



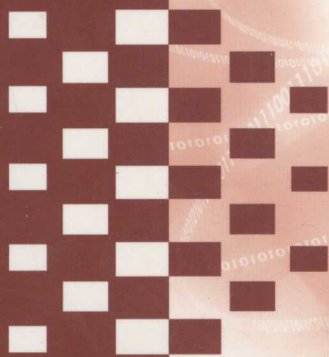
21世纪电子商务系列教材  
全国高等院校电子商务联编教材

# 电子商务安全 保密技术与应用

Security Technology and Application on E-Commerce

主 编 肖德琴

副主编 祁 明 彭丽芳



华南理工大学出版社

F713.36  
XDA

内容简介



21世纪电子商务系列教材  
全国高等院校电子商务联编教材

# 电子商务安全保密技术与应用

主 编 肖德琴

副主编 祁 明 彭丽芳

华南理工大学出版社

·广州·

## 内 容 简 介

电子商务安全保密技术与应用是当今电子商务领域最热门的话题之一。本书全面介绍了电子商务安全保密技术的基础理论、应用和实际的解决方案,内容包括:电子商务所涉及的典型密码算法、数字签名技术、认证技术、密钥管理技术、网络安全技术,电子商务安全常用的安全协议和 PKI 技术,移动商务安全技术,以及电子商务安全在电子政务、企业信息化中的特殊应用,国内外著名公司的电子商务安全解决方案等。

本书跟踪了当前电子商务发展的许多热点,观点新颖,论述深入浅出,内容丰富,引例生动,可读性和实践性强,章末附有习题。特别适合作为电子商务专业、计算机应用专业和金融、营销等专业的教材,也可作为计算机或电子商务领域的研究人员和专业技术人员的参考书。

## 图书在版编目 (CIP) 数据

电子商务安全保密技术与应用/肖德琴主编. —广州:华南理工大学出版社, 2003.9

(21 世纪电子商务系列教材)

ISBN 7-5623-1988-X

I. 电… II. 肖… III. 电子商务-安全技术-高等学校-教材  
IV. F713.36

中国版本图书馆 CIP 数据核字 (2003) 第 067928 号

总 发 行: 华南理工大学出版社 (广州五山华南理工大学 17 号楼, 邮编 510640)

发行部电话: 020-87113487 87111048 (传真)

E-mail: [scut202@scut.edu.cn](mailto:scut202@scut.edu.cn) <http://www2.scut.edu.cn/press>

责任编辑: 詹志青

印 刷 者: 中山市新华印刷厂有限公司

开 本: 787×960 1/16 印张: 23 字数: 504 千

版 次: 2003 年 9 月第 1 版第 1 次印刷

印 数: 1~5000 册

定 价: 32.00 元

版权所有 盗版必究

## “21 世纪电子商务系列教材”编委会

**顾问:** 宋 玲(国家级专家,教授)  
刘焕彬(俄罗斯工程院外籍院士,教授,博士生导师)  
邹 生(博士,高级工程师)

**主任:** 李元元(博士,教授,博士生导师)

**副主任:** 祁 明 王学东 杨琦峰 李新星

**编委**(以姓氏笔划为序):

王学东(华中师范大学)	王洪良(广东外语外贸大学)
刘才兴(华南农业大学)	关永宏(华南理工大学)
祁 明(华南理工大学)	许晶华(华南师范大学)
孙德林(江西师范大学)	张 军(广东商学院)
李 华(广东省电子商务示范基地)	李 丽(深圳大学)
李新星(广东省电子商务协会)	杜江萍(江西财经大学)
吴应良(华南理工大学)	余序洲(中南民族大学)
欧阳峰(汕头大学)	杨琦峰(武汉理工大学)
姜灵敏(广东商学院)	赵 波(广州大学)
胡矗明(暨南大学)	高京广(广东工业大学)
黄文标(广东省电子邮政局)	黄观辉(广东省信息中心)
彭丽芳(厦门大学)	

