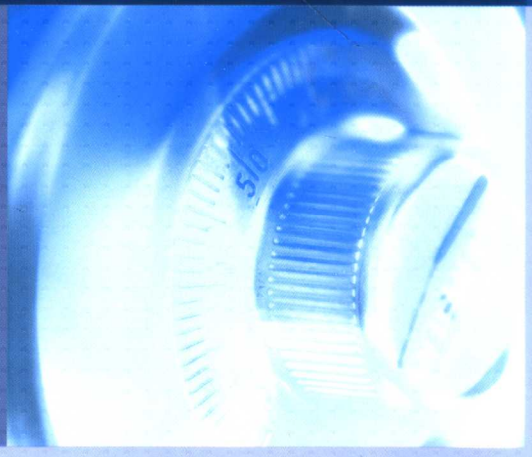
普通高等教育“十一五”国家级规划教材

电子商务安全与保密

(第2版)

□ 祁 明 主编



高等教育出版社
Higher Education Press

普通高等教育“十一五”国家级规划教材

电子商务安全与保密

（第2版）

祁　明　主　编
毕凌燕　左文明　许伯桐　编　著

高等教育出版社

图书在版编目(CIP)数据

电子商务安全与保密／祁明主编．—2版.—北京：高等教育出版社，2006.12

ISBN 7-04-020228-X

Ⅰ.电... Ⅱ.祁... 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(2006)第131134号

策划编辑 韩 飞 **责任编辑** 贺 玲 **封面设计** 王凌波 **责任绘图** 朱 静
版式设计 张 岚 **责任校对** 殷 然 **责任印制** 陈伟光

出版发行	高等教育出版社	**购书热线**	010－58581118
社　　址	北京市西城区德外大街4号	**免费咨询**	800－810－0598
邮政编码	100011	**网　　址**	http://www.hep.edu.cn
总　　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	北京宝旺印务有限公司	**畅想教育**	http://www.widedu.com
		版　　次	2001年7月第1版
开　　本	787×1092　1/16		2006年12月第2版
印　　张	34	**印　　次**	2006年12月第1次印刷
字　　数	710 000	**定　　价**	35.10元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　20228－00

内 容 简 介

本书是在第一版同名教材使用五年的基础上修订而成的，在保持原有基本体系结构的同时，添加了许多电子商务安全发展的新理论、新技术和新案例。本书比较系统地介绍了电子商务安全保密的基本理论和实用技术，既简明扼要地介绍了国内外的前沿研究成果，又详细介绍了电子商务中迫切需要的安全保密知识。

本书共分 18 章，涉及的范围比较广泛，主要内容有：电子商务安全的现状与趋势、信息论与数学基础、信息加密技术与应用、数字签名技术与应用、身份认证与访问控制、密钥管理与 PKI 体系、WWW 与 Web 服务安全、防火墙的构造与选择、计算机病毒的产生与防治、安全通信协议与交易协议、网络攻击与防御、信息隐藏与数字水印、电子邮件安全协议与系统设计、移动通信系统安全、反计算机犯罪与网上版权保护、计算机软件综合保护方法、系统评估准则与安全策略、计算机信息系统安全保护制度。

本书的习题有三种类型：复习题、思考题和上网题。这些练习使得老师能够根据学生的背景和需求灵活地调整练习难度和深度，同时也使得学生在掌握基本的知识点之后，在学术研究、技术开发和创业方面更快捷地找到对应的热点话题和课题。

本书可作为高等院校电子商务、物流工程与管理、经济信息管理、计算机科学与技术、通信工程专业及相关专业本科生或研究生的电子商务安全教材，也可供从事电子商务研究和应用开发人员学习参考。

郑重声明

前　言

自计算机网络出现以来，网络的安全就成为网络使用者不得不面对的问题。如今，随着网络应用水平的提高和电子商务的大力开展，计算机系统的安全隐患也日渐突出，诸如高科技犯罪、机密泄露、黑客入侵、病毒侵扰等，其危害之严重、手段之高超令人惊异。

据美国联邦调查局 FBI 的调查，美国每年因为网络安全造成的经济损失超过 170 亿美元，大约 75%的公司的财政损失是由于计算机系统的安全问题造成的，但其中只有 17%的公司愿意报告遭受过黑客的袭击，而大部分公司由于担心负面影响而不愿声张。

中国的网络安全和电子商务安全情况并不乐观。最近，国家有关专家曾对国内多家网站的安全性能做了测试，结果令人震惊——在测试的网站中有近 90%的网站存在着不同程度的安全隐患。黑客攻击网站的例子举不胜举，如新浪网、中国公众多媒体信息网、国家统计局网站等。总之，互联网与电子商务的安全问题已经引起了人们的担忧，各国政府、IT 厂商和业界同仁在感到震惊的同时，也开始积极思考对策和提供针对不同需求的解决方案。

为了普及计算机网络和电子商务的安全保密技术，推进我国信息安全产业的发展，增进与国内外同行之间的交流，我们编著了这本教材。

本书四位作者都来自华南理工大学电子商务学院。全书由祁明担任主编，其中第 1～4 章和第 17、18 章由祁明编写，第 8、9、14、15 章由毕凌燕编写，第 5、12、13、16 章由左文明编写，第 6、7、10、11 章由许伯桐编写。

