



普通高等教育“十一五”国家级规划教材  
高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会  
中国计算机学会教育专业委员会

共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

# 网络安全——技术与实践

## (第2版)

刘建伟 王育民 编著  
寇卫东 审

<http://www.tup.com.cn>

根据教育部高等学校信息安全类专业教学指导委员会制订的  
《信息安全专业指导性专业规范》组织编写

清华大学出版社





普通高等教育“十一五”国家级规划教材  
高等院校信息安全专业系列教材

教育部高等学校信息安全类专业教学指导委员会  
中国计算机学会教育专业委员会

共同指导

顾问委员会主任：沈昌祥 编委会主任：肖国镇

# 网络安全——技术与实践

## (第2版)

刘建伟 王育民 编著  
寇卫东 审

<http://www.tup.com.cn>

根据教育部高等学校信息安全类专业教学指导委员会制订的  
《信息安全专业指导性专业规范》组织编写

清华大学出版社  
北京

## 内 容 简 介

全书共分3篇15章。第1篇为网络安全基础,共3章,主要讨论了与网络安全有关的基础知识;第2篇为密码学基础,共5章,详细地讨论了网络安全中所涉及的各种密码技术;第3篇为网络安全技术与应用,共7章,深入介绍了在实践中常用的一些网络安全技术及产品。

本书内容丰富,概念清楚,语言精练。在网络安全基本知识和保密学理论的阐述上,力求深入浅出,通俗易懂;在网络安全技术与产品的讲解上,力求理论联系实际,具有很强的实用性。本书在每章的后面提供了大量思考题和练习题,以便于读者巩固课堂上所学的知识;在书末也提供了大量的参考文献,便于有兴趣的读者继续深入学习有关内容。

本书可作为信息安全、信息对抗、密码学等专业的本科生和研究生的网络安全课程教材,也可以作为网络安全工程师、网络管理员和计算机用户的参考书和培训教材。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

## 图书在版编目(CIP)数据

网络安全:技术与实践/刘建伟,王育民编著. —2版. —北京:清华大学出版社,2011.6  
ISBN 978-7-302-25721-9

I. ①网… II. ①刘… ②王… III. ①计算机网络—安全技术 IV. ①TP393.08

中国版本图书馆CIP数据核字(2011)第107437号

责任编辑:张民 薛阳

责任校对:焦丽丽

责任印制:何芊

出版发行:清华大学出版社

地 址:北京清华大学学研大厦A座

<http://www.tup.com.cn>

邮 编:100084

社 总 机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62795954, [jsjic@tup.tsinghua.edu.cn](mailto:jsjic@tup.tsinghua.edu.cn)

质 量 反 馈:010-62772015, [zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

印 装 者:北京鑫海金澳胶印有限公司

经 销:全国新华书店

开 本:185×260 印 张:28.5

字 数:653千字

版 次:2011年6月第2版

印 次:2011年6月第1次印刷

印 数:1~4000

定 价:43.00元

产品编号:039291-01

## 高等院校信息安全专业系列教材

### 编审委员会

顾问委员会主任：沈昌祥(中国工程院院士)

特别顾问：姚期智(美国国家科学院院士、美国人文及科学院院士、  
中国科学院外籍院士、“图灵奖”获得者)

何德全(中国工程院院士) 蔡吉人(中国工程院院士)

方滨兴(中国工程院院士)

主任：肖国镇

副主任：张焕国 王小云 冯登国 方勇

委员：(按姓氏笔画为序)

马建峰	毛文波	王怀民	王育民	王清贤
王新梅	刘建伟	刘建亚	谷大武	何大可
来学嘉	李建华	李晖	杨波	杨义先
张玉清	张宏莉	陈克非	宫力	胡爱群
胡道元	俞能海	侯整风	秦玉海	秦志光
卿斯汉	钱德沛	寇卫东	曹珍富	黄刘生
黄继武	谢冬青	韩臻	裴定一	廖明宏
戴宗坤				

