高等院校密码信息安全类专业系列教材

中国密码学会教育工作委员会推荐教材

现代密码学

马春光　编著

XIANDAI MIMAXUE

国防工业出版社
National Defense Industry Press

高等院校密码信息安全类专业系列教材
中国密码学会教育工作委员会推荐教材

现代密码学

马春光　编著

国防工业出版社
·北京·

内 容 简 介

本书依据教育部信息安全教学指导委员会发布的《信息安全专业指导性专业规范》中对密码学知识领域的要求，系统地介绍了现代密码学的基本内容，取材具有典型性。

全书共包括9章。第1章介绍了密码学的一些基本概念和术语，典型的古典密码体制及其统计分析。第2章介绍了分组密码的基本原理和典型的分组密码算法。第3章介绍了序列密码的基本原理和典型的序列密码算法。第4章介绍了Hash函数和消息认证码的概念，讲述了典型的Hash算法和消息认证码算法。第5章讲述了公钥密码的基本概念和典型的公钥密码，并对最新的身份基密码和属性基密码进行了介绍。第6章讲述了数字签名的基本概念和经典的数字签名方案，并介绍了一些特种数字签名方案。第7章从理论和技术角度讨论密钥管理中的若干重要问题。第8章对密码协议基础和几类重要的密码协议进行了介绍。第9章对密码学数学涉及到的数论和近世代数的基本概念、定理和算法进行了介绍。

本书是信息安全专业的专业基础课教材，适合作为高等院校信息安全专业或其他相关专业本科生和研究生的教材，也可作为相关领域中的教学、科研人员以及工程技术人员的参考书。

图书在版编目(CIP)数据

现代密码学/马春光编著. —北京：国防工业出版社，2014.8

高等院校密码信息安全类专业系列教材

ISBN 978-7-118-09476-3

Ⅰ.①现… Ⅱ.①马… Ⅲ.①密码-理论-高等学校-教材 Ⅳ.①TN918.1

中国版本图书馆CIP数据核字(2014)第151157号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路23号 邮政编码100048)

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 18¾ **字数** 427千字

2014年8月第1版第1次印刷 **印数** 1—2000册 **定价** 42.00元

总　序

信息系统所面临的各种安全威胁日益突出，信息安全问题已成为涉及国家政治、军事、经济和文教等诸多领域的战略安全问题。我国政府对网络与信息安全问题高度重视，国办印发的文件《关于网络信任体系建设的若干意见》明确指出了要特别重视网络安全的6方面内容；中办、国办印发的《国家2006年至2020年长期科学发展规划》中也突出了对各种网络安全问题的关注，将建设国家信息安全保障体系列为我国信息化发展的战略重点；国家“十一五”计划中也包含了提升国家信息安全保障服务能力的战略要求。西方发达国家纷纷制订了本国的网络与信息安全战略。比如，美国奥巴马政府正在采取措施加强美国网络战的备战能力，其中一项措施是创建网络战司令部，这表明美国的网络与信息安全战略已经由克林顿时代的“全面防御”、布什时代的“攻防结合”，转到奥巴马时代的“攻击为主，网络威慑”。

当前，制约我国网络与信息安全事业发展的瓶颈之一就是人才极度匮乏，为此，教育部从2001年起，陆续批准了包括北京邮电大学在内的近百所各类高校开设信息安全本科专业。但是，毕竟与其他经典的本科专业相比，信息安全本科专业的建设问题还面临许多挑战，需要全国同行共同努力，早日探索出一条办好信息安全专业的捷径。可喜的是，现在国内若干高校的教授团队都纷纷行动起来，各尽所能在信息安全本科专业建设方面取得了不少业绩。比如，灵创团队（http://www.cleader.net）就是众多热心于信息安全本科专业建设的创新团队，该团队中的“信息安全教学团队”被教育部和财政部批准为“2009年度国家级教学团队”；其完成的成果“信息安全专业规范研究与专业体系建设”获得了国家级教学成果奖二等奖；其带头人也被评为“国家级教学名师”并受到了胡锦涛等党和国家领导人的接见。希望国内能够有更多的类似教学团队投身于信息安全本科专业建设。

由于教材建设是信息安全专业建设的重点和难点之一，中国密码学会教育工作委员会自成立以来就一直致力于推进密码学与信息安全方面的教学和教材建设，比如，与国防工业出版社联合主办了“密码学与信息安全教学研讨会”等一系列研讨活动，并成立“普通高等教育本科密码信息安全类系列教材”编审委员会来组织策划相关系列教材。编审委员会在充分研究信息安全本科专业规范的基础上，经过细致研究，多次反复讨论，规划了与信息安全本科专业规范相配套的本系列教材。

