高等院校信息与计算科学专业系列教材

信息安全与密码学

徐茂智　游林　编著

清华大学出版社

高等院校信息与计算科学专业系列教材

信息安全与密码学

徐茂智　游林　编著

清华大学出版社
北京

内 容 简 介

本书介绍信息安全与密码学的基础理论与基本应用。信息安全的核心是密码学，所以密码学也是本书的重点。全书由绪论、信息安全初步、信息安全技术、传统密码学、公钥密码算法、Hash 函数、计算复杂性理论、零知识证明与比特承诺、基于身份的公钥密码学、数字签名、密钥管理和密码学中的基本数学知识(附录)组成，共 11 章及一个附录。所涉及的内容基本上涵盖了现代密码学的基本概念、基本算法，以及信息安全的基本知识。附录是对数论基本知识，以及群、环、域等一些基本代数概念的简单介绍。本书每章均配有习题，便于检验和加深学生对所学内容的理解和掌握。

本书可作为数学、计算机科学、通信、电子工程等相关专业的本科高年级学生或研究生一个学期课程的教材或参考书。

图书在版编目(CIP)数据

信息安全与密码学 / 徐茂智，游林编著. --北京：清华大学出版社，2007.1
(高等院校信息与计算科学专业系列教材)
ISBN 978-7-302-13958-4

Ⅰ. 信… Ⅱ. ①徐…②游… Ⅲ ①信息系统－安全技术－高等学校－教材②密码－理论－高等学校－教材 Ⅳ ①TP309②TN918.1

中国版本图书馆 CIP 数据核字(2006)第 120358 号

责任编辑：范素珍
责任校对：白　蕾
责任印制：孟凡玉

出版发行：清华大学出版社　　**地　　址**　北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　　**邮购热线**：010-62786544
投稿咨询：010-62772015　　**客户服务**：010-62776969

印 刷 者：北京市清华园胶印厂
装 订 者：三河市春园印刷有限公司
经　　销：全国新华书店
开　　本：140×203　　**印　张**：9.25　　**字　数**：227 千字
版　　次：2007 年 1 月第 1 版　　**印　次**：2007 年 1 月第 1 次印刷
印　　数：1～4000
定　　价：17.00 元

高等院校信息与计算科学专业系列教材

编辑委员会名单

序　言

数学科学不仅是自然科学的基础，也是一切重要技术发展的基础。电子计算机的发明及计算技术的发展都以数学为其理论基础。计算机技术的发展使得数学的应用更加直接和广泛，同时也正在改变人们对数学的传统认识。数学素质已成为今天培养高层次创新人才的重要基础。

计算数学是一门随着计算机发展而形成的学科，研究如何应用计算机有效地求解各类计算问题的方法和理论，其中涉及的计算问题主要来源于科学研究和工程设计，因此人们又称这门学科为科学计算。今天，计算和实验、理论分析一起成为当今科学活动的主要方式。在物理、化学、力学、材料科学、环境科学、信息科学和生物科学等领域，计算方法和技术已经成为被广泛接受的科学研究手段，这一系列计算性的分支学科统称为计算科学。现在，计算在科学研究和工程设计中几乎无处不在，对科技的发展起到举足轻重的作用。由于计算数学的发展已有50多年的历史，在教学科研方面有着深厚的积累，传统的教材建设也相对比较规范。伴随着计算机技术突飞猛进的发展，特别是超大规模计算机平台的建立和使用，以及科学研究中不断增长的对计算方法和技术的需求，传统的计算数学教材已不能满足教学的需要。

信息化已成为当今世界发展的重要趋势，也是衡量一个国家现代化水平的重要标志。信息科学可以理解为信息获取、传输、处理与控制的科学。我国信息科学发展的时间相对较短，但发展迅猛。发展信息科学需要数学基础，当然也离不开计算机科学。由于信息科学的多学科交叉的特点，在不同院校和专业，信息科学都

得到了一定的发展。但也正是这些原因，使得信息科学的学科定位，尤其是教材建设百家争鸣，缺乏统一的规范，为教学带来了很大的实际困难。

教育部 1998 年颁布的普通高等院校专业目录中，“信息与计算科学专业”被列为数学类下的一个新专业。这一新专业的设置很好地适应了新世纪以信息和计算技术为核心的数学人才的培养。然而，作为一个新专业，对其专业内涵、专业规范、教学内容与课程体系等有一个认识与探索的过程。教育部数学与统计学教学指导委员会经过多年艰苦细致的工作，对一些问题有了比较明确的指导意见，发表了《关于信息与计算科学专业办学现状与专业建设相关问题的调查报告》及《信息与计算科学专业教学规范》(讨论稿)(见《大学数学》第 19 卷 1 期(2003))。按照新的教学规范，信息与计算科学专业是以信息技术和计算技术的数学基础为研究对象的理科类专业。其目标是培养学生具有良好的数学基础和数学思维能力，掌握信息与计算科学基础理论、方法与技能，能解决信息技术和科学与工程计算中实际问题的高级专门人才。