策划编辑：张民

本书责任编辑：寇卫东

# 出版说明

21 世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继 2001 年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

- ① 体系完整、结构合理、内容先进。
- ② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。
- ③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。
- ④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由

专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于2006年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007年6月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断修订和完善。

我们的E-mail地址是：[zhangm@tup.tsinghua.edu.cn](mailto:zhangm@tup.tsinghua.edu.cn)；联系人：张民。

清华大学出版社

# 前言

随着各种网络技术的飞速发展和网络应用的普及，网络安全问题日益突出，社会对网络安全人才的需求也日益增长。许多大学都开设了信息安全或信息对抗专业，以培养信息安全和信息对抗方面的专业人才；一些从事网络安全产品开发的工程师，也迫切需要掌握网络安全方面的专业知识；对于计算机用户和网管人员来说，他们除了需要系统地学习网络安全方面的基础知识外，还需要深入了解网络安全技术和产品。因此，无论是大学教师还是网络安全工程师，都迫切需要一本理论联系实践的好书。

作者作为教育部高等学校信息安全类专业教学指导委员会委员和中国密码学会理事，参与编写了教育部的《信息安全类专业课程设置规范》。本教材所涉及的网络安全知识体系和知识点，是根据研究型大学《信息安全类专业课程设置规范》而定的。此外，作者长期从事网络安全的教学、科研和产品开发，积累了比较丰富的网络安全教学、科研和实践经验。作者想通过此书，把这些经验与读者分享。

本书共分3篇15章。第1篇为网络安全基础，共3章，主要介绍网络安全的基本概念，以及网络底层协议和高层协议的安全性。第2篇为密码学基础，共5章，主要介绍网络安全中所涉及的密码技术。第3篇为网络安全技术与应用，共7章，主要介绍一些常用的网络安全技术与应用。

本书主要有以下特色：

(1) 基本概念清晰，表述深入浅出。在基本概念的阐述上，力求准确而精练；在语言的运用上，力求顺畅而自然。在本教材中，作者尽量避免使用烦琐的语言描述晦涩难懂的理论知识，而是借助大量的图表来阐述深奥的理论。

(2) 内容翔实，重点突出。本书既简要介绍了密码学的主要内容，又重点阐述了网络安全的理论、技术与应用。在网络安全知识体系和知识点的选择上，充分参考了教育部高等学校信息安全类专业教学指导委员会制定的《信息安全类专业课程设置规范》。

(3) 理论与实践相结合。针对某些网络安全技术和产品，本教材给出相应的网络安全解决方案，从而使读者能够深入而全面地了解网络安全技术的具体应用，以提高读者在未来的网络安全实践中独立分析问题和解决问题的能力。



(4) 每章后面都附有精心斟酌和编排的思考题。通过深入分析和讨论思考题中所列问题，读者可加强对每章所学基本概念和理论的理解，从而进一步巩固所学的知识。

(5) 本书后面列出了大量的参考文献。这些参考文献为信息安全或信息对抗专业的本科生、研究生和其他技术人员提供了深入研究相关专题的途径和资料。

在本书的编写中，作者对第1版中的部分内容进行了修正，并增补了近年来密码学和网络安全领域出现的一些新理论和新技术。

本书可作为信息安全、信息对抗、密码学等专业的本科生和研究生的教材，也可以作为广大网络安全工程师、网管员和计算机用户的参考书和网络安全培训教材。

本书由刘建伟主编，刘建伟和王育民对全书进行了审校。第1~3章，第11~14章由刘建伟编著，第4~10章，第15章由王育民和刘建伟编著。

特别感谢北京航空航天大学张其善教授在各方面给予作者的关怀、支持与帮助。张教授无论在做人还是在做事方面，都是作者学习的楷模。在此，作者想由衷地表达对张其善教授深深的敬意。

