



普通高等教育“十一五”国家级规划教材
21世纪高职高专新概念教材

计算机网络安全技术

(第二版)

蔡立军 主 编
林亚平 龚理专 李立明 副主编



中国水利水电出版社
www.waterpub.com.cn



普通高等教育“十一五”国家级规划教材
21世纪中国计算机科学与技术系列教材

计算机网络安全技术

(第二版)

主 编 王 强 副主编 王 强 王 强
参 编 王 强 王 强 王 强



清华大学出版社
TSINGHUA UNIVERSITY PRESS

普通高等教育“十一五”国家级规划教材

21 世纪高职高专新概念教材

计算机网络安全技术

（第二版）

蔡立军 主 编

林亚平 龚理专 李立明 副主编

中国水利水电出版社

内 容 提 要

本书被评为“普通高等教育‘十一五’国家级规划教材”，是对第一版内容进行更新后的第二版。

本书详细介绍了计算机网络安全技术的基础理论、原理及其实现方法，概念、理论和实施技术并存。本书分为四篇 10 章，包括安全技术基础（安全模型、安全体系结构、安全服务与安全机制、安全的三个层次、评估标准）、实体安全防护与安全管理技术（场地环境的安全防护、电磁干扰及电磁防护、物理隔离、安全管理）、网络安全技术（防火墙技术、攻击检测与系统恢复技术、访问控制技术、网络存储备份技术、病毒防治技术）、信息安全技术（数据库安全技术、密码技术与压缩技术、认证技术）等内容。本书涵盖了计算机网络安全需要的“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

本书具有教材和技术资料的双重特征，既可以作为高职高专的计算机、网络安全、信息安全、通信等专业的教材使用，也可作为计算机网络安全的培训、自学教材；同时也可作为网络工程技术人员、网络管理员、信息安全管理的技术参考书。

本书配有免费电子教案，读者可从中国水利水电出版社网站（<http://www.waterpub.com.cn/softdown/>）下载。

图书在版编目（CIP）数据

计算机网络安全技术 / 蔡立军主编. —2 版. —北京：中国水利水电出版社，2007

普通高等教育“十一五”国家级规划教材. 21 世纪高职高专新概念教材

ISBN 978-7-5084-4692-9

I. 计… II. 蔡… III. 计算机网络—高等学校：技术学校—教材 IV. TP393

中国版本图书馆 CIP 数据核字（2007）第 102349 号

书 名	计算机网络安全技术（第二版）
作 者	蔡立军 主 编 林亚平 龚理专 李立明 副主编
出版 发行	中国水利水电出版社（北京市三里河路 6 号 100044） 网址：www.waterpub.com.cn E-mail: mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经 售	全国各地新华书店和相关出版物销售网点
排 版	北京万水电子信息有限公司
印 刷	北京蓝空印刷厂
规 格	787mm×1092mm 16 开本 18 印张 434 千字
版 次	2002 年 1 月第 1 版 2007 年 7 月第 2 版 2007 年 7 月第 7 次印刷
印 数	28001—33000 册
定 价	26.00 元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

版权所有·侵权必究

21 世纪高职高专新概念教材

编委会名单

主任委员 刘 晓 柳菊兴

副主任委员 胡国铭 张栢勤 王前新 黄元山 柴 野

张建钢 陈志强 宋 红 汤鑫华 王国仪

委 员 (按姓氏笔划排序)

马洪娟	马新荣	尹朝庆	方 宁	方 鹏
毛芳烈	王 祥	王乃钊	王希辰	王国思
王明晶	王泽生	王绍卜	王春红	王路群
东小峰	台 方	叶永华	宁书林	田 原
田绍槐	申 会	刘 猛	刘尔宁	刘慎熊
孙明魁	安志远	许学东	闫 菲	何 超
宋锦河	张 晞	张 慧	张弘强	张怀中
张晓辉	张浩军	张海春	张曙光	李 琦
李存斌	李作纬	李珍香	李家瑞	李晓桓
杨永生	杨庆德	杨名权	杨均青	汪振国
沈祥玖	肖晓丽	闵华清	陈 川	陈 炜
陈语林	陈道义	单永磊	周杨姊	周学毛
武铁敦	郑有想	侯怀昌	胡大鹏	胡国良
费名瑜	赵 敬	赵作斌	赵秀珍	赵海廷
唐伟奇	夏春华	徐 红	徐凯声	徐雅娜
殷均平	袁晓州	袁晓红	钱同惠	钱新恩
郭振民	曹季俊	梁建武	蒋金丹	蒋厚亮
覃晓康	谢兆鸿	韩春光	詹慧尊	雷运发
廖哲智	廖家平	管学理	蔡立军	黎能武
魏 雄				