**项目总策划:** 范家巧 潘宜玲

**执行策划:** 胡 元 詹志青

## 总 序

随着知识经济在全世界范围内的快速发展,人们对电子商务已经从怀疑、观望到大力支持,各行各业已经从消极适应走向主动参与,电子商务应用领域已经从局部走向全局,电子商务应用已经从专家推动、行业协会推动到政府推动,这就是世界和中国电子商务的今天。这种新的经济形式所包含的内容远远不止在线销售、物流配送、客户关系管理、电子政务和企业信息化等传统的电子商务内容,它既有企业之间跨越供应渠道或运用在线采购进行的国际贸易,也包含知识管理、技术创新、电子商务标准、PKI与数字证书、电子商务法律法规、金字系列工程、电子商务资本经营和社会信用系统等极为活跃的内容。本系列教材将上述两方面内容有机结合,使学生更透彻、全面了解电子商务的全新发展。

电子商务是当今世界经济和社会发展的新趋势。作为新经济时代先进生产力的代表,电子商务的水平已经成为衡量一个国家、一个城市现代化水平和综合实力的重要标志之一,也是加快实现经济体制和经济增长方式的根本性转变、推动产业结构的升级、提高城市现代化水平和增强国际竞争力的重要手段。目前,全国各地纷纷掀起电子商务建设和应用的热潮,可谓是形势喜人、形势催人、形势逼人。

电子商务系统建设是一项宏伟的系统工程,也是一项高投入工程。在实际的建设与应用中,无论在规划上、技术上和安全上,还是在实施中、应用中和管理中,都存在着许多亟待解决的问题。归纳起来主要包括:如何根据城市或企业自身特点进行科学的规划和建设,避免盲目地追求一步到位?如何防止各自为政、盲目投资、重硬轻软、重复建设?如何使资源得到充分的集中和共享,杜绝“信息孤岛”现象?如何推进实施力度,提高应用水平?如何解决在安全保密、环境体系、管理体制方面存在的问题,提高电子商务工程的成功率?存在这些问题的根源是我们缺乏电子商务应用型人才和管理人才,尤其是复合型电子商务应用型人才和管理人才的缺乏更成为制约电子商务发展的瓶颈。



这套由中国电子商务领域的众多专家和教授编写的关于电子商务技术和应用的系列教材，旨在提供对这一重要学科的整体概述。该系列教材涵盖了电子商务、电子政务、企业信息化、行业信息化、社会信息化等广泛领域中的重要课题。对于任何一位想更多地了解关于电子商务知识——从有关模型、技术到案例分析——的读者，特别是对于高校学生，这是一套出色的教材和参考资料。这套教材的显著特点是，不仅有一定的理论高度，而且能够将电子商务理论、当前的电子商务市场需求和电子商务人才能力培养相结合，能够将信息技术教育、工商管理教育和人文教育等多个学科的特点和优势与电子商务教育相结合，它必将极大地促进我国高素质电子商务复合型人才的培养。本系列教材对每一位从事电子商务规划工作、实施工作或使用电子商务系统及工具的读者，也将有所裨益。

中国电子商务协会理事长 **宋玲**

2003年8月

## 前 言

随着信息技术 Internet 的飞速发展, 电子商务(特别是通过 Internet 进行的电子商务)成为越来越多的人关注的焦点。而由于 Internet 的开放性和其他各种因素的影响, 在进行电子商务(特别是网络支付)活动时, 在 Internet 上需要传输消费者和商家的一些机密信息, 如用户信用卡号、商家用户信息和订购信息等, 而这些信息一直是网络非法入侵者或黑客的攻击目标。如何保证电子商务安全, 如何对敏感信息和个人信息提供机密性保障、认证交易双方的合法身份、保证数据的完整性和交易的不可否认性等, 已经成为制约电子商务发展的瓶颈, 对这些问题的担心也是导致很多人不愿意进行网上购物和支付的主要原因。

各种网络安全事故的发生, 使越来越多的行家意识到, 人们普遍对电子商务安全意识的淡薄和安全人才的奇缺是网络出现安全漏洞的一个非常重要的原因。因此, 出现了一批与电子商务安全相关的新兴职业, 如电子保安、电子商务律师、电子商务司法人员、电子商务法官、电子商务安全警察、电子商务安全员、电子商务安全策划等等。毫无疑问, 电子商务安全知识及其应用技术已成为电子商务从业人员了解和掌握的必备知识, 也成为众多学者、研究开发人员、政府人员和管理人员关注的目标。