本系列教材参照荣获国家级教学成果奖的信息安全最新专业规范，确定教材题目，组织教材书稿内容。所有教材严格按照“规范”要求，结合信息安全专业的学制、培养规格、素质结构要求、知识结构要求撰写，使其所含知识点完全覆盖“规范”中的要求，确保能够达到“规范”中的学习目标。由于本系列教材涉及的内容比较多，在教材内容选择时，一

方面要考虑教材内容相互的衔接，另一方面要考虑许多课程相互之间有内容交叉的现象；同时，充分考虑了先进性和成熟性之间的和谐关系，确保教材既能够反映信息安全领域的前沿科研状态，又能使学生掌握基础的核心知识和较成熟稳定的技能；编审委员会多次召开会议，审定教材的大纲，落实教材的主要知识点，避免了内容的重复。

本系列教材的作者都是在我国信息安全领域具有丰富教学和实践经验的一流专家，部分教材已经被评为“普通高等教育‘十一五’国家级规划教材”。

为便于高校教师选用本套教材，我们将为高校教师提供完善的教学服务，免费为选用本套教材的教师提供所有教材的电子教案和部分教材的习题答案。同时我们还提供信息安全专业本科教学实验室建设方案与实验教学指导咨询和信息安全专业本科生实习、实训与技能认证咨询。

本系列教材尽管通过反复讨论修改，但限于作者水平和其他客观条件限制，难免存在不足和值得商榷之处，敬请批评指正。

教授　博士生导师　国家级教学名师
灾备技术国家工程实验室主任
网络与信息攻防教育部重点实验室主任
北京邮电大学信息安全中心主任

2009 年 9 月 30 日

高等院校密码信息安全类专业系列教材
编委会名单

前　言

密码学是信息安全学科专业体系的核心之一。在教育部信息安全教学指导委员会发布的《信息安全专业指导性专业规范》中，密码学知识领域是信息安全专业的核心知识单元，密码学是信息安全专业的核心课程。本教材依据信息安全本科专业对密码学核心知识单元的要求进行内容组织，另外考虑到教学过程中对相关数学基础的需求，也将数论和近世代数的基本内容一并纳入，使得教材更具自含性，更有利于教学实施和教材的使用推广。

本教材系统介绍了现代密码学的基本内容，共包括9章。第1章密码学概述，介绍了密码学的一些基本概念和术语，典型的古典密码体制及其统计分析。第2章分组密码，讲述了分组密码的基本原理和几个典型的分组密码体制。第3章序列密码，讲述了序列密码的基本原理和几个典型的序列密码算法。第4章Hash函数和消息认证，讲述了Hash函数和消息认证码的概念，详述了典型的Hash算法和消息认证码算法。第5章公钥密码，讲述了公钥密码的基本概念和典型的公钥密码，并对最新的身份基密码和属性基密码进行了介绍。第6章数字签名，讲述了数字签名的基本概念和经典的数字签名方案，并介绍了一些特种数字签名方案。第7章密钥管理，从理论和技术角度讨论密钥管理中的若干重要问题。第8章密码协议，对密码协议基础和几类重要的密码协议进行了介绍。第9章密码学数学基础，对数论和近世代数的基本概念、定理和算法进行了介绍。

多年来，作者一直在哈尔滨工程大学为信息安全专业的本科生讲授现代密码学课程，本教材就是在此基础上，结合教学实践，在总结国内外密码学相关教材及文献的基础上，编写而成的。本教材在编写过程中，哈尔滨工程大学网络与信息安全研究团队（http://machunguang.hrbeu.edu.cn）的研究生李增鹏、石岚、汪定、谷德丽进行了部分资料收集和整理工作，在此表示诚挚的感谢。感谢北京邮电大学杨义先教授、雷敏博士，国防工业出版社在本书编写过程中给予的帮助和支持。

由于时间仓促以及知识水平所限，在教材中会有很多不足之处，甚至还有疏忽和错误，敬请广大读者批评指正。作者联系方式：machunguang@hrbeu.edu.cn。

本教材得到哈尔滨工程大学本科生教材立项重点资助项目、国家自然科学基金（61170241）和黑龙江省自然科学基金（F201229）的资助。本教材是黑龙江省高等教育学会“十二五”教育科研规划课题（HGJXHB2110336）研究成果一部分。

编者

2013年12月

目　录

第1章　密码学概述

密码学的研究与应用已有几千年的历史，其基本目的就是让通信双方能够在一个不安全的信道上进行保密通信。任何第三方即使在信道上截获了通信双方的通信内容，也无法知道所截获内容的准确含义。本章主要介绍密码学的一些基本概念和术语，典型的古典密码体制及其统计分析。