项目总策划 雨 轩

编委会办公室 主 任 周金辉

副主任 孙春亮 杨庆川

参编学校名单

(按第一个字笔划排序)

三门峡职业技术学院

三联职业技术学院

山东大学

山东交通学院

山东建工学院

山东省电子工业学校

山东农业大学

山东省农业管理干部学院

山东省教育学院

山东商业职业技术学院

山西运城学院

山西经济管理干部学院

万博科技职业学院

广东金融学院

广东科贸职业学院

广州市职工大学

广州城市职业技术学院

广州铁路职业技术学院

广州康大职业技术学院

中山火炬职业技术学院

中华女子学院山东分院

中国人民解放军第二炮兵学院

中国人民解放军军事经济学院

中国矿业大学

中南大学

天津职业技术师范学院

太原理工大学阳泉学院

太原城市职业技术学院

长沙大学

长沙民政职业技术学院

长沙交通学院

长沙航空职业技术学院

长春汽车工业高等专科学校

内蒙古工业大学职业技术学院

内蒙古民族高等专科学校

内蒙古警察职业学院

兰州资源环境职业技术学院

北京对外经济贸易大学

北京科技大学职业技术学院

北京科技大学成人教育学院

北华航天工业学院

四川托普职业技术学院

包头轻工职业技术学院

宁波城市职业技术学院

石家庄学院

辽宁交通高等专科学校

辽宁经济职业技术学院

安徽交通职业技术学院

安徽水利水电职业技术学院

华中科技大学

华东交通大学

华北电力大学

江汉大学

江西大宇职业技术学院

江西工业职业技术学院

江西城市职业学院

江西渝州电子工业学院

江西服装职业技术学院

江西赣西学院

西北大学软件职业技术学院

西安外事学院

西安欧亚学院

西安铁路职业技术学院

西安文理学院

扬州江海职业技术学院

杨陵职业技术学院

昆明冶金高等专科学校
武汉大学
武汉工业学院
武汉工程职业技术学院
武汉广播电视大学
武汉工程大学
武汉电力职业技术学院
武汉科技大学工贸学院
武汉科技大学外语外事职业学院
武汉软件职业学院
武汉商业服务学院
武汉铁路职业技术学院
河南济源职业技术学院
中原工学院
南昌工程学院
南昌大学共青学院
哈尔滨金融专科学校
重庆正大软件职业技术学院
重庆工业职业技术学院
济南大学
济南交通高等专科学校
济南铁道职业技术学院
荆门职业技术学院
贵州无线电工业学校
贵州电子信息职业技术学院
浙江水利水电高等专科学校
浙江工业职业技术学院
浙江国际海运职业技术学院

恩施职业技术学院
黄冈职业技术学院
黄石理工学院
湖北工业大学
湖北交通职业技术学院
湖北汽车工业学院
湖北长江职业学院
湖北药检高等专科学校
湖北经济学院
湖北教育学院
湖北职业技术学院
湖北鄂州大学
湖北水利水电职业技术学院
湖南大学
湖南工业职业技术学院
湖南大众传媒职业技术学院
湖南工学院
湖南涉外经济学院
湖南郴州职业技术学院
湖南商学院
湖南税务高等专科学校
湖南信息科学职业学院
蓝天学院
福建林业职业技术学院
福建水利电力职业技术学院
黑龙江农业工程职业学院
黑龙江司法警官职业学院

序

根据 1999 年 8 月教育部高教司制定的《高职高专教育基础课程教学基本要求》(以下简称《基本要求》)和《高职高专教育专业人才培养目标及规格》(以下简称《培养规格》)的精神,由中国水利水电出版社北京万水电子信息有限公司精心策划,聘请我国长期从事高职高专教学、有丰富教学经验的教师执笔,在充分汲取了高职高专和成人高等学校在探索培养技术应用性人才方面取得的成功经验和教学成果的基础上,撰写了这套《21 世纪高职高专新概念教材》。

