研究生数学丛书 2

Mathematics Series for Graduate Students

应用密码学

Applied Cryptography

孙淑玲 编著

Sun Shuling

清华大学出版社

Springer

研 究 生 数 学 丛 书 2
Mathematics Series for Graduate Students

应用密码学

Applied Cryptography

孙淑玲 编著
Sun Shuling


清华大学出版社
北京


Springer

内 容 简 介

应用密码技术是电子安全系统的关键技术，它主要实现保密性、完整性和不可否认性。本书包括密码算法、密码协议及使用方面的主要内容：分组密码算法、公钥密码算法、数字签名、哈希函数、密钥建立、密钥管理、身份识别、电子现金等。每章后附有阅读资料，部分章节配有习题。

本书是在中国科学院研究生院讲授多年的讲义的基础上形成的。可以作为高等学校计算机科学、通信工程、信息安全等专业的研究生教材，也可以供有关工程技术人员参考。

图书在版编目(CIP)数据

应用密码学/孙淑玲编著. —北京：清华大学出版社，2004
(研究生数学丛书)
ISBN 7-302-07847-5

Ⅰ.应… Ⅱ.孙… Ⅲ.密码－理论－研究生－教材 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2003)第 120200 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：刘　颖
文稿编辑：王海燕
封面设计：常雪影
印 刷 者：北京牛山世兴印刷厂
装 订 者：三河市新茂装订有限公司
发 行 者：新华书店总店北京发行所
开　　本：170×230　**印张**：13.25　**字数**：237 千字
版　　次：2004 年 3 月第 1 版　2004 年 3 月第 1 次印刷
书　　号：ISBN 7-302-07847-5/TP・5705
印　　数：1～3000
定　　价：29.00 元

研究生数学丛书 Mathematics Series for Graduate Students

编审委员会

总　序

数学是一门在非常广泛的意义下研究自然和社会现象中的数量关系和空间形式的科学。长期以来，在人们认识世界和改造世界的过程中，数学作为一种精确的语言和一个有力的工具一直发挥着重要的作用。在现代，数学科学已构成包括纯粹数学及应用数学内涵的众多分支学科和许多新兴交叉学科的庞大的科学体系。作为各门科学的重要基础，作为四化建设的重要武器，作为人类文明的重要支柱，数学科学在很多重要的领域中已起着关键性甚至决定性的作用，数学技术已成为高技术的突出标志和重要组成部分，数学的影响和作用已深入到各行各业，可以说无处不在。马克思当年的预言："一门科学只有当它成功地运用了数学之后，才算达到了真正完善的地步"，正在不断得到证实。在这样的背景下，数学科学的重要性已得到空前广泛的认同。在研究生（不限于数学专业的研究生）的培养中，重视数学基础的训练，强调数学思想的熏陶，也已成为一种必然的趋势。但是，国内研究生数学教材及参考读物的实际情况，无论从品种、数量及质量哪一方面来看，都远远不能适应这个形势，甚至也远远落后于本科生的数学教材。这已成为制约提高研究生培养质量的一个重要瓶颈。清华大学出版社和施普林格出版社(Springer-Verlag)合作，倡议出版这一套《研究生数学丛书》(Mathematics Series for Graduate Students)，可望改善这方面的状况，为我国的研究生打好数学基础、提高数学素质起到积极的作用。

根据数学这门科学的特点，同时考虑到研究生学习数学的基本要求和特有方式，这套以面向研究生（包括高年级本科生、硕士及博士研究生）的数学教材或参考读物，将力求体现以下的一些原则：

- 主题有理论或（和）应用方面的重要性；
- 在重点介绍基础性内容的前提下，兼顾学科前沿的重要发展趋势和研究成果；
- 在讲授数学内容的同时，充分体现数学的思想方法和精神实质；
- 少而精，在较小的篇幅中展现基本的内容；

- 有相当好的可读性，适宜读者自学；
- 附有习题、思考题及参考资料目录，书末有索引，方便读者深入学习与思考。

为了有利于体现这些原则，本丛书将采取相当灵活的体例及风格：内容可以是纯粹数学、应用数学或数学与其他学科的交叉；可以是较系统地介绍某一个分支的教材，或是介绍某一前沿分支状况的综述，也可以是课外参考书；可以是原著，也可以是译著；可以是国内作者，也可以是国外作者；可以用中文编写，也可以用英文编写，等等。

要实现本丛书的目标和宗旨，任重而道远，但千里之行，始于足下，在学界同仁和广大读者的支持和帮助下，让我们共同努力。

李大潜

2003 年 9 月于上海

出版前言

应用密码技术是电子安全系统的关键技术，它主要实现保密性、完整性和不可否认性。在现实生活中有许多用处，如对文件进行数字签名、身份识别、实现电子货币等。

本书是作者几年来在中国科学院研究生院教授“现代密码学——理论与实践”（60学时）的讲稿基础上形成的。不少内容取自“应用密码学手册”（1997年版）一书。教授的对象是信息学院的硕士研究生，他们大多是密码技术的实践者而不是研究者。

本书与其他已出版的书相比，希望内容上比较新（涉及AES、会议密钥、PKI、电子现金），而且理论与实践并重（强调使用算法和协议应该注意的问题、加大密钥管理的篇幅、概述密码技术标准）。本书大体分成密码算法和密码协议两个部分，前者包括第2章和第3章，后者包括第4,6,8,9章。由于学时限制并且在网络中数据采用包的形式传输，所以只是在概率公钥加密中谈及流密码。通常的基于线性反馈移位寄存器的流密码没有专门章节讲述。

