



普通高等教育“十一五”国家级规划教材
教育部普通高等教育精品教材
中央网信办暨教育部评选的**国家网络安全优秀教材奖**

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

网络空间安全重点规划丛书

顾问委员会主任：沈昌祥 编委会主任：封化民

网络安全

——技术与实践（第3版）

刘建伟 王育民 编著

根据教育部高等学校信息安全专业教学指导委员会编制的
《高等学校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
教育部普通高等教育精品教材
中央网信办暨教育部评选的**国家网络安全优秀教材奖**

教育部高等学校信息安全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

网络空间安全重点规划丛书

网络安全

——技术与实践（第3版）

刘建伟 王育民 编著

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,主要讨论网络安全的基础知识;第2篇为密码学基础,共5章,详细讨论各种密码算法和技术,特别深入地介绍我国已公布的标准密码算法;第3篇为网络安全技术与应用,共7章,深入介绍网络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密码学理论的阐述上,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,面向具体应用。本书在每章的后面提供了思考题和练习题,以便于读者巩固所学的知识点;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、信息对抗技术、密码学等专业的本科生教材,也可以用作网络空间安全一级学科的研究生教材。对于广大网络安全工程师、网络管理员和IT从业人员来说,本书也是很好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. —3版. —北京:清华大学出版社,2017
(网络空间安全重点规划丛书)

ISBN 978-7-302-46758-8

I. ①网… II. ①刘… ②王… III. ①计算机网络-网络安全-研究 IV. ①TP393.08

中国版本图书馆CIP数据核字(2017)第042441号

责任编辑:张 民

封面设计:常雪影

责任校对:白 蕾

责任印制:何 芊

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦A座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

课 件 下 载: <http://www.tup.com.cn>, 010-62795954

印 刷 者:三河市君旺印务有限公司

装 订 者:三河市新茂装订有限公司

经 销:全国新华书店

开 本:185mm×260mm 印 张:30.5 字 数:696千字

版 次:2005年6月第1版 2017年5月第3版 印 次:2017年5月第1次印刷

印 数:1~2000

定 价:59.50元

产品编号:070984-01

网络空间安全重点规划丛书

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：封化民

副主任：韩臻 李建华 王小云 张焕国 冯登国

委员：(按姓氏笔画为序)

马建峰 毛文波 王怀民 王劲松 王丽娜

王育民 王清贤 王新梅 石文昌 刘建伟

刘建亚 许进 杜瑞颖 谷大武 何大可

来学嘉 李晖 汪烈军 吴晓平 杨波

杨庚 杨义先 张玉清 张红旗 张宏莉

张敏情 陈兴蜀 陈克非 周福才 宫力

胡爱群 胡道元 侯整风 荆继武 俞能海

高岭 秦玉海 秦志光 卿斯汉 钱德沛

徐明 寇卫东 曹珍富 黄刘生 黄继武

谢冬青 裴定一

丛书策划：张民

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,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。系列教材的作者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。

该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。

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系列教材中,以进一步满足大家对外版书的需求。“高等院校信息安全专业系列教材”已于 2006 年年初正式列入普通高等教育“十一五”国家级教材规划。

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起到重要的指导和推动作用。2006年教育部给武汉大学下达了“信息安全专业指导性专业规范研制”的教学科研项目。2007年起该项目由教育部高等学校信息安全类专业教学指导委员会组织实施。在高教司和教指委的指导下,项目组团结一致,努力工作,克服困难,历时5年,制定出我国第一个信息安全专业指导性专业规范,于2012年年底通过经教育部高等教育司理工科教育处授权组织的专家组评审,并且已经得到武汉大学等许多高校的实际使用。2013年,新一届“教育部高等学校信息安全专业教学指导委员会”成立。经组织审查和研究决定,2014年以“教育部高等学校信息安全专业教学指导委员会”的名义正式发布《高等学校信息安全专业指导性专业规范》(由清华大学出版社正式出版)。