为了编写本套教材,出版社进行了广泛的调研,走访了全国百余所具有代表性的高等专科学校、高等职业技术学院、成人教育高等院校以及本科院校举办的二级职业技术学院,在广泛了解情况、探讨课程设置、研究课程体系的基础上,经过学校申报、征求意见、专家评选等方式,确定了本套书的主编,并成立了编委会。每本书的编委会聘请了多所学校主要学术带头人或主要从事该课程教学的骨干,教学大纲的确定以及教材风格的定位均经过编委会多次认真讨论。

本套《21 世纪高职高专新概念教材》有如下特点:

(1) 面向 21 世纪人才培养的需求,结合高职高专学生的培养特点,具有鲜明的高职高专特色。本套教材的作者都是长期在第一线从事高职高专教育的骨干教师,对学生的基本情况、特点和认识规律等有深入的了解,在教学实践中积累了丰富的经验。因此可以说,每一本书都是教师们长期教学经验的总结。

(2) 以《基本要求》和《培养规格》为编写依据,内容全面,结构合理,文字简练,实用性强。在编写过程中,作者严格依据教育部提出的高职高专教育“以应用为目的,以必需、够用为度”的原则,力求从实际应用的需要(实例)出发,尽量减少枯燥、实用性不强的理论概念,加强了应用性和实际操作性强的内容。

(3) 采用“问题(任务)驱动”的编写方式,引入案例教学和启发式教学方法,便于激发学习兴趣。本套书的编写思路与传统教材的编写思路不同:先提出问题;然后介绍解决问题的方法,最后归纳总结出一般规律或概念。我们把这个新的编写原则比喻成“一棵大树、问题驱动”的原则。即:一方面遵守先见(构建)“树”(每本书就是一棵大树),再见(构建)“枝”(书的每一章就是大树的一个分枝),最后见(构建)“叶”(每章中的若干小节及知识点)的编写原则;另一方面采用问题驱动方式,每一章都尽量用实际中的典型实例开头(提出问题、明确目标),然后逐渐展开(分析解决问题),在讲述实例的过程中将本章的知识点融入。这种精选实例,并将知识点融于实例中的编写方式,可读性、可操作性强,非常适合高职高专的学生阅读和使用。本书读者通过学习构建本书中的“树”,由“树”找“枝”,顺“枝”摸“叶”,最后达到构建自己所需要的“树”的目的。

(4) 部分教材配有实验指导和实训教程,便于学生练习提高。

(5) 部分教材配有动感电子教案。为顺应教育部提出的教材多元化、多媒体化发展的要求,大部分教材都配有电子教案,以满足广大教师进行多媒体教学的需要。电子教案用 PowerPoint 制作,教师可根据授课情况任意修改。相关教案的具体情况请到中国水利水电出版社网站 www.waterpub.com.cn 下载。

(6) 提供相关教材中所有程序的源代码,方便教师直接切换到系统环境中教学,提高教学效果。

总之,本套教材凝聚了数百名高职高专一线教师多年的教学经验和智慧,内容新颖,结构完整,概念清晰,深入浅出,通俗易懂,可读性、可操作性和实用性强。

本套教材适用于高等职业学校、高等专科学校、成人及本科院校举办的二级职业技术学院和民办高校。

新世纪吹响了我国高职高专教育蓬勃发展的号角,新世纪对高职教育提出了新的要求,高职教育占据了全面素质教育中所不可缺少的地位,在我国高等教育事业中占有极其重要的位置,在我国社会主义现代化建设事业中发挥着日趋显著的作用,是培养新世纪人才所不可缺少的力量。相信本套《21 世纪高职高专新概念教材》的出版能为高职高专的教材建设和教学改革略尽绵薄之力,因为我们提供的不仅是一套教材,更是自始至终的教育支持,无论是学校、机构培训还是个人自学,都会从中得到极大的收获。

当然,本套教材肯定会有不足之处,恳请专家和读者批评指正。

21 世纪高职高专新概念教材编委会

2001 年 3 月

第二版前言

计算机网络安全问题是各国、各部门、各行业以及每个计算机用户都十分关注的重要问题。为了提高我国各级计算机网络主管部门的安全意识,普及计算机网络安全知识,提高国内计算机从业人员的安全技术水平,有效地保护我国计算机网络的安全,对高职高专计算机专业及相近专业和本科计算机相近专业学生开设计算机网络安全技术课程十分必要,也很迫切。

本书承蒙各位读者的厚爱,多次重印。但计算机网络安全技术发展较快,第一版中有些软件版本、技术、实例都已落伍,已跟不上技术发展的需要。因此,作者综合了任课教师、学生及相关工程技术人员、部分读者的反馈意见,对原有内容和编排进行了较大调整,删除了陈旧的知识,增添了一些新的内容,如安全模型、Oracle 数据库的安全管理、物理隔离技术、攻击检测与系统恢复技术、访问控制技术、认证技术等,形成了第二版。

