普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

对称密码学及其应用

Duichen Mimaxue Jiqi Yingyong

李 晖 李丽香 邵 帅 主编

北京邮电大学出版社
www.buptpress.com

普通高等教育“十一五”国家级规划教材

信息安全专业系列教材

对称密码学及其应用

北京邮电大学出版社
·北京·

内 容 简 介

本书全面介绍了对称密码学的基本理论、主要方法和应用实例，内容涉及古典密码学、现代对称密码学及最新进展。本书在介绍密码学的历史的同时，介绍了密码学的基础知识和基本概念，然后重点描述了分组密码算法和序列密码算法，包括它们的设计准则、典型算法和主要分析方法，在此基础上介绍了密钥管理基础知识，讨论了对称密码学在数字通信系统中和工业控制系统中的应用，最后介绍了两种新型密码体制——量子密码和混沌密码。

本书适合作为高校计算机安全与信息安全专业的本科教材，也可供对密码学、信息安全、通信安全等内容感兴趣的技术人员或科研人员阅读参考。

图书在版编目(CIP)数据

对称密码学及其应用/李晖，李丽香，邵帅主编. —北京：北京邮电大学出版社，2009

ISBN 978-7-5635-1717-6

Ⅰ. 对… Ⅱ. ①李…②李…③邵… Ⅲ. 密码术—高等学校—教材 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字(2009)第 177539 号

书　　名：对称密码学及其应用
主　　编：李 晖　李丽香　邵 帅
责任编辑：崔　珞
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京忠信诚胶印厂
开　　本：787 mm×960 mm　1/16
印　　张：18.5
字　　数：399 千字
印　　数：1—5 000 册
版　　次：2009 年 4 月第 1 版　2009 年 4 月第 1 次印刷

ISBN 978-7-5635-1717-6　　定　价：30.00 元

信息安全专业系列教材（第2版）

编 委 会

第 2 版总序

发展 21 世纪中国信息安全要靠教育，而搞好信息安全教育就需要好的教材。2004 年，灵创团队北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材，该套教材被教育部列入了“普通高等教育‘十五’国家级规划教材”。至今，三年多的时间过去了，这套教材在信息安全专业的教学中发挥了重要的作用，起到了较好的教学效果，受到教师和学生的好评。

在这三年中，我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设和校企就业（创业）平台建设等在内的信息安全本科专业的全面建设。2005 年，作为组长单位我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题；召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”。我们完成的国内第一次制定的信息安全专业规范，从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系；由通识教育内容、专业教育内容和综合教育内容三大部分，构建课程参考体系；采用顶层设计的方法构建了带有实践性环节的教学体系。我们在国内第一次较全面地提出信息安全学科专业教学改革与创新的研究以及发展思路和政策建议；这些成果已提交教育部相关教学指导委员会，对于引导高等学校信息安全学科专业教学改革与建设，指导信息安全学科专业评估，促进信息安全学科专业教学规范建设与管理，提高专业教育质量和水平起到了重要的作用。多所举办信息安全专业的高校都参照该课题成果调整了自己的教学计划、课程体系和实验方案。

我们积极搭建信息安全专业校际交流平台，组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”和“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地 40 亩的全国信息安全专业本科生实习实训基地，接受了来自全国近 30 所高校的本科生进入该基地参加丰富多彩的实训。

我们努力建设精品课程，主办了“全国高校信息安全专业精品课程建设经验交流会议”，来自全国各地高校的专家齐聚北京邮电大学，介绍了精品课程建设的经验。我们组织建设了全国第一批信息安全实验室，并且编写出版了实验教材《信息安全实验指导》，我们的《现代密码学》课程已经被评为北京市精品课程，并在 2007 年度被评为“国家精品课程”。

经过灵创团队全体人员的共同努力，北京邮电大学信息安全本科专业被教育部评为

第二类优势特色专业。

三年多的时间过去了，无论信息安全的教育和产业都取得了丰硕的成果，随着信息安全向更高层次的发展，其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要，积极探索培养创新型高素质人才，我们按照制定的学科发展战略和专业规范的精神，结合近几年的教学实践，对这套信息安全专业本科系列教材进行了全面修订，并及时成立了灵创团队北京邮电大学数字内容研究中心。这次修订不仅对原来的系列教材在第1版的基础上进行修改和完善，还补充了信息安全最新的研究成果，使教材的内容更加翔实和新颖。同时，在原有的教材上又增加了一些新的课程教材，在新修订的系列教材中，目前有《信息安全概论》(第2版)、《现代密码学及其应用》、《网络安全》(第2版)、《信息安全管理》、《计算机病毒原理及防治》(第2版)、《数字版权管理》、《计算机系统安全》、《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与VPN》、《对称密码学及其应用》、《信息安全导论》、《数字图像取证技术》等13本教材，今后随着信息安全专业教学的需要，还将不断地有新的教材补充到这个系列中来，使之更加完善和系统。目前，计划列入的相关教材还有：《入侵检测》(第2版)、《信息内容安全》、《信息安全工程》、《软件安全》及《信息安全标准与法律法规》等。

我们组织了强大的师资队伍，广泛吸收了有着丰富教学科研经验并多次讲授该系列教材的教师充实到这次修订工作中。作者队伍中不但包括北京邮电大学的教师，还包括哈尔滨工程大学、北京交通大学等重点院校的教师。经过反复研讨，本着理论与实际相结合的原则，对原来的系列教材进行了较大的修改和扩充，我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向专业的不同需求。