2015年6月,国务院学位委员会、教育部出台增设“网络空间安全”为一级学科的决定,将高校培养网络空间安全人才提到新的高度。2016年6月,中央网络安全和信息化领导小组办公室(下文简称中央网信办)、国家发展和改革委员会、教育部、科学技术部、工业和信息化部及人力资源和社会保障部六大部门联合发布《关于加强网络安全学科建设和人才培养的意见》(中网办发[2016]4号)。为贯彻落实《关于加强网络安全学科建设和人才培养的意见》,进一步深化高等教育教学改革,促进网络安全学科专业建设和人才培养,促进网络空间安全相关核心课程和教材建设,在教育部高等学校信息安全专业教学指导委员会和中央网信办资助的网络空间安全教材建设课题组的指导下,启动了“网络空间安全重点规划丛书”的工作,由教育部高等学校信息安全专业教学指导委员会秘书长封化民校长担任编委会主任。本规划丛书基于“高等院校信息安全专业系列教材”坚实的工作基础和成果、阵容强大的编审委员会和优秀的作者队伍,目前已经有多本图书获得教育部和中央网信办等机构评选的“普通高等教育本科国家级规划教材”、“普通高等教育精品教材”、“中国大学出版社图书奖”和“国家网络安全优秀教材奖”等多个奖项。

“网络空间安全重点规划丛书”将根据《高等学校信息安全专业指导性专业规范》(及后续版本)和相关教材建设课题组的研究成果不断更新和扩展,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,并随着我国网络空间安全学科的发展不断完善,力争为我国网络空间安全相关学科专业的本科和研究生教材建设、学术出版与人才培养做出更大的贡献。

我们的E-mail地址是: zhangm@tup.tsinghua.edu.cn,联系人: 张民。

“网络空间安全重点规划丛书”编审委员会

前言

为了加强网络空间安全专业人才的培养，教育部已正式批准在 29 所大学设立网络空间安全一级学科博士点，全国已有 128 所高校相继设立了信息安全或信息对抗本科专业。为了提高网络空间安全人才培养质量，急需编写出版一批高水平的网络空间安全优秀教材。

作者作为教育部高等学校信息安全专业教学指导委员会委员和中国密码学会理事，参与编写了教育部高等学校信息安全专业教学指导委员会编制的《高等学校信息安全专业指导性专业规范》。在本书的编写过程中，力求使本教材的知识体系和知识点符合《高等学校信息安全专业指导性专业规范》的要求，并加入了对国产密码算法的阐述。

全书共分 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、计算机网络的基础知识，以及 TCP/IP 协议族的安全性。第 2 篇为密码学基础，共 5 章，主要介绍密码学中的各种密码算法和协议。第 3 篇为网络安全技术与应用，共 7 章，主要介绍 PKI/CA、密钥管理、无线网络的安全，以及防火墙、VPN、IDS 和身份认证等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。作者尽量避免使用晦涩难懂的语言描述深奥的理论和知识，而是借助大量的图表进行阐述。

(2) 内容全面，涵盖密码学和网络安全技术。本书既介绍了现代密码学的知识，又阐述了网络安全的理论与技术，特别适合于将密码学和网络安全合并为一门课进行授课的高校。

(3) 理论与实践相结合。针对某些网络安全技术和产品，本书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) 本书详细列出了大量的参考文献。这些参考文献为网络空间安全学科的研究生和密码学、信息安全、信息对抗技术等专业的本科生，以及其他网络安全技术人员提供了深入研究相关专题的途径和资料。

本书可作为密码学、信息安全和信息对抗技术等专业的本科生教材和网络空间安全学科的研究生教材，也可以作为网络安全工程师的参考书和培训教材。

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章由刘建伟编著，第2章由杜瑞颖编著，第3章由杜瑞颖和刘建伟编著，第11~14章由刘建伟编著，第4~10章和第15章由王育民和刘建伟编著。

感谢伍前红教授、尚涛副教授、毛剑老师、关振宇老师、修春娣老师、张宗洋老师给予的支持与帮助。感谢陈杰、刘巍然、毛可飞、周星光、王蒙蒙、何双羽、程东旭、刘哲、李大伟、程昊苏、钟林、王朝、姜勇、周林志等博士研究生，以及宋晨光、苏航、冯伯昂、周修文、陶芮、夏丹枫、樊一康、齐婵、刘懿中、王培人、马寒军、雷奇、李珂、崔键、史福田、杜岗、王沁、梁智等硕士研究生在书稿的整理过程中给予作者的大力支持与帮助。

