21世纪大学本科
计算机专业系列教材

阙喜戎 孙锐
龚向阳 王纯 编著

信息安全原理及应用

http://www.tup.com.cn

- 根据教育部高教司主持评审的《中国计算机科学与技术学科教程 2002》组织编写
- 与美国 ACM 和 IEEE/CS《Computing Curricula 2001》同步

清华大学出版社

21世纪大学本科计算机专业系列教材

信息安全原理及应用

阙喜戎 孙锐
龚向阳 王纯 编著

清华大学出版社
北京

内 容 简 介

本书重点介绍：密码学理论基础（信息理论基础、复杂性理论基础）；主要的加密算法及其理论基础（密码学的技术实现）；密码协议和安全协议（密码学的实际运用）；常用的系统安全技术和网络安全技术（实用技术）。本书从理论到技术实现和实际运用等方面对信息安全进行了全面的阐述，强调通过技术实现和实际运用加深对理论的理解，并且反过来为技术实现和实际运用提供指导。

本书深入而全面地探讨了信息安全领域人们关心的问题和相应的解决途径；注重运用常用的一些系统安全技术和网络安全技术在具体实践中保护网络信息系统的安全，解决实际问题。

本书可作为高等院校有关专业本科生和研究生的教材，也可作为通信工程师、计算机网络工程师和软件工程师的参考读物。

图书在版编目(CIP)数据

信息安全原理及应用/阙喜戎，孙锐，龚向阳，王纯编著. —北京：清华大学出版社，2003
(21世纪大学本科计算机专业系列教材)
ISBN 7-302-06551-9

Ⅰ.信… Ⅱ.①阙… ②孙… ③龚… ④王… Ⅲ.信息系统—安全技术—高等学校—教材 Ⅳ.TP309

中国版本图书馆CIP数据核字(2003)第027068号

出 版 者：清华大学出版社（北京清华大学学研大厦，邮编100084）
http://www.tup.com.cn
责任编辑：张瑞庆 徐跃进
印 刷 者：清华大学印刷厂
发 行 者：新华书店总店北京发行所
开 本：787×960 1/16 **印张**：23.5 **字数**：535千字
版 次：2003年7月第1版 2003年7月第1次印刷
书 号：ISBN 7-302-06551-9/TP·4908
印 数：0001～6000
定 价：29.80元

序言

21世纪是知识经济的时代，是人才竞争的时代。随着21世纪的到来，人类已步入信息社会，信息产业正成为全球经济的主导产业。计算机科学与技术在信息产业中占据了最重要的地位，这就对培养21世纪高素质创新型计算机专业人才提出了迫切的要求。

为了培养高素质创新型人才，必须建立高水平的教学计划和课程体系。在20多年跟踪分析ACM和IEEE计算机课程体系的基础上，紧跟计算机科学与技术的发展潮流，及时制定并修正教学计划和课程体系是尤其重要的。计算机科学与技术的发展对高水平人才的要求，需要我们从总体上优化课程结构，精炼教学内容，拓宽专业基础，加强教学实践，特别注重综合素质的培养，形成“基础课程精深，专业课程宽新”的格局。

为了适应计算机科学与技术学科发展和计算机教学计划的需要，要采取多种措施鼓励长期从事计算机教学和科技前沿研究的专家教授积极参与计算机专业教材的编著和更新，在教材中及时反映学科前沿的研究成果与发展趋势，以高水平的科研促进教材建设。同时适当引进国外先进的原版教材。

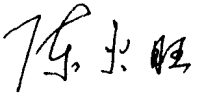
为了提高教学质量，需要不断改革教学方法与手段，倡导因材施教，强调知识的总结、梳理、推演和挖掘，通过加快教案的不断更新，使学生掌握教材中未及时反映的学科发展新动向，进一步拓广视野。教学与科研相结合是培养学生实践能力的有效途径。高水平的科研可以为教学提供最先进的高新技术平台和创造性的工作环境，使学生得以接触最先进的计算机理论、技术和环境。高水平的科研还可以为高水平人才的素质教育提供良好的物质基础。学生在课题研究中不但能了解科学研究的艰辛和科研工作者的奉献精神，而且能熏陶和培养良好的科研作风，锻炼和培养攻关能力和协作精神。

进入21世纪，我国高等教育进入了前所未有的大发展时期，时代的进步与发展对高等教育质量提出了更高、更新的要求。2001年8月，教育部颁发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》。文件指出，本科教育是高等教育的主体

和基础，抓好本科教学是提高整个高等教育质量的重点和关键。随着高等教育的普及和高等学校的扩招，在校大学本科计算机专业学生的人数将大量上升，对适合21世纪大学本科计算机科学与技术学科课程体系要求的，并且适合中国学生学习的计算机专业教材的需求量也将急剧增加。为此，中国计算机学会和清华大学出版社共同规划了面向全国高等院校计算机专业本科生的**"21世纪大学本科计算机专业系列教材"**。本系列教材借鉴美国ACM和IEEE/CS最新制定的《Computing Curricula 2001》(简称CC2001)课程体系，反映当代计算机科学与技术学科水平和计算机科学技术的新发展、新技术，并且结合中国计算机教育改革成果和中国国情。

中国计算机学会教育专业委员会和全国高等学校计算机教育研究会，在清华大学出版社的大力支持下，跟踪分析CC2001，并结合中国计算机科学与技术学科的发展现状和计算机教育的改革成果，研究出了《中国计算机科学与技术学科教程2002》(China Computing Curricula 2002，简称CCC2002)，该项研究成果对中国高等学校计算机科学与技术学科教育的改革和发展具有重要的参考价值和积极的推动作用。

