信息与通信工程研究生规划教材

密码学与通信安全基础

Foundation of Cryptology and Secure Communications

祝跃飞　王　磊　编著

華中科技大學出版社
http://www.hustp.com

信息与通信工程研究生规划教材

密码学与通信安全基础

Foundation of Cryptology and Secure Communications

祝跃飞　王　磊　编著

华中科技大学出版社
中国·武汉

图书在版编目(CIP)数据

密码学与通信安全基础/祝跃飞　王　磊　编著.—武汉:华中科技大学出版社,2008年11月
ISBN 978-7-5609-4568-2

Ⅰ.密…　Ⅱ.①祝…　②王…　Ⅲ.密码-理论　Ⅳ.TN918.1

中国版本图书馆(CIP)数据核字(2008)第074198号

密码学与通信安全基础　　祝跃飞　王　磊　编著

责任编辑:朱建丽　　封面设计:潘　群
责任校对:李　琴　　责任监印:周治超

出版发行:华中科技大学出版社(中国·武汉)
武昌喻家山　邮编:430074　电话:(027)87557437

录　排:武汉正风图文照排中心
印　刷:华中科技大学印刷厂

开本:850mm×1065mm　1/16　印张:10.5　字数:220 000
版次:2008年11月第1版　印次:2008年11月第1次印刷　定价:19.80元
ISBN 978-7-5609-4568-2/TN·115

信息与通信工程研究生规划教材
编　委　会

内 容 提 要

本书主要面向通信专业的硕士研究生，是基于这类读者的一般知识基础和学习密码学的目的而专门设计编写的。

本书内容按照4个层次编写：第1层次为应用密码学基础，在概要中介绍密码学学科体系，介绍各种基本密码技术；第2层次为应用密码学，较为系统地介绍密码技术在因特网中的应用，同时简单地介绍密码技术在各种无线通信网中的应用；第3层次为密码算法，重点介绍各种典型算法及其数学原理；第4层次简单介绍现代密码学的一些其他问题。另外，在附录中简要给出必要的数学基础和计算复杂性的理论基础知识。

本书的分层体系便于读者由浅入深逐步学习密码学，因内容不包括层次较深的密码安全理论和密码分析内容，故可供以应用为主而非研究为目的学习密码学的读者作为参考书籍。

Abstract

This book is specially designed for postgraduates majoring in communications, based on their general knowledge foundation and their purposes of learning cryptology.

The content of the book consists of four layers: the first layer is the basis of applied cryptology, which introduces various cryptographic basic technologies based on the overview of cryptology; the second layer is the applications of cryptology technologies in the Internet and wireless communications networks; the third layer is cryptographic algorithms, which presents the details and mathematical principles of various representative algorithms; the fourth layer is the briefly introduction of some other questions in modern cryptology. Moreover, the appendix of this book presents the necessary mathematical basis and the basic knowledge of computational complexity theory.

The system of the book can facilitate readers to learn the cryptology step by step. As the complicated secure theory of cryptology and cryptanalysis are not included, this book can also serve as a reference for readers with the purpose of applications of cryptology technologies.

总　序

随着信息时代的到来，人类已经生活在信息的“海洋”之中，信息和通信已渗入我们生活的各个方面。近年来，我国的电信产业以10%以上的年增长率迅猛发展，“中国制造”的通信产品广泛进入了全球市场。另一方面，信息和通信领域的理论与技术获得了迅速发展，不少技术难题已取得实质性突破，技术进步和产业发展相互推动、相互促进。

产业的发展带来了对人才，特别是高层次专业人才的巨大需求。信息与通信工程是我国工科门类中应用前景广阔、招生量比较大的学科，对我国的现代化建设起着非常重要的作用。其中的通信与信息系统更是近几年硕士研究生报考的热门专业之一。随着硕士研究生的不断招收，研究生教育成为一个突出的问题。鉴于通信学科的迅猛发展，广大科技工作者和硕士、博士研究生迫切需要学习与掌握信息和通信的现代理论与技术。目前，本专业的研究生教材已有一些，其中亦不乏典范之作，但针对研究生读者成系列出版的教材尚为少见。其中的一个原因是各校研究生课程设置自成体系，各校之间不尽相同，这为研究生教材的建设和推广造成困难。

