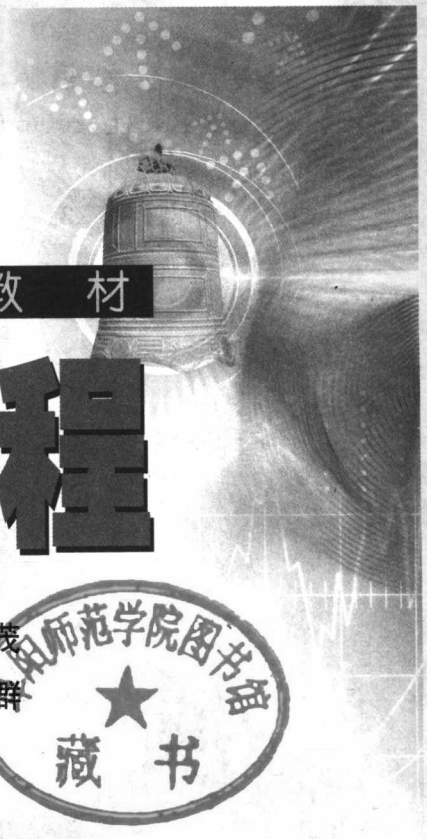
信息安全系列教材

密码学教程

主　编　张福泰　李继国　王晓明　林柏钢　赵泽茂
副主编　亢保元　马春光　沈丽敏　李素娟　王化群

WUHAN UNIVERSITY PRESS
武汉大学出版社



信息安全系列教材

密码学教程

主　编　张福泰　李继国　王晓明　林柏钢　赵泽茂
副主编　亢保元　马春光　沈丽敏　李素娟　王化群

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

密码学教程/张福泰，李继国，王晓明，林柏钢，赵泽茂主编．—武汉：武汉大学出版社，2006.9
信息安全系列教材
ISBN 7-307-05231-8

Ⅰ.密… Ⅱ.①张… ②李… ③王… ④林… ⑤赵… Ⅲ.密码—理论—高等学校—教材 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2006)第 116066 号

责任编辑：黄金文 史新奎 张敏 责任校对：程小宜 版式设计：支 笛

出版发行：武汉大学出版社 (430072 武昌 珞珈山)
(电子邮件：wdp4@whu.edu.cn 网址：www.wdp.com.cn)
印刷：湖北新华印务有限责任公司
开本：787×1092 1/16 印张：15.125 字数：381 千字
版次：2006 年 9 月第 1 版 2006 年 9 月第 1 次印刷
ISBN 7-307-05231-8/TP·217 定价：21.00 元

信息安全系列教材

编　委　会

内容提要

本书全面系统地介绍了密码学的体系结构，主要的理论和技术。包括密码学概论、古典密码体制、现代分组密码、流密码、公钥密码体制、密钥管理、Hash 函数、数字签名、身份识别、认证理论与技术、PKI 技术、密码应用软件，以及密码学新进展，共十三章。书末给出了参考过的主要文献资料的来源。可作为信息安全、计算机科学与技术、通信工程、数学与应用数学等本科专业密码学课程的教材，也可供初学密码学的研究生及相关的工程技术人员参考。

序 言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国 40 多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2006 年 9 月 19 日

前 言

在计算技术和网络技术快速发展的信息时代，信息安全受到了社会各界的高度关注。信息安全与国家的军事、外交、政治、经济、金融，甚至普通老百姓的日常生活的关系越来越密切。世界各个国家和地区政府都非常重视自己国家和地区的信息安全问题，在信息安全的基础设施建设、教学以及研究开发方面不断加大人力、物力和财力的投入。近十多年来，我国政府对信息安全的关注与支持与日俱增，在国家自然科学基金、863、973 等重要研究和开发计划中都把信息安全列入了重点资助对象，并相继在一些高等院校中设立了信息安全本科专业。《密码学教程》正是为信息安全本科专业编写的系列教材之一。