感谢张斯芸、袁延荣、张雨霏等同学对第2版书稿进行了仔细的整理和校对，感谢尚涛老师、毛剑老师、修春娣老师、魏凌波博士后给予的支持与帮助，感谢杨友福、邱修峰、刘建华、陈杰、刘哲等博士生，感谢刘书明、王冠、田园、李为宇、孙钰、韩庆同、张薇、宋璐、刘靖、陈庆余、赵朋川、徐先栋、张斯芸、袁延荣、周炼赤、王世帅、樊勇、张雨霏、马妍等硕士生在第2版书稿的整理过程中给予的帮助。感谢朱云茂硕士对参考文献和图表进行了认真的整理和校对。

感谢王琼副译审对全书的文字进行了校对，为提高本书的出版质量做出了贡献。

感谢北京航空航天大学电子信息工程学院的全体老师和朋友们多年来给予作者的关心、支持和帮助。

作者  
2011年6月  
于北京



# 目录

## 第 1 篇 网络安全基础

第 1 章 引言 .....	3
1.1 对网络安全的需求 .....	5
1.1.1 网络安全发展态势 .....	5
1.1.2 敏感信息对安全的需求 .....	6
1.1.3 网络应用对安全的需求 .....	7
1.2 安全威胁与防护措施 .....	7
1.2.1 基本概念 .....	7
1.2.2 安全威胁的来源 .....	8
1.2.3 安全防护措施 .....	10
1.3 网络安全策略 .....	11
1.3.1 授权 .....	12
1.3.2 访问控制策略 .....	12
1.3.3 责任 .....	13
1.4 安全攻击的分类 .....	13
1.4.1 被动攻击 .....	13
1.4.2 主动攻击 .....	14
1.5 网络攻击的常见形式 .....	15
1.5.1 口令窃取 .....	16
1.5.2 欺骗攻击 .....	16
1.5.3 缺陷和后门攻击 .....	17
1.5.4 认证失效 .....	18
1.5.5 协议缺陷 .....	19
1.5.6 信息泄漏 .....	19
1.5.7 指数攻击——病毒和蠕虫 .....	20
1.5.8 拒绝服务攻击 .....	21
1.6 开放系统互连安全体系结构 .....	22
1.6.1 安全服务 .....	23
1.6.2 安全机制 .....	25
1.6.3 安全服务与安全机制的关系 .....	26

1.6.4 在 OSI 层中的服务配置 .....	27
1.7 网络安全模型 .....	27
习题 .....	28
<b>第 2 章 低层协议的安全性 .....</b>	<b>30</b>
2.1 基本协议 .....	30
2.1.1 网际协议 .....	30
2.1.2 地址解析协议 .....	32
2.1.3 传输控制协议 .....	33
2.1.4 用户数据报协议 .....	35
2.1.5 Internet 控制消息协议 .....	35
2.2 网络地址和域名管理 .....	36
2.2.1 路由协议 .....	36
2.2.2 BOOTP 和 DHCP .....	38
2.2.3 域名系统 .....	39
2.3 IPv6 .....	42
2.3.1 IPv6 简介 .....	42
2.3.2 过滤 IPv6 .....	44
2.4 网络地址转换 .....	45
习题 .....	45
<b>第 3 章 高层协议的安全性 .....</b>	<b>47</b>
3.1 电子邮件协议 .....	47
3.1.1 SMTP .....	47
3.1.2 POP3 协议 .....	49
3.1.3 MIME .....	50
3.1.4 Internet 消息访问协议 .....	51
3.2 Internet 电话协议 .....	52
3.2.1 H.323 .....	52
3.2.2 SIP .....	52
3.3 消息传输协议 .....	53
3.3.1 简单文件传输协议 .....	53
3.3.2 文件传输协议 .....	54
3.3.3 网络文件传输系统 .....	57
3.3.4 服务器消息块协议 .....	59
3.4 远程登录协议 .....	59
3.4.1 Telnet .....	59