由于作者水平所限，书中难免会存在错误和不妥之处。敬请广大读者朋友批评指正。

作者
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
第 2 章	计算机网络基础	30
2.1	计算机网络的定义	30
2.2	计算机网络体系的结构	30
2.2.1	网络体系结构的定义	30
2.2.2	两种典型的网络体系结构	32
2.2.3	网络协议及协议封装	34
2.3	分组交换技术	35
2.3.1	分组交换技术的概念	35
2.3.2	分组交换的特点	35
2.4	Internet 的基本知识	36
2.4.1	Internet 的构成	36
2.4.2	服务类别	37
2.4.3	IPv4 地址	37
2.4.4	端口的概念	40
	习题	41
第 3 章	Internet 协议的安全性	43
3.1	Internet 协议概述	43
3.2	网际层协议	43
3.2.1	IP 协议	43
3.2.2	ARP 协议	45
3.2.3	ICMP 协议	46
3.2.4	IGMP 协议	47
3.2.5	OSPF 协议	48
3.2.6	BGP 协议	49
3.3	传输层协议	50
3.3.1	TCP 协议	51
3.3.2	UDP 协议	52
3.4	应用层协议	53
3.4.1	RIP 协议	53
3.4.2	HTTP 协议	54
3.4.3	TELNET 协议	55
3.4.4	SSH 协议	56

3.4.5	DNS 协议	57
3.4.6	SMTP 协议	58
3.4.7	MIME 协议	60
3.4.8	POP3 协议	60
3.4.9	IMAP4 协议	61
3.4.10	PGP 协议	63
3.4.11	FTP 协议	64
3.4.12	TFTP 协议	65
3.4.13	NFS 协议	65
3.4.14	SNMP 协议	66
3.4.15	DHCP 协议	67
3.4.16	H.323 协议	68
3.4.17	SIP 协议	69
3.4.18	NTP 协议	70
3.4.19	FINGER 协议	71
3.4.20	Whois 协议	72
3.4.21	LDAP 协议	73
3.4.22	NNTP 协议	74
	习题	75

第 2 篇 密码学基础

第 4 章	单 (私) 钥密码体制	79
4.1	密码体制的定义	79
4.2	古典密码	80
4.2.1	代换密码	81
4.2.2	换位密码	83
4.2.3	古典密码的安全性	84
4.3	流密码的基本概念	85
4.3.1	流密码框图和分类	86
4.3.2	密钥流生成器的结构和分类	87
4.3.3	密钥流的局部统计检验	88
4.4	快速软、硬件实现的流密码算法	89
4.4.1	A5	89
4.4.2	加法流密码生成器	90
4.4.3	RC4	91
4.4.4	祖冲之密码	92

4.5	分组密码概述	98
4.6	数据加密标准	101
4.6.1	DES 介绍	101
4.6.2	DES 的核心作用：消息的随机非线性分布	103
4.6.3	DES 的安全性	103
4.7	高级加密标准	104
4.7.1	Rijndael 密码概述	105
4.7.2	Rijndael 密码的内部函数	106
4.7.3	AES 密码算法	109
4.7.4	AES 的密钥扩展	111
4.7.5	AES 对应用密码学的积极影响	112
4.8	中国商用分组密码算法 SM4	113
4.8.1	SM4 密码算法	113
4.8.2	SM4 密钥扩展算法	116
4.8.3	SM4 的安全性	117
4.9	分组密码的工作模式	117
4.9.1	电码本模式	118
4.9.2	密码分组链接模式	118
4.9.3	密码反馈模式	119
4.9.4	输出反馈模式	120
4.9.5	计数器模式	122
	习题	122
第5章 双（公）钥密码体制		124
5.1	双钥密码体制的基本概念	125
5.1.1	单向函数	125
5.1.2	陷门单向函数	126
5.1.3	公钥系统	126
5.1.4	用于构造双钥密码的单向函数	126
5.2	RSA 密码体制	128
5.2.1	RSA 密码体制	129
5.2.2	RSA 的安全性	130
5.2.3	RSA 的参数选择	133
5.2.4	RSA 体制应用中的其他问题	135
5.2.5	RSA 的实现	135
5.3	ElGamal 密码体制	136
5.3.1	密钥生成	136