这次修订我们对内容进行了精心的组织和安排，希望能促进信息安全课程的建设，涌现出更多的信息安全精品课程。虽然我们在这次修订中投入了很大精力，但是由于水平有限，时间仓促，且信息安全专业的发展速度非常快，书中的不足之处和错误在所难免，我们衷心期望使用和关心该系列教材的师生，继续对新的系列教材提出宝贵的意见和建议。

本套系列教材也是国家重点基础研究发展计划(973)(课题编号：2007CB310704和2007CB311203)资助的成果，并被教育部增补为“普通高等教育‘十一五’国家级规划教材”的选题。

在本系列教材的修订过程中，得到了北京邮电大学出版社的大力支持，同时也得到了灵创团队的骨干机构(北京邮电大学信息安全中心和北京邮电大学数字内容研究中心)三百余位成员的支持与配合，在此一并表示感谢。

教授、博导、长江学者特聘教授

杨义先

前　言

本书的目标是介绍密码学的重要分支——对称密码学，包括它的基本概念、主要设计原理和典型应用。

密码学是一个富有神秘色彩的学科，它不仅仅局限于数学与计算机学科，而是超越了传统的学术学科，是一个古老而又充满了新的挑战的综合学科。由于它的研究内容包括了历史、政治、工厂、语言军事学、伦理、数学和工业技术学等，任何单本书都无法从上述所有这些方面来介绍密码学。因此，本书只是选择了密码学中具有悠久历史的一个分支——对称密码学进行介绍，作为学习密码学知识和理解密码学复杂而有意义的内容的一个起点。

有两个原因促成了本书的写作。第一，目前密码学技术已经被广泛地应用到信息技术的所有领域，使得密码学的研究范围更深更广，“广”意味着密码学的内容将涉及加解密技术、数字签名技术、信息鉴别技术、身份认证技术、密钥管理和安全协议等多个分支，而“深”则表示需要对这些技术进行更为深入的介绍，以满足求学者系统学习其中某个分支的需要，本书将针对对称密码学开展深入系统的讨论。第二，在目前通信及信息技术迅速发展的大环境下，急需大量的信息安全人才，他们不仅需要了解加解密算法的设计原理和思想，而且需要了解加解密算法的基本使用方法和应用情况，因此本书将介绍加解密算法的应用实例作为重点，以满足日益增长的对信息安全实用性技术知识的需求。

全本书共分五部分。第一部分是密码学简介和古典密码学，包括第 1 章和第 2 章，介绍密码学的基础知识，主要内容包括密码学的基本概念、对称密码体制的概念与分类、对称密码学的应用领域和几种典型的古典密码算法及分析等；第二部分是分组密码算法，包括第 3 章、第 4 章和第 5 章，主要内容包括分组密码算法的设计准则、典型分组密码算法和分组密码的统计测试原理及攻击方法等；第三部分介绍序列密码，由第 6 章、第 7 章和第 8 章组成，主要内容包括序列密码概述、序列密码的设计与分析和典型序列密码算法等；第四部分介绍密码技术及应用，由第 9、10、11 章组成，主要内容包括密钥管理、对称密码学在数字通信系统中和工业控制系统中的应用等；第五部分介绍密码学的新进展，由第 12 章和第 13 章组成，分别介绍以量子力学理论为基础的量子密码和利用混沌现象实现

信息保护的混沌密码。

本书作为本科学生的专业教材，参考学时为 50 学时。此外，本书也可以供从事相关领域研究的科研人员阅读参考。

本教材的策划、统稿和修改工作由李晖负责。参加编写的主要人员有李丽香、邵帅、温雨凝、封莎、刘衍斐、邵琳、赵子铭、秦新、李杰华等，另外周玲玲和李翔也参与了本书部分章节的修改工作，王健博士对本书提出了很多有益的建议，在此对他们的辛勤工作表示感谢！

感谢杨义先教授、钮心忻教授、罗群副教授、郑世慧博士，他们对本书的撰写和出版都提出了很多宝贵的意见和建议。

本书在编写过程中还参阅了国内、外同行的大量文献，在此向这些文献的作者表示由衷的感谢！

我们力图将复杂的密码学知识以一种较为简单的、易于理解的方式呈现给读者，同时也希望保证所述内容的完整性和正确性。但由于水平有限、时间紧张，书中难免出现疏漏，甚至错误，恳请广大同行和读者指正，并提出宝贵意见，以便我们再版时修改和完善。编者的电子邮箱是 lihuill@bupt.edu.cn。

编　者

目　　录

第 1 部分　密码学简介和古典密码学

第 2 部分　分组密码

第 3 章　分组密码简介与设计准则

第 4 章　典型分组密码简介

第 4 部分　密码技术及应用

第 9 章　密钥管理

第 10 章　对称密码学与数字通信安全

第 5 部分　对称密码学新进展

第 1 部分　密码学简介和古典密码学

通信的发展和信息化的进程使人们生活在一个充满变化的时代。利用因特网，人们可以发送和接收电子邮件，可以不出家门进行网上购物，不必去银行排队就可以支付账单和转账，通过手机等设备，甚至可以在任何地方完成上述事情。但是，人们在享受这些便捷服务的同时，也在担心自己的银行账号和密码是否会被其他人窃取，自己的私密信息是否也会被其他人看到，等等，所有这些，都对信息的安全性提出了更高的要求。可见，信息安全已经和人们的日常生活联系在了一起，实际上，信息安全在军事、政治等领域占有更加重要的特殊地位，毫不夸张地说，信息安全与国家安定、民族兴衰息息相关。

密码学能够保护人们的秘密信息，为信息安全提供关键理论和技术，现在已经成为了辅助信息技术发展的重要手段。密码学是一门古老而又充满活力的学科，作为本书的第一部分，将主要介绍密码学的发展史、基本概念和古典密码学。