3.4.2	SSH.....	60
3.5	简单网络管理协议.....	61
3.6	网络时间协议.....	62
3.7	信息服务.....	63
3.7.1	用户查询服务.....	63
3.7.2	数据库查询服务.....	64
3.7.3	LDAP.....	65
3.7.4	WWW 服务.....	67
3.7.5	网络消息传输协议.....	68
3.7.6	多播及 Mbone.....	68
	习题.....	69

## 第 2 篇 密码学基础

<b>第 4 章</b>	<b>单（私）钥密码体制.....</b>	<b>73</b>
4.1	密码体制的定义.....	73
4.2	古典密码.....	74
4.2.1	代换密码.....	75
4.2.2	换位密码.....	77
4.2.3	古典密码的安全性.....	78
4.3	流密码的基本概念.....	79
4.3.1	流密码框图和分类.....	80
4.3.2	密钥流生成器的结构和分类.....	81
4.3.3	密钥流的局部统计检验.....	82
4.3.4	随机数与密钥流.....	83
4.4	快速软、硬件实现的流密码算法.....	83
4.4.1	A5.....	83
4.4.2	加法流密码生成器.....	84
4.4.3	RC4.....	85
4.5	分组密码概述.....	86
4.6	数据加密标准（DES）.....	89
4.6.1	DES 介绍.....	89
4.6.2	DES 的核心作用：消息的随机非线性分布.....	91
4.6.3	DES 的安全性.....	92
4.7	高级加密标准（AES）.....	92
4.7.1	Rijndael 密码概述.....	93
4.7.2	Rijndael 密码的内部函数.....	94

4.7.3	AES 密码算法 .....	97
4.7.4	AES 的密钥扩展 .....	98
4.7.5	AES 对应用密码学的积极影响 .....	101
4.8	其他重要的分组密码算法 .....	101
4.8.1	IDEA .....	101
4.8.2	SAFER K-64 .....	105
4.8.3	RC5 .....	107
4.9	分组密码的工作模式 .....	109
4.9.1	电码本模式 .....	110
4.9.2	密码分组链接模式 .....	111
4.9.3	密码反馈模式 .....	111
4.9.4	输出反馈模式 .....	112
4.9.5	计数器模式 .....	114
	习题 .....	114
<b>第 5 章</b>	<b>双（公）钥密码体制 .....</b>	<b>116</b>
5.1	双钥密码体制的基本概念 .....	117
5.1.1	单向函数 .....	117
5.1.2	陷门单向函数 .....	118
5.1.3	公钥系统 .....	118
5.1.4	用于构造双钥密码的单向函数 .....	118
5.2	RSA 密码体制 .....	121
5.2.1	体制 .....	121
5.2.2	RSA 的安全性 .....	122
5.2.3	RSA 的参数选择 .....	125
5.2.4	RSA 体制实用中的其他问题 .....	127
5.2.5	RSA 的实现 .....	127
5.3	背包密码体制 .....	128
5.3.1	背包问题 .....	128
5.3.2	简单背包 .....	129
5.3.3	Merkle-Hellman 陷门背包 .....	129
5.3.4	M-H 体制的安全性 .....	130
5.3.5	背包体制的缺陷 .....	131
5.3.6	其他背包体制 .....	131
5.4	Rabin 密码体制 .....	131
5.4.1	Rabin 体制 .....	131
5.4.2	Williams 体制 .....	132