除第 1 章概述外, 本书可分三大篇。第 1 篇包括第 2~10 章, 是电子商务安全基础篇, 主要概述电子商务所涉及的典型密码算法、数字签名技术、认证技术、密钥管理技术、网络安全技术、电子商务安全常用的安全协议标准和 PKI 技术、移动商务安全技术等。第 2 篇包括第 11 章, 是电子商务安全应用篇, 主要陈述电子商务安全在电子政务、企业信息化、社会信息化和社区信息化中的应用。第 3 篇包括第 12 章和第 13 章, 是电子商务安全解决篇, 主要陈述国内外大公司的种种实际的安全解决方案和各种安全产品的采购策略, 具有可操作性。

本书具有如下特点:

(1) 每章开头有生动活泼的引例, 引人入胜。

(2) 内容丰富, 知识系统全面, 既有密码基础知识、网络基础知识, 又有安全协议标准、社会安全基础设施等方方面面的电子商务安全知识,



使读者对电子商务安全有一个完整的认识。

(3) 系统性强而不复杂,对基础技术点到为止,既避免涉及复杂的密码和网络理论,又较完整地介绍了基础知识,使读者对电子商务安全有一个深层次的理解。

(4) 内容新颖,跟踪了当前电子商务发展的许多热点,如PKI、安全电子支付、移动商务安全、电子政务安全和企业信息化安全等。

(5) 实用性和可操作性强,对照书中的方案和方法,极易找出适合本单位、本部门需求的电子商务安全解决方案。

(6) 图例丰富,对较复杂的概念、过程、原理等配有图解,便于讲解和自学。

(7) 章末附有习题,便于教学,同时习题生动活泼、意味深长,使读者乐于思考。

(8) 使用本书的教师可以经由出版社确认向作者获取电子讲稿。

本书观点新颖,论述深入浅出,内容丰富,可读性和实践性强,章末附有习题,特别适合作为电子商务专业、计算机应用专业和金融、营销等专业的教材,也可作为计算机或电子商务领域的研究人员和专业技术人员的参考书。

本书由华南理工大学出版社组织编写,经广东省许多大学教授、专家讨论而定。

本书第1、3、4、8、9、10章由肖德琴编写,第2章和第5章由广州大学周权编写,第6、7章由华南农业大学刘才兴和肖德琴合作编写,第11章由华南农业大学肖德琴和华南理工大学祁明合作编写,第12章由肖德琴和厦门大学彭丽芳合作编写,第13章由彭丽芳编写。全书的习题由肖德琴、祁明、康敏、阳文、李坚超和郭艾侠共同提供,引例由郭艾侠和肖德琴共同提供。

本书涉及面较广,同时因为作者水平有限,疏漏之处在所难免,恳请读者批评指正。有关意见请发电子邮件至 [deqinx@21cn.com](mailto:deqinx@21cn.com),不胜感激!

编者

2003年6月

# 目 录

1 电子商务安全概述 .....	1
引例：电子商务发展的主要障碍是什么？ .....	1
本章要点 .....	1
1.1 电子商务安全概况 .....	2
1.1.1 电子商务安全概念与特点 .....	2
1.1.2 电子商务面临的安全威胁 .....	3
1.1.3 电子商务的安全需求 .....	5
1.2 电子商务安全基础 .....	7
1.2.1 电子商务安全基础技术 .....	7
1.2.2 电子商务安全体系结构 .....	8
1.2.3 电子商务安全服务规范 .....	9
1.3 电子商务安全与其他领域的交融 .....	10
1.3.1 政务信息化 .....	11
1.3.2 社会信息化 .....	11
1.3.3 企业信息化 .....	12
1.3.4 社区信息化 .....	12
本章小结 .....	13
思考与练习 .....	13
2 现代加密技术 .....	14
引例：秘密是一种力量 .....	14
本章要点 .....	14
2.1 加密技术概述 .....	15
2.1.1 密码基本概念 .....	15
2.1.2 密码技术的分类 .....	16
2.1.3 密码系统的设计原则 .....	17
2.2 分组密码体制 .....	18
2.2.1 数据加密标准 (DES) .....	18
2.2.2 国际数据加密算法 (IDEA) .....	23
2.2.3 高级加密标准 (AES) .....	24
2.3 公开钥密码体制 .....	29