密码学在信息安全中占有非常重要的地位，能够为信息安全提供关键理论与技术。因此，密码学是信息安全本科专业的主要专业课程之一。

《密码学教程》是针对我国信息安全本科专业学生的基础和实际情况，根据国家的有关指导性意见编写的。教材全面系统地介绍了密码学的体系结构，主要的理论技术、典型的密码应用软件与产品，以及密码学研究中的一些新进展。全书共分 13 章。第 1 章密码学概论，介绍了密码学中的一些基本术语、密码学的体系结构和密码学发展简史。第 2 章古典密码体制，介绍了一些重要的古典密码算法和对古典密码体制的主要攻击方法。第 3 章现代分组密码，介绍了现代分组密码的原理、设计方法、操作模式、最具代表性的几个分组密码算法，以及对分组密码的差分和线性分析方法。第 4 章流密码，介绍了流密码的原理、设计方法以及 RC4、A5、SNOW2.0 等著名的流密码算法。第 5 章公钥密码体制，介绍了公钥密码体制的原理、RSA、ElGalmal、ECC 等主流的公钥密码体制。第 6 章密钥管理，介绍密钥分配模式、密钥传送、密钥协商、秘密共享、会议密钥、密钥托管技术等。第 7 章 Hash 函数，介绍 Hash 函数安全性的概念、构造方法，以及 MD5、SHA-1 等 Hash 函数算法。第 8 章数字签名，介绍数字签名的概念、安全性要求和一些著名的数字签名方案，如 RSA、ElGamal、Schnorr、DSS，ECDSA 等。第 9 章身份识别，主要介绍身份识别的概念、方法和一些重要的身份识别协议。第 10 章认证理论与技术，介绍认证的理论、技术和一些重要的认证协议。第 11 章 PKI 技术，介绍 PKI 的理论基础、组成、功能、相关协议及一些有代表性的 PKI 产品。第 12 章密码应用软件，介绍安全邮件标准、邮件加密软件 PGP、PGP Universial、IPSec 的安全性及电子商务的安全技术等。第 13 章密码学新进展，介绍量子密码学、基于身份的密码体制、无证书密码体制、环签名和指定验证人签名，以及 DNA 密码等研究热点。

教材内容全面系统，叙述简洁清楚。把必要的数学知识分散到了各相关章节，以免使学生感到枯燥乏味。考虑到本科生的实际情况和篇幅所限，本教材比较偏重于密码编码学，对密码分析学介绍得不够细致，在很多地方只是介绍了安全性的基本概念及一些密码体制的安全性的主要结果，而没有详细叙述对这些结果的证明或某种攻击方法的攻击过程。在有些章节，以附录方式给出了我们认为重要，但又不能在正文中叙述的一些密码算法等内容，供有兴趣的学生课后阅读。除了第 12 章和 13 章外，其余各章大多设置了必要的实验和习题，供读者操作和

训练，以加强对所学原理、方法的掌握和应用。

包括实验在内，建议总学时数为 72 学时。授课教师可根据学生情况及教学时间，适当选取课堂讲授内容，特别是对第 4 章、第 6 章、第 11 章至第 13 章的内容可舍弃或选讲部分。

整个教材由多所高校的富有教学和研究经验的教师合作编写，总体负责为南京师范大学的张福泰教授。统稿和修改工作由张福泰与河海大学的李继国副教授负责。参与编写或部分编写的主要人员有：暨南大学的王晓明教授、福州大学的林柏钢教授、杭州电子工业学院的赵泽茂副教授、中南大学的亢保元副教授、哈尔滨工程大学的马春光副教授、南京师范大学的沈丽敏讲师、南京工业大学的李素娟老师、南京邮电大学的王化群老师等，他们绝大多数都获得了密码学或相关专业的博士学位。南京师范大学与河海大学的研究生徐倩、王爱琴、陈礼青、张磊、孙银霞等同学仔细阅读了部分或全部初稿，提出了不少宝贵的修改意见。在此对所有参与编写和修改的老师和同学表示衷心的感谢。还要感谢武汉大学的张焕国教授、武汉大学出版社的黄金文副编审对编写本教材所给予的帮助和支持，感谢我的导师王育民教授多年来的关心、鼓励和支持。