本书内容全面、系统,涵盖了计算机网络安全需要的“攻、防、测、控、管、评”等多方面的基础理论和实施技术。本书由四篇 10 章组成:

第一篇是安全技术基础(第 1 章),包括安全模型、网络安全体系结构框架、安全服务和安全机制、计算机网络安全的三个层次、安全技术评估标准等内容。

第二篇是实体安全防护与安全管理技术(第 2 章),包括计算机房场地环境的安全要求、电磁干扰及电磁防护、物理隔离技术、安全管理(网络管理结构模型、SNMP/CMIP 协议、安全管理的基本原则与工作规范)等内容。

第三篇是网络安全技术,重点介绍了防火墙技术(第 3 章)、攻击检测与系统恢复技术(第 4 章)、访问控制技术(第 5 章)、网络存储备份技术(第 6 章)、病毒防治技术(第 7 章)。

第四篇是信息安全技术,详细讲解了数据库安全技术(第 8 章)、密码技术与压缩技术(第 9 章)、认证技术(第 10 章)等内容。

本书具有教材和技术资料的双重特征,既可以作为高职高专的计算机、网络安全、信息安全、通信等专业的教材使用,也可作为计算机网络安全的培训、自学教材;同时也可作为网络工程技术人员、网络管理员、信息安全管理的技术参考书。

本书由蔡立军任主编,林亚平、龚理专、李立明任副主编。参加本书大纲讨论与编写工作的还有杜四春、银红霞、凌民、蔡益红、何英、池鹏、蒋正文、柳志刚、王展辉、雷衍凤、陈燕、刘红飞等做了本书的文字录入和图表制作工作,在此一一表示感谢。

由于作者水平有限,书中的错误和缺点在所难免,欢迎广大读者批评指正。

编者

2007 年 4 月

第一版前言

计算机网络安全问题是各国、各部门、各行业以及每个计算机用户都十分关注的重要问题。随着 Internet 与 Intranet 的普及和广泛应用,计算机技术和网络技术已深入到社会的各个领域,人类对计算机、对网络的依赖程度越来越大。计算机网络安全问题也变得越来越重要,成为了维护国家和社会稳定的一个焦点。为了提高我国各级计算机网络主管部门的安全意识,普及计算机网络安全知识,提高国内的安全技术水平,有效地保护我国计算机网络安全,对高职高专计算机专业及相近专业和本科计算机相近专业学生开设计算机网络安全技术课程十分必要,也很迫切。这门课程是计算机网络课程的延伸,涉及到的问题也正是广大网络工程技术人员极为关心的、亟待解决的问题。

本书从工程应用角度出发,立足于“看得懂、学得会、用得上”,方法与技术并重,深入浅出、循序渐进。全书共 10 章,主要内容有:计算机网络安全技术概论(第一章);实体安全与硬件防护技术(第二章);软件系统安全(第三章);网络安全防护技术(第四章);数据信息安全,包括备份技术、密码技术与压缩技术、数据库安全等(第五、六、七章);病毒防治技术(第八章);网络站点安全,包括防火墙技术、系统平台的安全、Web 站点安全、防黑客技术(第九、十章)。每章都有典型案例。全书涵盖了计算机网络安全需要的“攻、防、测、控、管、评”等多方面的基础理论和实施技术。

作为面向 21 世纪的高职高专新概念教材,本书选题适当,以必需、够用为度,讲清概念、结合实际、强化训练,突出适应性、实用性和针对性,有利于学生学以致用,解决实际工作中所遇到的问题,是一本计算机网络安全和安全管理维护的实用教材。

本书具有教材和技术资料的双重特征,既可以作为高职高专计算机专业及相近专业和本科计算机相近专业教材,也适合作为计算机网络安全培训、自学教材,同时也是网络管理员、信息安全管理人員和网络工程技术人员的技术参考资料。

本书配有电子教案(用 PowerPoint 制作,可以任意修改),使用本教材的学校可以与中国水利水电出版社联系。

本书由蔡立军主编,李立明、李峰任副主编。参加本书大纲讨论与部分编写工作的还有雷建军、舒望皎、杜红兵等。刘红飞、凌红武、邓玉华、陈霞、陈知、余俊良、李中发、罗俊、周志芳、唐美玲、张宝红、蔡辉、黄生群等做了本书的文字录入和图表制作工作。在此一一表示感谢。