近年来在教育部领导下，高等院校每年大量扩大招生，从而使得我国的高等教育从精英化向大众化转变。现在全国大约有 400 所高校开办了“信息与计算科学专业”，每年招收 3 万名左右的本科生。其中大部分学校缺乏从事该领域教学科研经验的教师，对专业的定位和课程设置也不太明确。即使是全国一流的高校，也是偏向于单一学科，新专业没有一个完整的切实可行的教学大纲，适合交叉学科专业的教材极其匮乏。

“信息与计算科学专业”属于数学类，前两年的课程基本上是明确的，教材也很多。本套系列教材重点满足后两年的专业课设置需求。由于重点高校大部分有自己的课程体系和教材建设，本系列教材主要针对普通高等院校开办的该类专业。依据教育部“强基础，宽口径，重实际，有侧重，创特色”的办学指导思想，清华

大学出版社组织的《高等院校信息与计算科学专业系列教材》编委会成员对专业定位、课程设置、教材内涵等进行了深入的探讨，并邀请有多年教学和科研经验的教师编写系列教材。特别是北京大学姜明教授等对涉及信息科学的教材建设花费了大量心血，在此对他们表示感谢。

为适应不同类型院校和不同层次要求的课程需求，教材建设也需要多样化和层次化。我们相信，该系列教材的出版对缓解本专业教材的紧缺局面，逐步形成专业定位与课程设置，推动信息与计算科学的发展，培养适应时代发展的交叉学科人才，提高中国数学教育水平起到一定的作用。

张平文

2005 年 7 月 6 日

前　言

计算机技术的快速发展促进了网络技术的迅速发展与广泛应用。通过网络传输或获取信息，已从军事、政治、外交等重要领域日益普及到人们日常生活的各个领域。因而，保障信息在网络传输的过程中不受各种干扰破坏或不发生泄露，已成为当今信息时代的一个重要问题。

当然，在存储信息或对信息进行处理时也可能遭受到无意或恶意的破坏。保障信息的安全就是要保护信息在传输、获取、存储、处理以及使用的过程中，信息的机密性、完整性、不可抵赖性和可用性不受到无意或恶意破坏。

保障信息安全的技术可分为承载数据的系统安全、数据安全及事务安全3个方面。系统安全包括访问控制、防火墙、物理隔离等保护技术，入侵检测、安全审计、漏洞扫描、病毒扫描等检测技术，还包括负载均衡、冗余备份等恢复技术。而密码技术通过加密、鉴别、身份识别、数字签名等机制构成数据安全、事务安全的基本工具集。密码技术和访问控制技术共同构成信息安全保护的核心技术。没有密码学就没有信息安全。

本书介绍信息安全与密码学的基本概念及一些基本知识。在前3章对信息安全的一些知识进行了介绍，为信息安全准备了一些重要的应用背景。后续章节重点讲述的是现代密码学的基本理论。

在选材原则上，本书对目前应用比较广泛，或是当前研究热点的密码体制、算法或安全协议做了较详细的讲述。而对其他一些影响程度不大，或应用范围不广的密码体制或算法，则只做了摘要

性的介绍。

全书由绪论、信息安全初步、信息安全技术、传统密码学、公钥密码算法、Hash 函数、计算复杂性理论、零知识证明与比特承诺、基于身份的公钥密码学、数字签名、密钥管理和密码学中的基本数学知识(附录)组成,共 11 章及一个附录。所涉及的内容基本上涵盖了现代密码学的基本概念、基本算法,以及信息安全的基本知识。

在绪论中简要介绍了古典密码术中的 4 个著名的密码:Caesar 密码、Vigenére 密码、Playfair 密码、Hill 密码,以及 7 种著名的密码机:Vernam 密码机、ENIGMA 密码机、SIGABA 密码机、B-21 密码机、M-209 密码机、TYPEX 密码机、PURPLE 密码机。在附录中介绍了密码学中所涉及的一些基本数论知识及代数学知识,以便于读者阅读。

考虑到本书是为数学、计算机科学、通信、电子工程等相关专业开设信息安全与密码学课程的教学需要而编著的,所以在编写过程中,力求内容简明扼要、条理清晰、通俗易懂。同时本书对于如 Hash 函数等方面的一些新的研究成果也做了简单的介绍。

本书在写作过程中得到国家自然科学基金网络与信息安全重大项目(批准号 90104004)、国家 973 项目(批准号 1998030420),以及北京数盾信息科技有限公司的支持和资助。同时得益于与北京大学安全与密码工程研究中心王杰教授、赵春来教授,以及许多研究生的共同讨论,在此一并表示感谢。

本书是在作者多年从事信息安全与密码学的研究与教学的基础上编写而成的,并经多次修改,但疏漏与不妥之处在所难免,诚望读者与同行专家、学者不吝予以批评指正。

作 者

2006 年 8 月

目　录