有鉴于此，来自清华大学等十多所高校、科研单位的教授和专家相约聚首，对通信专业研究生课程体系设置进行探讨，尝试从各校现有的课程体系中提取共同性的知识结构框架，并结合他们多年的教学实践积累，编写一套针对通信专业研究生，兼顾高年级本科生的系列教材，为研究生教育做一点工作。

本系列研究生教材针对性强，知识覆盖较为全面，相信该系列教材的出版将会为读者系统掌握通信科学、信息科学的基础理论与技巧，以及本领域的先进技术方法和现代技术手段提供相对便捷的途径，对培养具有从事通信科学、信息科学以及相关领域的科研与开发和教学工作能力的人才提供有益的手段，对本专业研究生教学起到积极的推动作用。

本系列教材的作者均来自信息和通信学科实力较强的院校，不但有较为丰富的教学经验，而且在研究方向和地域分布上具有一定的代表性。我有感于他们对教育事业的热忱、对教书育人的执著，遂为之序。

中国工程院院士　李乐民

2007年8月

前　言

鉴于安全机制和通信系统早已紧密结合甚至融合，通信专业的硕士研究生学习必要的密码理论和技术已经成为现实的需要。本书正是专门针对这一需要而编写的。

当前，密码学的内容非常丰富，通信专业的研究生应该掌握哪些基本的密码理论和技术是编写本书首先需要考虑的问题。基于通信专业研究生学习密码学的目的和一般所具备的知识基础考虑，我们在下述思想指导下进行了内容的选取和体系设计。

第一，通信专业研究生学习密码学的主要目的是理解和掌握基本的密码技术，进而理解其在通信系统中应用的基本思想和方法。因此，本书的重点在于应用密码学和掌握典型密码算法，而未包括难度较大的密码安全性理论和密码分析方面的内容。

第二，考虑到读者学习过大学工科数学和信息论与编码课程，书中就不再涉及相关的数学原理。由于目前国内信息安全数学基础课程已经成熟，因此教材中没有包含相关数学基础的详细内容，仅在附录中给出主要的概念和结论。另外，考虑到一般通信专业学生没有系统学习计算复杂性理论，在附录中简要介绍了相关的基本知识供读者参考。

第三，读者学习密码学的最终目的是在理解和掌握现有的核心密码技术及其应用的基础上，深入理解密码学的思想和应用方法，从而能够较好地适应密码学和通信安全技术快速发展的需要，因此本书建立了一个密码学的体系结构，重点揭示了密码设计思想及密码应用模式和方法。

第四，在密码应用方面，选取因特网应用作为重点介绍，既取决于目前通信现实，更利于深入系统地理解密码技术的应用思想，同时介绍各种无线通信网的安全体系，从而使读者较为全面地了解目前密码学在通信中的应用。在这些内容的介绍中，采用了先阐述原理再展开对细节做必要介绍的模式，而不是以技术手册的方式进行全面细节介绍，这样更符合教材的特点。

第五，为了适应读者不同层次学习的需求，本书分为 4 个层次。第 1 个层次为 1～4 章，其内容为应用密码学基础，其中，第 1 章概要介绍密码学学科体系，第 2～4 章分别介绍加密体制、认证系统和基本密码协议。第 2 个层次包括第 5～9 章，内容为应用密码学，较为系统地介绍了密码技术在因特网中的综合应用，同时简单介绍了各种无线通信网和密码相关的安全机制。第 3 个层次包括第 10～12 章，内容为密码算法，重点介绍各种典型算法的细节和数学原理，供需要深入了解算法进而实现算法的读者学习。最后 1 个层次是第 13 章，介绍了密码学的其他典型内容，供读者全面地了解密码学。前 2 个层次为基本内容，而后 2 个层次为深入学习的内容。这种分层次的体系结构非常便于读者由浅入深的学习。