由于作者水平有限,书中的错误和缺点在所难免,欢迎广大读者批评指正。

编者

2001 年 8 月

目 录

序

第二版前言

第一版前言

第一篇 安全技术基础

第1章 计算机网络安全技术概论	1
本章学习目标	1
1.1 计算机网络安全系统的脆弱性	1
1.2 安全模型	3
1.2.1 P ² DR 安全模型	3
1.2.2 PDRR 网络安全模型	5
1.3 网络安全体系结构	5
1.3.1 开放式系统互联参考模型 (OSI/RM)	5
1.3.2 Internet 网络体系层次结构	6
1.3.3 网络安全体系结构框架	7
1.4 安全服务与安全机制	9
1.4.1 安全服务的基本类型	9
1.4.2 支持安全服务的基本机制	10
1.4.3 安全服务和安全机制的关系	11
1.4.4 安全服务与网络层次的关系	11
1.5 计算机网络安全的三个层次	14
1.5.1 安全立法	14
1.5.2 安全技术	16
1.5.3 安全管理	19
1.6 安全技术评估标准	19
1.6.1 可信计算机系统评估标准	19
1.6.2 信息系统评估通用准则	22
1.6.3 安全评估的国内通用准则	23
习题一	25

第二篇 实体安全防护与安全管理技术

第2章 实体安全防护与安全管理技术	27
本章学习目标	27

2.1	物理安全技术概述	27
2.2	计算机机房场地环境的安全防护	28
2.2.1	计算机机房场地的安全要求	28
2.2.2	设备防盗措施	28
2.2.3	机房的三度要求	29
2.2.4	防静电措施	30
2.2.5	电源	30
2.2.6	接地与防雷	31
2.2.7	计算机场地的防火、防水措施	34
2.3	电磁防护	35
2.3.1	电磁干扰	36
2.3.2	电磁防护的措施	38
2.4	物理隔离技术	43
2.4.1	物理隔离的安全要求	43
2.4.2	物理隔离技术的发展历程	43
2.4.3	物理隔离的性能要求	46
2.5	安全管理	47
2.5.1	安全管理概述	47
2.5.2	计算机网络管理系统的逻辑结构模型	50
2.5.3	安全管理协议——SNMP 和 CMIP	53
2.5.4	安全管理的制度与规范	56
	习题二	62

第三篇 网络安全技术

第3章	防火墙技术	63
	本章学习目标	63
3.1	防火墙技术概述	63
3.1.1	防火墙的定义	63
3.1.2	防火墙的发展简史	64
3.1.3	设置防火墙的目的与功能	64
3.1.4	防火墙的局限性	66
3.1.5	防火墙技术发展动态和趋势	66
3.2	防火墙技术	68
3.2.1	防火墙技术的分类	68
3.2.2	防火墙的主要技术及实现方式	75
3.2.3	防火墙的常见体系结构	79
3.3	防火墙的主要性能指标	81

3.4 分布式防火墙	83
3.4.1 分布式防火墙的体系结构	83
3.4.2 分布式防火墙的特点	84
3.5 Windows 2000 环境下防火墙及 NAT 的实现	86
习题三	90
第 4 章 攻击检测与系统恢复技术	91
本章学习目标	91
4.1 网络攻击技术	91
4.1.1 网络攻击概述	91
4.1.2 网络攻击的原理	93
4.1.3 网络攻击的步骤	97
4.1.4 黑客攻击实例	101
4.1.5 网络攻击的防范措施及处理对策	103
4.1.6 网络攻击技术的发展趋势	105
4.2 入侵检测系统	106
4.2.1 入侵检测系统概述	106
4.2.2 入侵检测系统的数学模型	108
4.2.3 入侵检测的过程	110
4.2.4 入侵检测系统的分类	113
4.3 系统恢复技术	118
4.3.1 系统恢复和信息恢复	118
4.3.2 系统恢复的过程	118
习题四	123
第 5 章 访问控制技术	124
本章学习目标	124
5.1 访问控制概述	124
5.1.1 访问控制的定义	124
5.1.2 访问控制矩阵	126
5.1.3 访问控制的内容	126
5.2 访问控制模型	126
5.2.1 自主访问控制模型	127
5.2.2 强制访问控制模型	128
5.2.3 基于角色的访问控制模型	129
5.2.4 其他访问控制模型	130
5.3 访问控制的安全策略与安全级别	131
5.3.1 安全策略	131
5.3.2 安全级别	132

