位；

b1，b0：字符长度，具体设置及含义如下：

表 2.4　线路控制寄存器控制字

b1	b0	含义
0	0	5 位
0	1	6 位
1	0	7 位
1	1	8 位

（2）线路状态寄存器（LSR）

用于提供与线路有关的状态信息，使用中可随时查询，I/O 端口地址为 3FDh 或 2FDh。

b7：恒置 0；

b6：发送保持移位寄存器空（TSRE）；

b5：发送保持寄存器空（THRE），置 1 表示允许向 THR 输出数据；

b4：断点中断（BI）；

b3：帧（字符）格式错（FE）；

b2：奇偶校验错（PE）

b1：超载错误（OE）

b0：数据就绪（DR），置 1 表示 RBR 中有数据。

（3）波特率因子寄存器（DLL、DLM，只写）

两个寄存器组成一个 16 位寄存器，存放一个波特率因子（分频值）。对 1.843 2 MHz 频率进行分配，从而得到用户需要的波特率。DLL 存放波特率因子的低 8 位，DLM 存放波特率因子的高 8 位。I/O 端口地址为 3F8H/3F9H 或 2F8H/2F9H，典型的波特率因子值可以根据公式得到

波特率因子=1 843 200/（波特率×16）

例如，对于 4 800 的波特率：因子=1 843 200/(4 800×16)=24(18h)；于是 DLL 应设置为

0，DLM 应设置为 18h。

表 2.5 所示的波特率取值主要针对使用 8250 的 UART：

表 2.5 波特率设置

波特率	DLM	DLL
110	4h	17h
150	3h	0h
300	1h	80h
600	0h	c0h
1 200	0h	60h
2 400	0h	30h
4 800	0h	18h
9 600	0h	ch

（4）接收缓冲寄存器（RBR，只读）

用来存放从线路上接收的有效字符，等待本地读取，I/O 端口地址为 3F8h 或 2F8h。

（5）发送保持寄存器（THR）

用来存放待发送的数据，与 RBR 使用同一 I/O 地址，但互不干扰。

（6）中断允许寄存器（IER，只写）

用来设置哪些中断源可以产生中断，响应位置 0 禁止，置 1 允许。I/O 端口地址为 3F9h 或 2F9h。

b7 到 b4：恒置 0；

b3：MODEM 状态中断；

b2：线路状态中断；

b1：发送中断；

b0：接收中断。

（7）中断识别寄存器（IIR，只读）

用于提供与中断原因有关的信息，在中断服务例程中需要查询。I/O 端口地址为 3FAh 或 2FAh。

b7 到 b3：恒置 0；

b2、b1、b0：中断原因，组合及含义如表 2.6 所示。

表 2.6 中断类型

b2 b1 b0	中断类型	中断原因	复位动作
X X 1	无中断		
1 1 0	线路状态	线路状态变化	读 LSR
1 0 0	接收数据有效	RBR 中的输入字符有效	读 RBR
0 1 0	THR 空	THR 空（可发下个字符）	读 IIR 或写 THR
0 0 0	MODEM 状态	MODEM 状态变化	读 MSR

4. 连线方式

实现点到点的异步串行通信，需要利用串行接口将两台计算机直接连接起来，其中关键是将发送数据链路（TD）和接受数据链路（RD）交叉连接，其余连接要满足控制信号要求。图 2.8 和图 2.9 所示为 DB-25 或 DB-9 的几种连接方式。

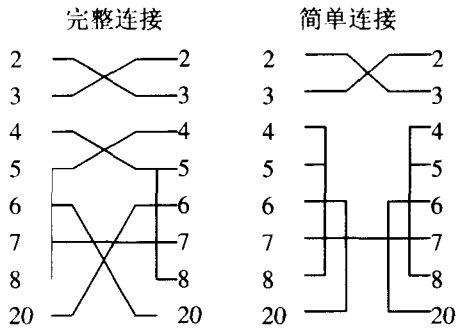

图 2.8　25 针—25 针连接线

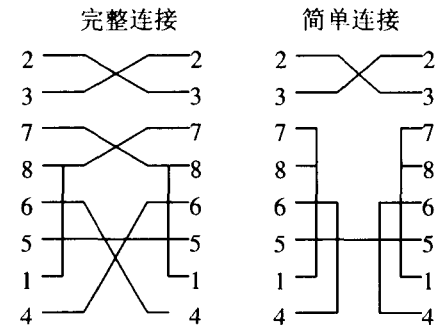

图 2.9　9 针—9 针连接线

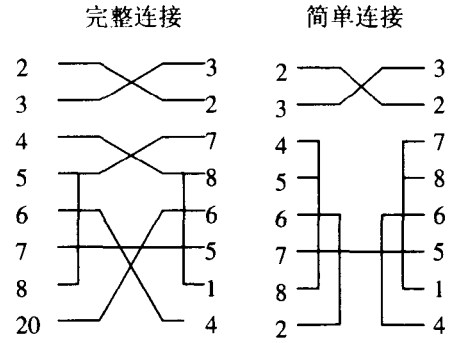

图 2.10　25 针—9 针连接线

实验时，由于不需要检测线路的状态，所以用 3 根导线就可以实现串行通信口相连，要求两台计算机的 DB-9 接口的第 3 号线（接收数据线）与第 2 号线（发送数据线）交叉连接，第 5 号信号地与另一台计算机的第 5 号信号地直接相连即可。

（三）RS-232 串行通信编程实例

利用 RS-232 进行异步通信编程时，首先要对使用的 8250 UART 进行初始化，设置一些必要的异步通信参数，包括速率、字符长度、停止位、奇偶校验方式等，所有这些参数的设置都是通过编程向相应地址的寄存器写入相应数值实现的。

1. 利用汇编语言实现串行通信

基于 8250 芯片实现异步串行通信一般有两种方式，一种是查询方式，另一种是中断方式，使用哪种方式取决于进行初始化时寄存器的设置。

查询方式需要不断查询、读取相应的寄存器，以判断是否应该发送或接收数据。如果