在写作过程中，作者试图从理论和实践相结合的角度较系统地介绍电子商务安全保密的基本理论和实用技术。既介绍国内外的前沿研究成果，又介绍目前已经成熟的实用技术；既注重介绍安全保密的基本概念和算法，又照顾到学习电子商务课程学生来源的广泛性、知识背景的多样性和要求的多层次性。尽管作者有以上初衷，但因学术水平有限和篇幅所限，许多与电子商务有关的安全保密技术未能介绍或介绍得不够全面。另外，本书编校虽力求完美，然而谬误之处在所难免，对此，作者恳请读者的理解和批评指正。

本书是作者在 2001 年第一版教材五年多教学和研究的基础上修改而成的。作者在写作过程中参阅了大量的国内外资料，在此谨向书中所提到的和参考文献所列出的各位作者表示衷心的感谢。

本书的编写和有关研究工作还得到了高等教育出版社的热情关心和支持，在此我们深表谢意！

编　者

2006 年 7 月于广州

目　录

第 1 章　电子商务安全的现状与趋势

电子商务已成为业界的新热点，但我国大多数电子商务系统只是在一般 Web 站点的基础上增加了简单的产品目录和订购单。这种比较初级的电子商务系统因还没有与内部网连接，也就没有涉及太多的安全问题。然而，随着信息化进程的深入，它们即将被新的、真正的电子商务系统所取代，即 Web 站点与公司的后端数据库系统相连接，这样就可以向客户提供有关产品的库存、发货情况以及账款状况的实时信息。这种充分集成的电子商务系统可以向客户提供只能通过 Web 才能得到的重要服务，同时还可以帮助商家实现业务处理的流水化。由于这种新的完整的电子商务系统可以将内部网与 Internet 连接，使小到本企业的商业机密、商务活动的正常运转，大至国家的政治、经济机密都将面临网上黑客与病毒的严峻考验。这样，安全问题便成了电子商务系统的首要问题。

目前，影响 Internet 交易的最大阻力是交易安全，使用者担心在网络上传输的信用卡及个人资料信息被截取，或是不幸遇到“黑店”，信用卡资料被不正当运用。另一方面，特约商店也担心收到的是被盗用的信用卡号码，或是交易不认账等，还有可能因网络不稳定或是应用软件设计不良导致被黑客侵入所引发的损失。由于在消费者、特约商店，甚至与金融单位之间的权责关系还未理清，以及每一家电子商场或商店的支付系统所使用的安全控管机制不一致等问题，都会造成使用者有无所适从的感觉。以上种种令不少对 Internet 网有兴趣的购物者因担忧安全而犹豫不前。因此，电子商务顺利开展的核心和关键问题是保证交易的安全性，这是网络交易的基础，也是电子商务技术的难点所在。

本章着重介绍电子商务系统安全的基本概念、安全性的基本要求、国内外电子商务安全技术的发展和实际应用状况。

1.1　电子商务安全概述

1.1.1　电子商务安全结构与要求

1. 安全性定义

在给安全性下一个详细的定义前，通常需要先定义一系列新的术语。为了理解本章所述各种安全性的含意，有必要先了解以下术语：

（1）密码安全

通信安全的最核心部分，由技术上提供强韧的密码系统及其正确应用来实现。

（2）计算机安全

一种确定的状态，使计算机化数据和程序文件不致被非授权人员、计算机或其他程序所访问、获取或修改。安全的实施可通过限制被授权人员使用计算机系统的物理范围、利用特殊（专用）软件和将安全功能构造于计算机操作规程中等方法来实现。

（3）网络安全

包括所有保护网络的措施：物理设施的保护、软件及职员的安全，以防止非授权的访问、偶发或蓄意的常规手段的干扰或破坏。因此，有效的安全措施是技术与人事管理的一种均衡或合理配合。

（4）信息安全

保护信息财富，使之免遭偶发的或有意的非授权泄露、修改、破坏。

以上几类安全性之间的关系，可用图 1.1 所示的安全环表示。

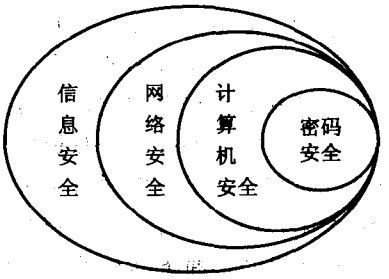


图 1.1　安全环

2．电子商务安全的基本要求

表 1.1 列出了电子商务所需的七种安全性要求。其中，保密性、完整性和不可否认性最为关键。

表 1.1　网络安全性要求

术　语	定　义
保密性	保障个人的、专用的和高度敏感数据的机密
认证性	确认通信双方的合法身份
完整性	保证所有存储和管理的信息不被篡改
可访问性	保证系统、数据和服务能被合法地访问
防御性	能够阻挡不希望的信息或黑客
不可否认性	防止通信或交易双方对已进行业务的否认
合法性	保证各方的业务符合可适用的法律和法规

1.1.2　电子商务安全案例与分析

近年来，随着网络技术和电子商务的迅猛发展，人们在网络上购买书、日用品、计算机或是进行房产交易、股票炒作、资金运作等活动剧增，随之而来的网络安全问题日益引起人们的关注。

2004 年 9 月，浙江某大学计算机系学生谢某因在网上开设“91See”影院网站并提供