由于本书定位于通信安全的密码学基础，对密码学的介绍还是比较基本的，如果需要进一步深入学习，请参考有关的专业书籍（如参考文献[2]、[5]等）。

感谢国家自然科学基金项目和国家“863”项目的支持。

作　者

2008 年 2 月

目　录

第 1 章　密码学概要

历史上，密码在军事、外交上的许多重大事件中起过重要甚至决定性的作用，事例不胜枚举。

第二次世界大战的历史更是集中体现了密码的意义："月光之夜"的故事可谓密码价值的经典事例。德国制订了代号为"月光之夜"的行动计划，计划夜间毁灭性地空袭英国工业重镇考文垂，英国通过破译德军密码及时获悉了这一计划，但如果采取措施来减轻对其重要工业基地的损失，将暴露已破译德军密码，进而导致德军很快更换密码，为了通过已破译密码获得更有价值的情报，英国首相丘吉尔艰难地选择了牺牲考文垂。中途岛海战是太平洋战场的转折点，美国胜利的根本原因在于及时破译了日本偷袭中途岛的情报，从而设伏使日本海军遭到致命的打击。由于行动计划被完全破译，日本战争核心人物山本五十六大将在视察途中被美国空军拦截击落座机而亡。有专家估计，盟军密码专家的破译工作，至少使第二次世界大战缩短了 8 年。

由于密码的特殊作用，世界大多数国家的军政部门始终都有庞大的、秘密的密码研究机构。当今，世界范围内的政治、军事、外交、经济等斗争更加尖锐与复杂，特别是社会信息化导致了国家安全战略的变化，各国都在不断加强对密码学研究。

随着新的技术革命——信息革命的突飞猛进，社会信息化迅猛深化，信息的价值日益重要，对信息的安全存储、安全传输和安全处理等的需求日益迫切，因此信息系统的安全特别是信息的安全，已经成为并将继续作为信息时代的重大课题。密码技术是无可替代的核心信息安全技术。伴随着信息化进程对信息安全的需要，公开密码学的研究与应用应运而生，并得到迅猛、蓬勃的发展。

本章先简要介绍密码学的历史，然后重点介绍所建立的密码学的体系结构。

1.1　密码学的简要历史

历史上很早就出现了用于保密的密码，恺撒大帝就曾将后来被称为"恺撒密码"的密码用于军事通信。由于在军事、外交等领域的特殊作用，密码的应用和研究曾长期处于秘密之中，民间只有极少数的业余爱好者使用和研究密码。

在漫长的岁月里，虽然随着实现技术的进步产生了从手工密码到机械密码再到电子密码的转变，但 1949 年以前都只能称为密码的"艺术"时期，因为此前密码的设计和破译主要是凭直觉或信念而非推理或证明来进行的。

1949 年，Shannon 发表了"保密系统的通信理论"，为当时的秘密密钥密码系统建立了理论模型，并采用他刚刚创立的信息论研究密码系统，该项工作得到一些极具理论和实践指

导意义的结果，从此密码学才真正成为一门科学。

此后直到1975年，密码学的理论研究进展还不大，只是电子技术和计算机技术的发展使密码学进入了电子时代。其间虽然出现了如Kahn的《破译者》等一些关于密码学的书刊和文献，但密码学的研究机构仍然主要局限于军队和政府的机要部门。

为适应由通信发展带动的公众，特别是商业领域对敏感信息保护的现实需求，美国国家标准局(National Bureau of Standard，NBS)于1973年发布了公开征集密码标准算法的请求。1975年，NBS对选定的数据加密标准(Data Encryption Standard)的算法细节进行了公布，这就揭开了密码学的神秘面纱，吸引了许多学者从事密码学的研究，从此兴起公开研究密码学。

1976年，Whitefield Diffie和Martin Hellman发表了《密码学的新方向》，突破秘密密钥密码的理念，提出了公开密钥密码思想，为密码学开辟了崭新的研究领域，带来了广阔的应用前景，从而导致了密码学的一场革命。

上述两个事件标志着现代密码学的诞生，从此，公开密码学的研究得到迅猛发展，从事密码学方面工作的人数、召开的会议、发表的文章和出版的书刊都以惊人的速度增加。

随着社会信息化的不断深化，对安全的需求不断扩展，密码学的研究内容也得到不断丰富，不仅从保密扩展到包括数字签名、消息认证和身份认证等各种认证，而且从20世纪80年代起上升到密码协议层次，即试图通过精心设计的使用保密和认证等基本密码工具的协议来解决各种复杂的安全问题。另外，如秘密共享、零知识证明等各种解决安全问题的新方法不断被提出，密码学的研究和应用领域不断扩大。同时，密码学的理论基础特别是相关的数学理论以及密码学自身的理论都得到不断丰富和深入发展。