在写这本书时最困难的问题是要包括多少数学基础知识。因为不理解基础的数学理论，要真正理解密码系统运作是不可能的。而密码学宽泛的内容需要许多数学分支的知识，如数论、线性代数、近世代数、概率论、信息论、计算复杂性理论等。考虑到学生在大学阶段数学基础课的设置，本书的附录中只包括所需的有限域、初等数论知识。

密码技术的实践者通过这本书只能对原来不熟悉的专题有个初步了解。有些章节配有少量习题，以方便读者进一步思考。另外每章都提供了进一步阅读的线索。

最后向过去几年里对本书的前身提供意见的教师和学生表示深深的谢意，作者也欢迎读者对本书给予更多的批评和指正。

序　言

20世纪的科学技术发展，特别是信息科学技术的发展，继农业(从狩猎到农耕)、工业（使用煤油电能源）革命之后又带来了一次生产力革命——信息革命。早在《第三次浪潮》中 Alvin Toffler 预言：计算机网络的建立和普及将彻底改变人类生存和生活模式。

信息化以通信和计算机为技术基础，以数字化和网络化为技术特点。它有别于传统方式的信息获取、储存、处理、传输和使用，从而也给现代社会的正常发展带来了一系列的前所未有的风险和威胁。人类社会是一个有序运作的实体，理想、信念、道德、法规从不同侧面维系社会秩序。传统的一切准则在电子信息环境中如何体现与维护，到现在并没有根本解决，一切都在完善之中。例如，我们通过信封来防止他人阅读信件内容达到保密的效果；在合同上，则通过签名盖章来保证它的真实性和法律效用。对于电子信息环境，如何建立互不相识的人之间的信任关系、如何做到责任的不可抵赖等问题需要解决。

当今，信息、资源和能源是人类生存的三大支柱。信息是社会发展不可或缺的财富。党的十五届五中全会明确指出，大力推进国民经济和社会信息化是覆盖现代化建设全局的战略举措。要以信息化带动工业化，发挥后发优势实现社会生产力跨越式发展。

今天当人们享受信息技术带来的巨大变革的同时，也承受着信息被篡改、泄露、伪造的威胁，以及计算机病毒及黑客入侵等安全问题。全世界由于信息系统安全的脆弱性而导致的经济损失逐年上升，安全问题日益严重。信息安全的风险制约着信息的有效使用，并对经济、国防乃至国家的安全带来威胁。也就是说信息安全对现代社会健康有序地发展，保障国家安全和社会稳定有着重要作用，对信息革命的成败有着关键的影响。

2002年6月全球互联网协会年会上，专家委员会主席迈克尔·纳尔逊列举了互联网发展面临的十大技术问题是：身份识别技术、保护知识产权技术、保护个人隐私技术、新一代互联网通信协议 IPv6、下一代互联网的网络技术、无

限互联网技术、将传统电话网和互联网相融合的技术、更有效的网上视频传输技术、防止垃圾邮件的过滤技术、网络安全技术。由此可见，安全问题占有很大比重。密码技术是信息安全技术的核心，它是实现保密性、完整性、不可否认性的关键。

自从“9.11 事件”以后，各国政府纷纷站在国家安全的角度把信息安全列入国家战略。重视对网络信息和内容传播的监控，更加严格地加固网络安全防线，把信息安全威胁降到最低限度。2002 年 11 月 27 日美国总统签署了网络安全法案。在未来几年中美国政府将为大学拨款 9 亿美元资金，用于成立计算机安全中心，招聘研究生和进行安全研究。其中 2.75 亿美元用于计算机系统安全博士后和高级研究人员奖学金；2.33 亿美元用于九大安全领域的研究，包括加密、隐私、无线安全、网络犯罪调查和指控等。

2000 年是我国认证之年，着力建立我国的公钥基础设施。我国政府将启动信息系统安全等级保护和网络身份认证管理服务体系。2003 年 2 月底广东省率先成立数字证书服务中心和电子密钥管理中心，使得全省有了统一的标准体系、基础设施和安全认证平台。

为适应这一新的形势，需要大力培养信息安全方面的人才。密码学的基本概念和技术已经成为信息科学工作者知识结构中不可或缺的组成部分。

目　录

第1章 密码学概述

1.1 引论

早期的密码学研究密写和非法解密问题，至今已有几千年的历史。人类有记载的通信密码始于公元前400年。D. Kahn搜集整理两次世界大战的历史资料，出版的《破译者》一书中对那个年代密码学在军事、外交方面的辉煌成绩（如1940—1945年间英国成功破译德国的ENIGMA密码机报文，1940年夏美国成功解密日本的紫密机）有较为详细的介绍。在电报发明以后，商业方面对密码学的兴趣主要集中在密码本的编制上；到20世纪初集中在与机械和电动机械加密机的设计和制造上。信息技术的发展迅速改变了这一切，随着计算机和通信技术的迅猛发展，大量敏感信息要通过公共通信设施或计算机网络进行交换。因特网的广泛应用大大促进了电子商务和电子政务。大量个人信息（如信用卡号、银行账号等）需要保密，密码学的应用已经不仅仅局限在政治、军事、外交等领域，它的商业和社会价值日益显著，与人们的日常生活愈加密切相关。

密码学领域实际上已被当作应用数学和计算机科学的一个分支。数学理论在当前的密码学研究中发挥着重要作用，其中包括数论、群论、组合逻辑、复杂性理论、遍历理论及信息论。对于计算机科学家而言，密码学与操作系统、数据库、计算机网络联系非常紧密。密码学的理论和技术已经得到迅速的发展。

1.1.1 信息安全与应用密码学

对于运行系统中的信息而言，它的安全性体现在：

- 保密性（confidentiality）：信息不能泄露给未经授权的人；
- 数据完整性（data integrity）：保证真实的信息从信源到信宿，在传输过程中不被篡改；
- 实体认证（entity authentication）：确证一个实体的身份；