2.3.1	公开密钥密码系统原理	30
2.3.2	RSA 加密系统	31
2.3.3	ElGamal 加密系统	33
2.3.4	椭圆曲线加密体制	33
2.4	非数学的加密理论与技术	36
2.4.1	信息隐藏	36
2.4.2	生物识别	37
2.4.3	量子密码	38
	本章小结	40
	思考与练习	40
3	数字签名技术	42
	引例：中国首例电子邮件案	42
	本章要点	42
3.1	数字签名概述	43
3.1.1	数字签名的概念和特点	43
3.1.2	数字签名方案的分类	45
3.1.3	数字签名使用模式	45
3.1.4	数字签名使用原理	46
3.2	常规数字签名方法	47
3.2.1	RSA 数字签名系统	47
3.2.2	Hash 签名	48
3.2.3	美国数字签名标准 (DSA)	50
3.2.4	椭圆曲线数字签名算法 (ECDSA)	52
3.3	特殊数字签名方法	53
3.3.1	盲签名	53
3.3.2	双联签名	54
3.3.3	团体签名	54
3.3.4	不可争辩签名	55
3.3.5	多重签名方案	55
3.3.6	数字时间戳	56
3.4	数字签名法律	57
3.4.1	数字签名法律的内涵	57
3.4.2	电子签名立法原则	58
3.4.3	全球电子签名立法特点	59
3.4.4	我国电子签名立法现状	60



08	本章小结 .....	60
04	思考与练习 .....	61
4	<b>身份认证技术</b> .....	62
20	引例：认证的信任危机 .....	62
80	本章要点 .....	62
40	<b>4.1 消息认证</b> .....	63
80	4.1.1 消息认证的概念 .....	63
00	4.1.2 消息认证的方法 .....	63
80	4.1.3 消息认证的模式 .....	64
80	4.1.4 认证函数 .....	65
80	<b>4.2 身份认证的方法</b> .....	69
00	4.2.1 身份认证的概念 .....	69
00	4.2.2 口令认证 .....	70
001	4.2.3 持证认证 .....	72
001	4.2.4 生物识别 .....	72
10	<b>4.3 身份认证协议</b> .....	73
501	4.3.1 一次一密机制 .....	73
501	4.3.2 X.509 认证协议 .....	74
101	4.3.3 Kerberos 认证协议 .....	75
001	4.3.4 零知识身份识别 .....	75
50	本章小结 .....	76
01	思考与练习 .....	77
5	<b>密钥管理技术</b> .....	78
11	引例：管好你的“钥匙” .....	78
51	本章要点 .....	78
01	<b>5.1 概述</b> .....	79
21	<b>5.2 密钥管理</b> .....	80
811	5.2.1 对称密钥管理 .....	80
511	5.2.2 公开密钥管理 .....	81
511	5.2.3 第三方托管技术 .....	84
51	<b>5.3 密钥交换协议</b> .....	85
811	5.3.1 Diffie-Hellman 密钥交换协议 .....	85
811	5.3.2 Internet 密钥交换协议 (IKE) .....	86
051	5.3.3 因特网简单密钥交换协议 (SKIP) .....	88
151	5.3.4 秘密共享协议 .....	88



5.3.5	量子密钥分配 BB84 协议	89
5.4	PGP 密钥管理技术	89
5.4.1	PGP 的安全机制	90
5.4.2	PGP 的密钥	92
5.4.3	PGP 公钥管理系统	93
5.4.4	PGP 软件使用简介	94
	本章小结	96
	思考与练习	96
6	互联网安全技术	98
	引例：互联网安全状况令人担忧	98
	本章要点	98
6.1	网络安全基础	99
6.1.1	网络安全的定义	99
6.1.2	网络安全服务内涵	100
6.1.3	网络安全防范机制	100
6.1.4	网络安全关键技术	101
6.2	防火墙技术	102
6.2.1	防火墙的功能特征	102
6.2.2	防火墙的基本类型	104
6.2.3	防火墙的基本技术	106
6.2.4	防火墙的配置结构	107
6.2.5	防火墙的安全策略	110
6.3	VPN 技术	111
6.3.1	VPN 的功能特征	111
6.3.2	VPN 的基本类型	112
6.3.3	VPN 的基本技术	113
6.3.4	VPN 的配置结构	115
6.3.5	VPN 的安全策略	116
6.4	网络入侵检测	117
6.4.1	入侵检测系统的概念	117
6.4.2	入侵检测系统的原理	117
6.4.3	入侵检测系统的分类	118
6.4.4	入侵检测的主要方法	118
6.4.5	入侵检测系统的实现步骤	120
	本章小结	121