1.2 密码学的体系结构

密码学的主题是试图通过各种安全而且有效的密码技术去解决各种信息安全问题。

密码学(cryptology)分为密码编码学(cryptography)和密码分析学(cryptanalysis)。编码的目的是设计各种密码体制用以保障各种安全，而分析的目的则是试图攻破各种密码体制。设计时必须考虑各种可能的攻击，而分析的深入必然促进设计水平的提高，进而带动分析的更加深入，这两者的矛盾是密码学发展的内在动力。

1.2.1 安全问题

现实生活对信息安全的需求是密码学发展的外在动力。密码学的内容是随着安全问题的不断出现以及对问题认识的不断深入而逐步丰富起来的，并将随着新问题的不断出现和对问题认识的不断提高而得到不断扩展和深化。

显然，对现实问题一一研究不具备理论意义，密码学从各种实际问题中抽象出一些安全问题，且考虑解决这些安全问题的方法和技术。

本书将密码学已经和试图解决的安全问题按层次分为下述4类。

1. 基本的通信安全问题

此类问题指直接的点到点通信或逻辑上为两点间通信所面临的安全问题，包括以下4

个问题：

(1) 在不安全信道上传送消息，攻击者可能进行被动攻击，通过窃听获得消息，对此，需要保护消息的保密性；

(2) 攻击者可能发动主动攻击，即伪造消息或篡改发送的消息，对此，需要保护消息的来源真实和内容完整；

(3) 在有些情况下，收方要防止发方可能否认曾发送过某消息，对此，需要提供消息的不可否认性；

(4) 在现实中有许多场合需要对身份进行确认，即需要防止攻击者冒充通信某一方，此问题早期称为身份认证或鉴别问题，后来一般化为主体真实性问题。

其中，保密性和完整性要求也适用于静态数据的安全保护，而身份认证和访问控制紧密相关。

2. 通信系统的通信安全问题

随着通信技术的迅猛发展，直接的点到点的通信方式在现实中的应用越来越少，取而代之的是以网络化为特征的各种通信系统，这些通信系统都涉及复杂的分层通信协议。通信系统中两点间的通信只是逻辑上的两点，实际上往往经过许多中间环节和层次。实现通信系统中两点间的安全通信，必须解决以上基本安全问题的密码技术和通信协议的有机结合。特别是当前主要的通信系统网络和各种无线通信网，都建立了安全体系结构，通过将合适的基本密码技术应用到不同的协议层次，形成了各种对应的安全通信协议。这类问题也常被视为密码在通信系统中的应用问题。

3. 应用安全问题

现实中有许多应用，需要提供对应的安全保障。特别是，基于各种通信系统，人们设计、开发了各种应用。但许多应用需要的安全保障是通信系统的安全性无法提供的。例如，电话掷币问题，通信双方试图通过电话交谈完成公平的硬币抛掷，显然，所基于的电话网的安全不能保证抛币功能的安全(公平)实现。又如，网络扑克问题，多方在网络上如何安全地(能防止各种作弊)玩扑克游戏？再如，电子选举问题，如何确保通过网络实现公平、公正的选举？显然，所基于的网络的安全不能保证上述问题安全(公平)地实现。因此，必须为各种具体应用问题的安全实现提供相应的密码技术。

4. 其他安全问题

除以上三个层次的问题以外，还有许多其他问题，这些问题大都来自为解决以上问题而引发出的新问题，还有一部分来自一些特殊的应用。例如，零知识证明问题是研究 Alice 如何在不泄露秘密内容的前提下向 Bob 证明她知道某一秘密，该问题源于如何抗击密码协议参与者中的主动攻击者(作弊者)。再如，秘密共享问题，研究的是如何将一秘密分交给若干个人共同保管，只有预先设定的部分用户联合起来才能恢复秘密，这一问题既是一个特殊的应用问题，又与密码中关键密钥的分享管理相关。

1.2.2　基本密码技术

1. 算法与密钥

解决保密性的密码技术是加密，通信双方用事先秘密协商好的方式，对称为明文(plain-