5.3.2	加解密	136
5.3.3	安全性	136
5.4	椭圆曲线密码体制	137
5.4.1	实数域上的椭圆曲线	137
5.4.2	有限域 Z_p 上的椭圆曲线	138
5.4.3	$GF(2^m)$ 上的椭圆曲线	140
5.4.4	椭圆曲线密码	141
5.4.5	椭圆曲线的安全性	142
5.4.6	ECC 的实现	143
5.4.7	当前 ECC 的标准化工作	143
5.4.8	椭圆曲线上的 RSA 密码体制	144
5.4.9	用圆锥曲线构造双钥密码体制	144
5.5	基于身份的密码体制	145
5.5.1	引言	145
5.5.2	双线性映射和双线性 D-H 假设	146
5.5.3	IBE 方案	147
5.5.4	IBE 方案的安全性	148
5.6	中国商用密码 SM2 算法	151
5.6.1	SM2 椭圆曲线推荐参数	151
5.6.2	辅助函数	151
5.6.3	密钥生成	152
5.6.4	加密	152
5.6.5	解密	153
5.6.6	实例与应用	155
5.7	公钥密码体制的安全性分析	155
	习题	157
第 6 章	消息认证与杂凑函数	159
6.1	认证函数	159
6.1.1	消息加密	159
6.1.2	消息认证码	163
6.1.3	杂凑函数	165
6.2	消息认证码	166
6.2.1	对 MAC 的要求	167
6.2.2	基于杂凑函数的 MAC	168
6.2.3	基于分组加密算法的 MAC	169
6.3	杂凑函数	169

6.3.1	单向杂凑函数.....	169
6.3.2	杂凑函数在密码学中的应用.....	170
6.3.3	分组迭代单向杂凑算法的层次结构.....	170
6.3.4	迭代杂凑函数的构造方法.....	171
6.3.5	应用杂凑函数的基本方式.....	172
6.4	常用杂凑函数.....	174
6.4.1	MD 系列杂凑函数.....	174
6.4.2	SHA 系列杂凑函数.....	178
6.4.3	中国商用杂凑函数 SM3.....	181
6.5	HMAC.....	184
6.5.1	HMAC 的设计目标.....	184
6.5.2	算法描述.....	185
6.5.3	HMAC 的安全性.....	186
	习题.....	187
第 7 章	数字签名	189
7.1	数字签名基本概念.....	189
7.2	RSA 签名体制.....	190
7.2.1	体制参数.....	190
7.2.2	签名过程.....	191
7.2.3	验证过程.....	191
7.2.4	安全性.....	191
7.3	ElGamal 签名体制.....	191
7.3.1	体制参数.....	191
7.3.2	签名过程.....	192
7.3.3	验证过程.....	192
7.3.4	安全性.....	192
7.4	Schnorr 签名体制.....	193
7.4.1	体制参数.....	193
7.4.2	签名过程.....	193
7.4.3	验证过程.....	193
7.4.4	Schnorr 签名与 ElGamal 签名的不同点.....	194
7.5	DSS 签名标准.....	194
7.5.1	概况.....	194
7.5.2	签名和验证签名的基本框图.....	195
7.5.3	算法描述.....	195
7.5.4	DSS 签名和验证框图.....	196