5.5	ElGamal 密码体制.....	132
5.5.1	方案.....	133
5.5.2	加密.....	133
5.5.3	安全性.....	133
5.6	椭圆曲线密码体制.....	133
5.6.1	实数域上的椭圆曲线.....	134
5.6.2	有限域 $Z_p$ 上的椭圆曲线.....	135
5.6.3	$GF(2^m)$ 上的椭圆曲线.....	137
5.6.4	椭圆曲线密码.....	138
5.6.5	椭圆曲线的安全性.....	139
5.6.6	ECC 的实现.....	139
5.6.7	当前 ECC 的标准化工作.....	140
5.6.8	椭圆曲线上的 RSA 密码体制.....	141
5.6.9	用圆锥曲线构造双钥密码体制.....	141
5.7	基于身份的密码体制.....	142
5.7.1	引言.....	142
5.7.2	双线性映射和双线性 D-H 假设.....	143
5.7.3	IBE 方案描述.....	144
5.7.4	IBE 方案的安全性.....	145
5.8	公钥密码体制的分析.....	147
	习题.....	149
<b>第 6 章</b>	<b>消息认证与杂凑函数.....</b>	<b>151</b>
6.1	认证函数.....	151
6.1.1	消息加密.....	151
6.1.2	消息认证码.....	155
6.1.3	杂凑函数.....	157
6.1.4	杂凑函数的性质.....	158
6.2	消息认证码.....	159
6.2.1	对 MAC 的要求.....	159
6.2.2	基于密钥杂凑函数的 MAC.....	160
6.2.3	基于分组加密算法的 MAC.....	161
6.3	杂凑函数.....	162
6.3.1	单向杂凑函数.....	162
6.3.2	杂凑函数在密码学中的应用.....	162
6.3.3	分组迭代单向杂凑算法的层次结构.....	162
6.3.4	迭代杂凑函数的构造方法.....	163

6.3.5	应用杂凑函数的基本方式.....	164
6.4	MD-4 和 MD-5 .....	166
6.4.1	算法步骤.....	166
6.4.2	MD-5 的安全性.....	169
6.4.3	MD-5 的实现.....	169
6.4.4	MD-4 与 MD-5 算法差别.....	170
6.4.5	MD-2 和 MD-3 .....	170
6.5	安全杂凑算法.....	170
6.5.1	算法.....	170
6.5.2	SHA 的安全性.....	172
6.5.3	SHA 与 MD-4、MD-5 的比较.....	173
6.6	HMAC.....	174
6.6.1	HMAC 的设计目标.....	174
6.6.2	算法描述.....	175
6.6.3	HMAC 的安全性.....	175
	习题.....	176
<b>第 7 章</b>	<b>数字签名 .....</b>	<b>178</b>
7.1	数字签名基本概念.....	178
7.2	RSA 签名体制.....	179
7.3	Rabin 签名体制.....	180
7.4	ElGamal 签名体制.....	181
7.5	Schnorr 签名体制.....	182
7.6	DSS 签名标准.....	184
7.6.1	概况.....	184
7.6.2	签名和验证签名的基本框图.....	184
7.6.3	算法描述.....	184
7.6.4	DSS 签名和验证框图.....	185
7.6.5	公众反应.....	185
7.6.6	实现速度.....	185
7.7	基于椭圆曲线的数字签名体制.....	186
7.8	其他数字签名体制.....	186
7.8.1	离散对数签名体制.....	186
7.8.2	不可否认签名.....	187
7.8.3	防失败签名.....	187
7.8.4	盲签名.....	187
7.8.5	群签名.....	188

7.8.6	代理签名	189
7.8.7	指定证实人的签名	189
7.8.8	一次性数字签名	189
7.8.9	双有理签名方案	190
7.8.10	数字签名的应用	190
	习题	190
<b>第 8 章</b>	<b>密码协议</b>	<b>191</b>
8.1	协议的基本概念	191
8.1.1	仲裁协议 (Arbitrated Protocol)	191
8.1.2	裁决协议 (Adjudicated Protocol)	193
8.1.3	自动执行协议 (Self-Enforcing Protocol)	193
8.2	安全协议分类及基本密码协议	195
8.2.1	密钥建立协议	195
8.2.2	认证建立协议	200
8.2.3	认证的密钥建立协议	204
8.3	秘密分拆协议	213
8.4	会议密钥分配和秘密广播协议	214
8.4.1	秘密广播协议	214
8.4.2	会议密钥分配协议	215
8.5	密码协议的安全性	216
8.5.1	对协议的攻击	216
8.5.2	密码协议的安全性分析	220
	习题	221

