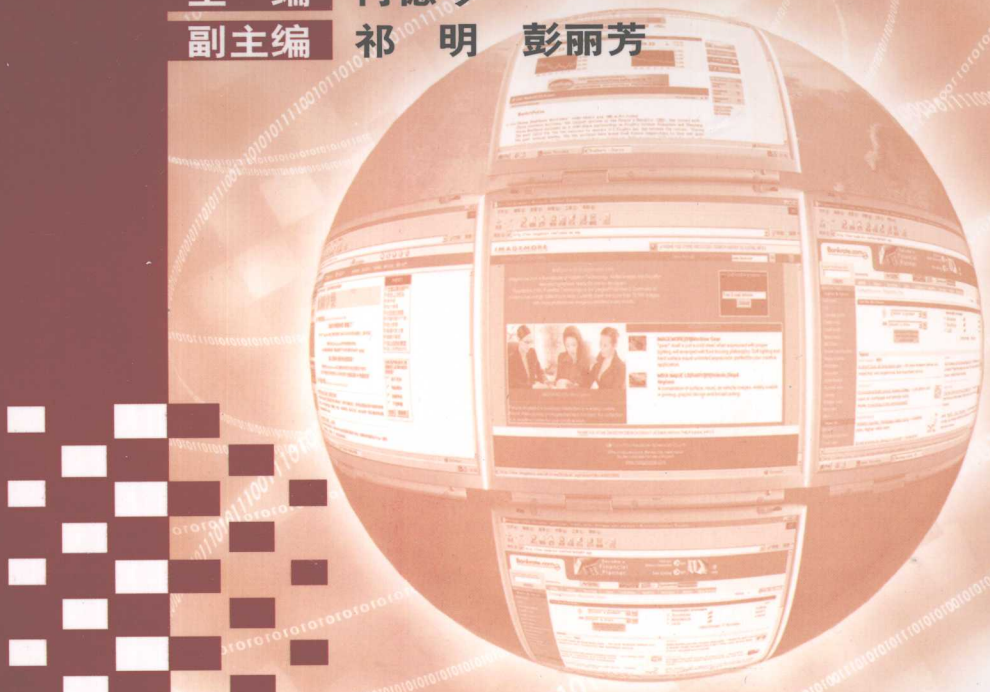
21世纪电子商务系列教材
全国高等院校电子商务联编教材

电子商务安全保密技术与应用

Security Technology and Application on E-Commerce

(第二版)

主　编　肖德琴
副主编　祁　明　彭丽芳



華南理工大學出版社

电子商务安全保密技术与应用

（第二版）

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. —2版 .—广州：华南理工大学出版社，2008.8

（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

ISBN 978-7-5623-2893-3

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（2008）第118482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）

营销部电话：020-87113487 87110964 87111048（传真）

E-mail：z2cb@scut.edu.cn **http**：//www.scutpress.com.cn

责任编辑：詹志青

印 刷 者：广东省农垦总局印刷厂

开 本：787mm×960mm 1/16 **印张**：23 **字数**：510千

版 次：2008年8月第2版 2008年8月第5次印刷

印 数：14001～17000册

定 价：38.00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(广东外语外贸大学)	赵　波(广州大学)
胡蠡明(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大趋势。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、形势迫人。

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、技术和安全上，还是在实施、应用和管理中，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，尤其是综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。

此为试读，需要完整PDF请访问：www.ertongbook.com

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

第二版前言

电子商务正在改变着人们的工作方式和生活方式，电子商务的发展与应用业已成为影响一个国家和地区政治、经济、科学与文化发展的重要因素之一。基于网络技术的电子政务、电子商务、远程教育、远程医疗和信息安全技术正以前所未有的速度发展。电子商务安全保密技术是当今电子商务领域发展最为迅速的技术之一，也是电子商务应用中一个空前活跃的领域。

我国电子商务产业的发展，需要大批掌握电子商务技术与安全技术的人才，因此，电子商务安全技术已经成为计算机专业、电子商务专业、经济管理专业及其他相关专业学生学习的一门重要课程，也是从事电子商务应用与信息技术研究、应用的专业技术人员应该掌握的重要知识。

作者在多年的教学实践中深刻地体会到，在课程教学中需要注意两方面的问题：一是教学内容的系统性，二是如何在教材的组织中反映不断出现的新技术。根据作者多年从事本科生、研究生电子商务与安全保密课程教学实践与科研工作的经验，结合电子商务技术的最新发展，对本教材作较大规模的修订，希望为广大读者提供一本既保持知识的系统性、又能反映当前电子商务安全技术发展最新成果，概念准确，层次清晰，易于学习的教材。

第二版依然保留从原理到技术再到应用的组织体系结构，同时，更加突出了以密码学为基础、以网络安全为载体、以社会安全为目标，注重电子商务安全发展最新成果的宗旨，并增加了许多新技术的介绍，例如，电子商务安全的认证识别技术、防病毒技术、电子商务安全管理、电子商务安全策略、电子商务安全立法、应急响应、PKI 应用方案、PKI 服务新技术、电子商务安全标准研究进展等方面的内容模块。此外，根据当前电子商务安全技术解决方案和产品的最新进展，对案例和产品部分进行了全新改写。同时，为了不使全书篇幅过于膨胀，删除了一些目前离电子商务应用较远的、较陈旧的次要内容。

本书的第 1、3、4、6、7、8 章由肖德琴编写，第 2、5、10 章由广州

大学周权编写，第9章由华南农业大学冯健昭改编，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、13章由周权和厦门大学彭丽芳合作编写。全书的习题由肖德琴、祁明、康敏、阳文、李坚超、冯健昭和郭艾侠共同提供，引例由郭艾侠、冯健昭和肖德琴共同提供。本次修订得到了武汉大学张焕国和王丽娜教授、华南农业大学杨波教授和张明武副教授的指导和帮助，在此一并表示感谢。

面对电子商务安全技术日益更新和迅速发展，要完成这样一个高标准的写作任务，编者感到压力很大。限于作者的学术水平，书中难免有错误与不妥之处，诚恳地希望读者批评指正。对使用本书第一版并提出宝贵意见和建议的老师们深表感谢，也请诸位继续关注和指教。我们衷心希望得到读者（尤其是广大的同学与老师）的支持与帮助，共同探讨电子商务安全课程教学体会，共同提高我国电子商务安全课程的教学水平。

为方便教学和交流，选用本教材的教师们可发电子邮件至 deqin.x@163.com 索取电子讲稿或提出对本书的意见和建议，不胜感激！

编　者

2008年8月

前　言

随着信息网络技术 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、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。可发电子邮件至deqinx@21cn.com索取电子讲稿或提出对本书的意见和建议，不胜感激！

编 者

2003年6月

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

此为试读，需要完整PDF请访问：www.ertongbook.com