思考与练习	122
<b>7 安全防范与对策</b>	123
引例：全美最大的电脑流氓落网	123
本章要点	125
<b>7.1 安全防范策略概述</b>	125
7.1.1 安全防范策略制定原则	126
7.1.2 安全防范策略制定步骤	126
7.1.3 安全防范策略的基本内容	127
<b>7.2 物理安全防范</b>	128
7.2.1 机房环境安全	128
7.2.2 电磁防护	130
7.2.3 硬件防护	130
<b>7.3 访问权限控制</b>	130
<b>7.4 黑客防范策略</b>	132
7.4.1 黑客攻击行为分析	133
7.4.2 黑客入侵的步骤	134
7.4.3 黑客攻击的原理和方法	135
7.4.4 黑客攻击常用工具	137
7.4.5 黑客防范措施	138
<b>7.5 风险管理</b>	140
7.5.1 风险管理的步骤	140
7.5.2 风险评估	142
7.5.3 风险管理对策	142
7.5.4 风险管理工具	144
<b>7.6 灾难恢复</b>	145
7.6.1 灾难恢复概念	145
7.6.2 灾难恢复策略	145
7.6.3 灾难恢复系统	147
本章小结	150
思考与练习	150
<b>8 安全协议与安全标准</b>	152
引例：匿名汇票“双重花费”问题	152
本章要点	152
<b>8.1 商务安全协议概述</b>	153
<b>8.2 安全套接层协议</b>	153



8.2.1	SSL 协议提供的安全服务	153
8.2.2	SSL 协议的运行步骤	154
8.2.3	SSL 协议的体系结构	155
8.2.4	SSL 协议的安全措施	157
8.2.5	Windows 2000 中 SSL 协议的配置与应用	159
8.3	安全电子交易规范	161
8.3.1	SET 协议提供的安全服务	161
8.3.2	SET 协议的运行步骤	162
8.3.3	SET 协议的体系结构	162
8.3.4	SET 协议的安全措施	163
8.3.5	SET 协议和 SSL 协议的比较	165
8.4	电子支付专用协议	166
8.4.1	NetBill 协议	167
8.4.2	First Virtual 协议	167
8.4.3	iKP 协议	168
8.5	安全超文本传输协议	169
8.5.1	S-HTTP 协议概述	169
8.5.2	SSL 与 S-HTTP 的比较	170
8.6	安全电子邮件协议	171
8.6.1	保密增强邮件 (PEM)	171
8.6.2	安全多功能 Internet 电子邮件扩充 (S/MIME)	171
8.6.3	Outlook Express 下的安全电子邮件传送	172
8.7	Internet 电子数据交换协议	174
8.7.1	EDI 消息处理原理	175
8.7.2	EDI 系统面临的安全威胁	176
8.7.3	EDI 系统的安全策略	177
8.7.4	Internet EDI 安全服务的实现	178
8.8	IP <sub>Sec</sub> 安全协议	178
8.8.1	IP <sub>Sec</sub> 组成	179
8.8.2	IP <sub>Sec</sub> 的工作原理	179
8.8.3	IP 认证协议	180
8.8.4	IP 安全封装负载协议 (ESP)	182
8.8.5	Windows 2000 的 IP <sub>Sec</sub> 策略	183
8.9	安全技术评估标准	185
	本章小结	186