5.4 安全审计	133
5.4.1 安全审计概述	133
5.4.2 日志的审计	134
5.4.3 安全审计的实施	136
5.5 Windows NT 中的访问控制与安全审计	138
5.5.1 Windows NT 中的访问控制	138
5.5.2 Windows NT 中的安全审计	139
习题五	141
第 6 章 网络存储备份技术	142
本章学习目标	142
6.1 网络存储技术	142
6.1.1 网络存储技术概述	142
6.1.2 RAID 存储技术	142
6.1.3 DAS 存储技术	146
6.1.4 SAN 存储技术	148
6.1.5 NAS 存储技术	149
6.1.6 存储技术的比较	152
6.2 网络备份技术	154
6.2.1 网络备份技术概述	154
6.2.2 主要存储备份介质	157
6.2.3 网络存储备份软件	160
6.3 常用网络系统备份方案	161
6.3.1 备份硬件和备份软件的选择	162
6.3.2 系统备份方案的设计	163
6.3.3 日常备份制度设计	164
6.3.4 灾难恢复措施设计	166
6.4 基于 CA ARC Serve 的典型备份案例	167
习题六	168
第 7 章 计算机病毒防治技术	169
本章学习目标	169
7.1 计算机病毒概述	169
7.1.1 计算机病毒的定义	169
7.1.2 病毒的发展历史	169
7.1.3 病毒的分类	171
7.1.4 病毒的特点和特征	172
7.1.5 病毒的运行机制	174
7.2 网络计算机病毒	177

7.2.1	网络计算机病毒的特点	177
7.2.2	网络对病毒的敏感性	178
7.3	反病毒技术	180
7.3.1	反病毒涉及的主要技术	180
7.3.2	病毒的检测	180
7.3.3	病毒的防治	182
7.4	软件防病毒技术	186
7.4.1	防病毒软件的选择	186
7.4.2	防病毒软件工作原理	188
7.4.3	构筑防病毒体系的基本原则	190
7.4.4	金山毒霸网络版中小企业网络防病毒解决方案	191
	习题七	192

第四篇 信息安全技术

第 8 章	数据库系统安全技术	194
	本章学习目标	194
8.1	数据库系统安全概述	194
8.1.1	数据库系统的组成	194
8.1.2	数据库系统安全的含义	195
8.1.3	数据库系统的安全性要求	195
8.1.4	数据库系统的安全框架	197
8.1.5	数据库系统的安全特性	199
8.2	数据库的保护	201
8.2.1	数据库的安全性	201
8.2.2	数据库中数据的完整性	204
8.2.3	数据库并发控制	205
8.3	死锁、活锁和可串行化	207
8.3.1	死锁与活锁	207
8.3.2	可串行化	208
8.3.3	时标技术	208
8.4	攻击数据库的常用方法	209
8.5	数据库的恢复	211
8.6	Oracle 数据库的安全管理	213
8.6.1	Oracle 的安全性策略	213
8.6.2	Oracle 的用户管理	215
8.6.3	权限和角色	216
8.6.4	概要文件	217

8.6.5 数据审计	219
习题八	220
第9章 密码技术与压缩技术	222
本章学习目标	222
9.1 密码技术概述	222
9.1.1 密码通信系统的模型	222
9.1.2 密码学与密码体制	223
9.1.3 加密方式和加密的实现方法	226
9.2 加密方法	227
9.2.1 加密系统的组成	227
9.2.2 四种传统加密方法	228
9.3 密钥与密码破译方法	231
9.4 数据加密标准 DES 算法	232
9.4.1 DES 算法概述	232
9.4.2 DES 算法加密原理	234
9.5 RSA 公开密钥密码算法	240
9.6 数据压缩	244
9.6.1 数据压缩的基本概念	244
9.6.2 WinRAR 的使用方法	245
习题九	248
第10章 认证技术	250
本章学习目标	250
10.1 身份认证	250
10.1.1 身份认证概述	250
10.1.2 物理认证	252
10.1.3 身份认证协议	254
10.1.4 零知识身份认证	257
10.2 消息认证	258
10.2.1 消息认证方案	259
10.2.2 散列函数	260
10.2.3 MD5 算法	261
10.3 数字签名	264
10.3.1 数字签名原理	264
10.3.2 数字签名标准	267
习题十	268
参考文献	269