### 第 3 篇 网络安全技术与应用

<b>第 9 章</b>	<b>数字证书与公钥基础设施</b>	<b>225</b>
9.1	PKI 的基本概念	225
9.1.1	PKI 的定义	225
9.1.2	PKI 的组成	225
9.1.3	PKI 的应用	227
9.2	数字证书	228
9.2.1	数字证书的概念	229
9.2.2	数字证书的结构	229
9.2.3	数字证书的生成	231
9.2.4	数字证书的签名与验证	233



9.2.5	数字证书层次与自签名数字证书.....	235
9.2.6	交叉证书.....	237
9.2.7	数字证书的撤销.....	238
9.2.8	漫游证书.....	243
9.2.9	属性证书.....	244
9.3	PKI 体系结构——PKIX 模型.....	245
9.3.1	PKIX 服务.....	245
9.3.2	PKIX 体系结构.....	245
9.4	PKI 实例.....	246
9.5	授权管理设施——PMI.....	247
9.5.1	PMI 的定义.....	247
9.5.2	PMI 与 PKI 的关系.....	248
9.5.3	实现 PMI 的机制.....	249
9.5.4	PMI 模型.....	250
9.5.5	基于 PMI 建立安全应用.....	251
习题	.....	252
<b>第 10 章</b>	<b>网络加密与密钥管理.....</b>	<b>254</b>
10.1	网络加密的方式及实现.....	254
10.1.1	链路加密.....	254
10.1.2	节点加密.....	255
10.1.3	端到端加密.....	255
10.1.4	混合加密.....	256
10.2	硬件、软件加密及有关问题.....	257
10.2.1	硬件加密的优点.....	257
10.2.2	硬件种类.....	258
10.2.3	软件加密.....	258
10.2.4	存储数据加密的特点.....	258
10.2.5	文件删除.....	259
10.3	密钥管理基本概念.....	259
10.3.1	密钥管理.....	259
10.3.2	密钥的种类.....	260
10.4	密钥生成.....	261
10.4.1	密钥选择对安全性的影响.....	262
10.4.2	好的密钥.....	262
10.4.3	不同等级的密钥产生的方式不同.....	262
10.5	密钥分配.....	263
10.5.1	基本方法.....	263

10.5.2	密钥分配的基本工具.....	265
10.5.3	密钥分配系统的基本模式.....	265
10.5.4	可信第三方 TTP.....	265
10.5.5	密钥注入.....	267
10.6	密钥的证实.....	267
10.6.1	单钥证书.....	268
10.6.2	公钥的证实技术.....	269
10.6.3	公钥认证树.....	269
10.6.4	公钥证书.....	270
10.6.5	基于身份的公钥系统.....	271
10.6.6	隐式证实公钥.....	272
10.7	密钥的保护、存储与备份.....	273
10.7.1	密钥的保护.....	273
10.7.2	密钥的存储.....	274
10.7.3	密钥的备份.....	274
10.8	密钥的泄漏、吊销、过期与销毁.....	275
10.8.1	泄漏与吊销.....	275
10.8.2	密钥的有效期.....	275
10.8.3	密钥销毁.....	275
10.9	密钥控制.....	276
10.10	多个管区的密钥管理.....	277
10.11	密钥管理系统.....	279
	习题.....	281
<b>第 11 章</b>	<b>无线网络安全.....</b>	<b>282</b>
11.1	无线网络面临的安全威胁.....	282
11.2	无线蜂窝网络的安全性.....	285
11.2.1	GSM 的安全性.....	285
11.2.2	CDMA 的安全性.....	288
11.2.3	3G 系统的安全性.....	290
11.3	无线数据网络的安全性.....	292
11.3.1	有线等效保密协议.....	292
11.3.2	802.1x 协议介绍.....	294
11.3.3	802.11i 标准介绍.....	295
11.3.4	802.16 标准的安全性.....	298
11.3.5	WAPI 标准简介.....	301
11.3.6	WAP 的安全性.....	302