01	思考与练习	186
9	公钥基础设施与应用	188
11	引例：电子商务安全，怎么迈过这道槛？	188
11	本章要点	188
9.1	公钥基础设施概述	189
9.1.1	PKI 的基本概念	189
9.1.2	PKI 的功能与特性	190
9.1.3	PKI 的基本组成	190
9.1.4	PKI 加密/签名原理	191
9.2	PKI 系统的常用信任模型	192
9.2.1	认证机构的严格层次结构模型	192
9.2.2	分布式信任结构模型	193
9.2.3	Web 模型	194
9.2.4	以用户为中心的信任模型	195
9.3	PKI 管理机构——认证中心	195
9.3.1	CA 的功能	196
9.3.2	CA 的组成	197
9.3.3	CA 体系结构	197
9.4	PKI 核心产品——数字证书	197
9.4.1	数字证书的概念	198
9.4.2	X.509 证书类型	198
9.4.3	数字证书功能	199
9.4.4	证书格式	200
9.4.5	证书管理	200
9.4.6	数字证书应用实例	202
9.5	中国 PKI 战略发展与应用	203
9.5.1	中国 PKI 体系建设现状	203
9.5.2	国家 PKI 基本目标及指导思想	204
9.5.3	国家 PKI 的体系框架	204
9.5.4	当前 PKI 建设的主要工作	206
9.6	国际 PKI 发展现状	207
9.6.1	亚洲 PKI 发展现状	208
9.6.2	西方各国 PKI 发展现状	212
9.6.3	国外著名 PKI 厂商、产品	214
9.7	Windows 2000 的 PKI/CA 结构	214



本章小结	216
思考与练习	216
<b>10 移动商务安全与应用</b>	<b>217</b>
引例：安全性：移动商务的又一道槛	217
本章要点	217
10.1 移动商务安全概述	218
10.1.1 移动商务安全目标	218
10.1.2 移动数据安全的基本措施	219
10.1.3 移动终端安全及其防护措施	221
10.2 移动安全协议和标准	224
10.2.1 蓝牙标准	224
10.2.2 无线应用协议（WAP）和无线传输层	226
10.2.3 无线 PKI	229
10.2.4 Mobile 3-D Secure 标准	229
10.2.5 无线网络标准 IEEE 802.11b	230
10.3 移动系统安全	231
10.3.1 移动支付系统安全方案	231
10.3.2 GSM 安全	234
10.3.3 3G 系统的安全体系	234
本章小结	240
思考与练习	240
<b>11 电子政务与企业信息化安全</b>	<b>241</b>
引例：世界各国各行各业纷纷加大网络安全投资	241
本章要点	241
11.1 电子政务安全	242
11.1.1 电子政务安全概述	242
11.1.2 电子政务的信息安全目标	244
11.1.3 电子政务的信息安全机制	244
11.1.4 电子政务安全框架	245
11.2 社会信息化安全	248
11.2.1 社会信息化安全概述	248
11.2.2 金融信息化与安全	249
11.2.3 网上证券交易与安全	251
11.2.4 电信信息化与安全	251
11.2.5 电力行业信息化与安全	253



11.2.6	居民身份证与安全	254
11.2.7	公安信息化与安全	255
11.3	企业信息化安全	255
11.3.1	企业信息化安全需求概述	256
11.3.2	企业信息化安全现状	258
11.3.3	企业网络安全策略	258
11.3.4	企业信息安全策略的核心	259
11.3.5	中小企业安全管理实施方案	261
11.4	社区信息化安全	261
11.4.1	社区信息化安全概述	262
11.4.2	社区信息化安全特点	263
11.4.3	社区信息化安全需求	263
11.4.4	小区安全防范框架体系	263
	本章小结	265
	思考与练习	265
12	电子商务安全解决方案	267
	引例：面对众多的安全解决方案：何去何从？	267
	本章要点	267
12.1	国外公司电子商务安全解决方案	268
12.1.1	IBM公司OA数据安全解决方案	268
12.1.2	CA公司的eTrust企业管理安全解决方案	279
12.1.3	CISCO公司解决方案（SAFE 蓝图）	282
12.1.4	3Com公司无线网络安全解决方案	288
12.1.5	爱立信 Mobile e-Pay 解决方案	291
12.1.6	美国联邦 PKI 解决方案	295
12.1.7	加拿大政府 PKI 解决方案	298
12.2	国内公司电子商务安全解决方案	299
12.2.1	国瑞数码公司的电子商务安全平台解决方案	299
12.2.2	清华得实公司的 WebST BtoB 安全解决方案	301
12.2.3	广东电子商务认证中心银行信息化安全解决方案	309
12.2.4	中国金融认证中心（CFCA）的 CA 解决方案	312
12.2.5	联想电子政务安全解决方案	316
12.2.6	华为电子政务安全解决方案	318
12.2.7	华为“i <sup>3</sup> 安全”端到端安全解决方案	322
	本章小结	326