"21世纪大学本科计算机专业系列教材"正是借鉴美国ACM和IEEE/CS CC2001课程体系，依据CCC2002基本要求组织编写的计算机专业教材。相信通过这套教材的编写和出版，能够在内容和形式上显著地提高我国计算机专业教材的整体水平，继而提高我国大学本科计算机专业的教学质量，培养出符合时代发展要求的具有较强国际竞争力的高素质创新型计算机人才。



中国工程院院士
国防科学技术大学教授
21世纪大学本科计算机专业系列教材编委会名誉主任
2002年7月

前　言

计算机系统和信息的安全问题很早就已经存在，例如大家所熟知的计算机病毒问题就是一个典型的例子。随着社会进入信息化时代，由于互联网的开放性，计算机和信息的安全问题将更加突出。而且，随着网络使用者和网上应用的增加，特别是电子商务所涉及的金额不断提高，网络和连接在网络上的信息系统已经开始面临各种复杂的、严峻的安全威胁。为了维护信息化社会的有序运作，需要大量的基础扎实、技术过硬的网络信息安全人才。针对这种情况，大多数高等院校陆续开设了信息安全原理及应用方面的课程，社会上各类继续教育机构也纷纷开展了网络信息安全方面的培训。作者在从事信息安全原理及应用相关课程的教学时，一直没有找到很合适的教材。恰逢中国计算机学会组织编写“21世纪大学本科计算机专业系列教材”，于是根据密码学和计算机网络安全的新发展和新趋势，结合平时的教学体会和学生反馈，编写了此书。

信息安全是一个综合的、交叉的学科领域，涉及数学、信息、通信和计算机等诸多学科的长期知识积累和最新发展成果。本书主要阐述现代密码技术的原理及其在信息系统安全中的应用，重点内容包括：密码学的理论基础（信息理论基础、复杂性理论基础）；加密算法及其理论基础（密码学的技术实现）；密码协议和安全协议（密码学的实际运用）；常用的一些系统安全技术和网络安全技术（实用技术）。希望读者在阅读本书后，能够认识网络信息安全领域人们关心的问题和相应的解决途径；对信息安全的关键技术——密码学，应从理论要求、技术实现和实际运用等方面有一个较全面的了解；并能运用常用的一些系统安全技术和网络安全技术在具体实践中保护网络信息系统的安全，解决实际问题。

全书共分12章。在教学安排时，可根据学时及学生基础安排学习本书的全部或部分章节。同时，本书也配备了相关的教学课件和材料，以便教师授课时选用。本书的第1、第10、第12章由阙喜戎编写，第2、第3、第4、第5、第6章由孙锐编写，第7章由王纯编写，第8、第9、第11章由龚向阳编写。阙喜戎负责全书的总体规划与内容组织，并对

全书进行了修改和定稿。

本书在编写过程中得到了“21 世纪大学本科计算机专业系列教材”编委会的指导，国际科技大学计算机学院宁洪教授认真地审阅了全书，并提出了许多宝贵意见；北京邮电大学计算机学院刘辰教授给予本书多方面的帮助；北京邮电大学交换技术与通信网国家重点实验室宽带网中心的领导和同事热情支持了本书的编写工作；清华大学出版社大力支持了本书的出版工作。此外，为了编著本书我们参考和吸收了国内外许多同行学者的研究成果，许多朋友都为此书付出了辛勤的劳动，在此一并表示衷心感谢。

随着技术的进步和需求的变化，信息安全技术还会不断地发展，我们希望得到各位读者的支持，也期待着与大家共同探讨信息安全技术的发展动向及相关课程的教学体会。由于我们水平有限，书中错误在所难免，欢迎读者批评指正。

作　者

于北京邮电大学计算机学院

rongqx@bupt.edu.cn

2003 年 1 月

目　录

CONTENTS

第 1 章 信息系统安全概述

信息技术的发展带动了全球信息化的发展，从而使信息基础设施成为社会基础设施中必不可少的关键基础设施，与此同时，网络信息系统的安全问题也逐渐引起人们的重视。不解决信息安全问题，不强化网络化的信息安全保障，信息化将得不到可持续的健康发展。

在现实应用中，信息系统已由传统意义上的存放和处理信息的独立系统演变为互相连接、资源共享的系统集合，也就是说，信息系统同时也是一个网络系统。此外信息安全是一个极大的技术领域，本书的侧重点在于网络中的信息安全，因此为叙述和理解方便，本书中信息系统也被称为网络信息系统。

本章首先分析安全问题的起因及信息系统面临的各种攻击，然后介绍网络信息系统的安全需求、安全服务及知名的安全评估标准，使大家对网络信息系统的安全问题有个大致的了解。鉴于加密技术在处理安全问题时的广泛应用，本章最后对加密功能的实施进行了探讨。

1.1 网络信息系统的脆弱性

所谓网络信息系统，是指互相连接起来的独立自主的计算机信息系统的集合。网络信息系统中的计算机能够方便地交换信息、共享资源。随着现代通信技术和计算机技术的不断发展，计算机网络的规模以前所未有的速度快速增长，信息共享应用日益广泛和深入。不难发现，以个人计算机(PC)为中心的计算方式，正在向以网络为中心的计算方式发展。

网络信息系统促使了科学、技术、文化、教育和生产的快速发展，为提高现代人的生活质量提供了极大的便利。随着网络经济和网络社会时代的到来，网络将会进入一个