7.5.5	公众反应.....	196
7.5.6	实现速度.....	196
7.6	中国商用数字签名算法 SM2.....	197
7.6.1	体制参数.....	197
7.6.2	签名过程.....	197
7.6.3	验证过程.....	198
7.6.4	签名实例.....	199
7.7	具有特殊功能的数字签名体制.....	200
7.7.1	不可否认签名.....	200
7.7.2	防失败签名.....	200
7.7.3	盲签名.....	201
7.7.4	群签名.....	201
7.7.5	代理签名.....	202
7.7.6	指定证实人的签名.....	202
7.7.7	一次性数字签名.....	203
7.7.8	双有理签名方案.....	203
7.8	数字签名的应用.....	203
	习题.....	203
第 8 章	密码协议.....	205
8.1	协议的基本概念.....	205
8.1.1	仲裁协议.....	205
8.1.2	裁决协议.....	207
8.1.3	自动执行协议.....	207
8.2	安全协议分类及基本密码协议.....	209
8.2.1	密钥建立协议.....	209
8.2.2	认证建立协议.....	214
8.2.3	认证的密钥建立协议.....	218
8.3	秘密分拆协议.....	226
8.4	会议密钥分配和秘密广播协议.....	228
8.4.1	秘密广播协议.....	228
8.4.2	会议密钥分配协议.....	229
8.5	密码协议的安全性.....	229
8.5.1	对协议的攻击.....	230
8.5.2	密码协议的安全性分析.....	233
	习题.....	235

第3篇 网络安全技术与应用

第9章 数字证书与公钥基础设施	239
9.1 PKI的基本概念	239
9.1.1 PKI的定义	239
9.1.2 PKI的组成	239
9.1.3 PKI的应用	241
9.2 数字证书	242
9.2.1 数字证书的概念	243
9.2.2 数字证书的结构	243
9.2.3 数字证书的生成	245
9.2.4 数字证书的签名与验证	247
9.2.5 数字证书层次与自签名数字证书	249
9.2.6 交叉证书	251
9.2.7 数字证书的撤销	252
9.2.8 漫游证书	257
9.2.9 属性证书	258
9.3 PKI体系结构——PKIX模型	259
9.3.1 PKIX服务	259
9.3.2 PKIX体系结构	259
9.4 PKI实例	260
9.5 授权管理设施——PMI	261
9.5.1 PMI的定义	261
9.5.2 PMI与PKI的关系	262
9.5.3 实现PMI的机制	263
9.5.4 PMI模型	264
9.5.5 基于PMI建立安全应用	265
习题	266
第10章 网络加密与密钥管理	268
10.1 网络加密的方式及实现	268
10.1.1 链路加密	268
10.1.2 节点加密	269
10.1.3 端到端加密	269
10.1.4 混合加密	270
10.2 硬件、软件加密及有关问题	271

10.2.1	硬件加密的优点.....	271
10.2.2	硬件种类.....	272
10.2.3	软件加密.....	272
10.2.4	存储数据加密的特点.....	272
10.2.5	文件删除.....	273
10.3	密钥管理基本概念.....	273
10.3.1	密钥管理.....	273
10.3.2	密钥的种类.....	274
10.4	密钥生成.....	275
10.4.1	密钥选择对安全性的影响.....	276
10.4.2	好的密钥.....	276
10.4.3	不同等级的密钥产生的方式不同.....	276
10.5	密钥分配.....	277
10.5.1	基本方法.....	277
10.5.2	密钥分配的基本工具.....	279
10.5.3	密钥分配系统的基本模式.....	279
10.5.4	可信第三方 TTP.....	279
10.5.5	密钥注入.....	281
10.6	密钥的证实.....	281
10.6.1	单钥证书.....	282
10.6.2	公钥的证实技术.....	283
10.6.3	公钥认证树.....	283
10.6.4	公钥证书.....	284
10.6.5	基于身份的公钥系统.....	285
10.6.6	隐式证实公钥.....	286
10.7	密钥的保护、存储与备份.....	287
10.7.1	密钥的保护.....	287
10.7.2	密钥的存储.....	288
10.7.3	密钥的备份.....	288
10.8	密钥的泄漏、吊销、过期与销毁.....	289
10.8.1	泄漏与吊销.....	289
10.8.2	密钥的有效期.....	289
10.8.3	密钥销毁.....	289
10.9	密钥控制.....	290
10.10	多个管区的密钥管理.....	291
10.11	密钥管理系统.....	293
	习题.....	295