尽管我们对全部书稿进行了多次的修改和订正，但由于时间仓促以及知识水平所限，书中错误和不当之处在所难免，恳请使用这本教材的老师和同学把所发现的问题、意见和建议及时反馈给我们，可发 E-mail 到 Zhangfutai@ njnu. edu. cn，lijiguo@ hhu. edu，cn，或 ffttzhang@ sina. com。任何意见和建议都是对我们的鞭策与支持，谢谢你们。

张福泰

2006 年 8 月

目 录

第1章 密码学概论

信息是社会发展的重要战略资源。在信息时代的今天,任何一个国家的政治、军事和外交都离不开信息,经济建设、科学发展和技术进步也同样离不开信息。计算技术和网络技术的快速发展,使得电子商务、电子政务、电子银行等成为现实,给我们的生活和工作带来了极大的便利。然而,人们在享受网络信息所带来的巨大利益的同时,也面临着信息安全的严峻考验。信息安全已成为世界性的现实问题,它与国家安全、民族兴衰息息相关。因此,加强信息安全研究、营造信息安全氛围,既是时代发展的客观要求,也是祖国建设的迫切需求。

密码学能够为信息安全提供关键理论和技术,在信息安全领域占有不可替代的重要地位。本教材将系统介绍密码学的体系结构、基本知识以及在信息安全中发挥着重要作用的各种密码理论与技术。

本章主要介绍密码学的基本概念及体系结构,并简述密码学发展的历史及其应用前景。

1.1 密码学的基本概念

密码学(Cryptology)研究的是如何保证信息系统的安全。它以认识密码变换的本质、研究密码保密与破译的基本规律为对象,主要以可靠的数学方法和理论为基础,对解决信息安全中的机密性、数据完整性、认证和身份识别,信息的可控性,以及不可抵赖性等提供系统的理论方法和技术。

我们首先来介绍密码学中的一些基本术语。对机密信息的保护一般通过加密来实现。假设 Alice 想给 Bob 发送机密信息,而 Eve 企图获取 Alice 和 Bob 之间的通信内容。Alice 要给 Bob 发送的原始消息称为明文(Plaintext)消息。为了不让 Eve 获取他们的明文消息,他们要以某种方式对消息进行变换后再传输。这种变换可以使他们自己容易地恢复明文,而使 Eve 不能恢复。这种对消息进行变换,以使非法用户不能获取原始消息的过程称为加密(Encryption)。消息经过加密变成了密文(Ciphertext),从密文恢复明文的过程称为解密(Decryption)。对消息加(解)密使其变成密(明)文的算法,称为加(解)密算法。加(解)密算法中使用的除了明(密)文消息外的另一个输入称为加(解)密密钥。解密密钥只有消息的合法接收方才拥有。非法用户不能解密,正是由于他不知道解密密钥。Alice 将明文加密成密文,Alice 的角色是一个密码编码者,Bob 是消息的合法接收者。非法截获者 Eve 企图从密文恢复明文,即对密文进行破译,这类人被称为密码分析者或攻击者或破译者。这样,一个保密通信系统中就有三方参与者:发送方(密码编码者)、合法接收者以及攻击者。发送方要通过加密算法,并借助于加密密钥对明文消息加密,然后把得到的密文消息传送给接收方。接收方收到的是加密过的消息——密文,他要读取明文消息,必须用相应的解密算法,并借助于自己拥有的秘密的解密密钥来对密文解密。攻击者截获的是密文消息,他要想方设法,在不拥有解密密钥的情况下,从密文恢复出明文。图 1-1 给出了保密通信系统的模型。