1.1　密码学发展概况

密码学是一门既古老又年轻的学科，其历史可以追溯到几千年前。大约4000年前，古埃及人就开始使用密码。古代的行帮暗语和一些文字猜谜游戏等，实际上就是对信息的加密。这种加密方法通过原始的约定，把需要表达的信息限定在一定的范围内交流。可以说，自从有了战争，就有了保密通信。在信息的保密和破译上，斗争双方进行着激烈的，有时甚至是生死存亡的斗争。例如，在第二次世界大战期间，盟军对德国和日本密码的破译对许多战役的胜利发挥了关键性的作用，并加速了战争结束的进程。随着技术的进步，特别是计算机和现代通信技术的发展，这种斗争更加扩大、更为激烈。

密码学有一个奇妙的发展历程，当然，秘而不宣总是扮演着主要角色。第一次世界大战之前，密码学重要的进展很少出现在公开文献中，但该领域却和其他专业学科一样向前发展着。直到1918年，William F. Friedman的专题论文“重合指数及其在密码学中的应用”(The Index of Coincidence and Its Applications in Cryptography)作为私立Riverbank实验室的一份研究报告问世，其中提出了多表代替密码的破译方法，它是20世纪最有影响的密码分析文章之一。其实，这篇论文所涉及的工作是在战时完成的。同年，美国加州奥克兰的Edward H. Hebern申请了第一个转轮机专利，这种装置在差不多50年里被指定为美军的主要密码设备。

第一次世界大战结束之后，完全处于密码工作状态的美国陆军和海军的机要部门开始在密码学方面取得根本性的进展。在20世纪三四十年代，有多篇基础性的文章出现在公开文献中，还出现几篇专题论文，只不过这些论文的内容离当时的技术水平相去甚远。战争结束时，情况急转直下，公开文献几乎殆尽。

1949年以前，密码技术基本上可以说是一门技巧性很强的艺术，而不是科学，在这一期间，密码专家常常是凭直觉和信念进行密码设计和密码分析，而不是基于推理和证明。1949年，Claude E. Shannon的论文“The Communication Theory of Secrecy System”(保密系统的通信理论)出现在“Bell System Technical Journal”(贝尔系统技术杂志)上，它类似于Friedman 1918年的文章，也是战时工作的产物。这篇文章在第二次世界大战后即被解密，可能是由于失误。Shannon的这篇著名论文把密码学置于坚实的数学基础之上，标志着密码作为一门学科的形成。

从1949年到1967年，密码学文献近乎空白。1967年，David Kahn的“The Codebreakers”（破译者）出版，尽管它并没有任何新的技术思想，但却对密码学的历史做了相当完整的记述，使成千上万原本不知道密码学的人了解了密码学。自此，密码学研究引起民间的兴趣，新的密码学文章慢慢开始源源不断地发表出来。大约在同一时期，早期为美国空军研制敌我识别装置的Horst Feistel在位于纽约约克镇高地的IBM Watson实验室里花费毕生精力致力于密码学的研究，他的工作包括领导设计了后来成为美国数据加密标准DES的LUCIFFER密码。

1976年，W. Diffie和M. E. Hellmen发表了“New Directions in Cryptography”（密码学中的新方向）一文，提出了一种崭新的密码设计思想，导致了密码学的一场革命。他们首次证明了从发送端到接收端无密钥传输的保密通信的可能性，从而开创了公钥密码学的新纪元。1978年，Rivest、Shamir和Adleman首先提出了一个实用的公钥密码体制RSA，使公钥密码的研究进入了快速发展阶段。

1973年，美国国家标准局（National Bureau of Standards，NBS）开始征集加密标准，IBM将LUCIFFER的改进版本递交评审，并于1977年获得批准，此后这一受到批准的算法被称为DES（Data Encryption Standard）。这是密码史上的一个创举，开创了向世人公开加密算法的先例。DES设计精巧、安全、方便，是近代密码成功的典范。它成为商用密码的世界标准，为确保数据安全做出了重大贡献。通过对DES算法的研究和分析，民间的密码学水平取得了突飞猛进的提高。

1984年底，美国总统里根下令美国保密局研制一种新密码，准备取代DES。经过10年的研制和试用，1994年美国颁布了密钥托管加密标准EES（Escrowed Encryption Standard），这是密码史上的又一创举。EES的密码算法被设计成允许法律监听的保密方式，即如果法律部门不监听，则加密是不可破译的，但是经法律部门允许可破译密码进行监听。如此设计的目的在于既要保护正常的商业通信秘密，又要在法律部门允许的条件下可破译监听，以阻止不法分子利用保密通信进行犯罪活动。EES只提供芯片而不公开身份，这标志着美国的密码政策由公开征集转向秘密设计，由公开算法转向算法保密。商界和学术界对不公开算法只承诺安全的做法表示不信任，强烈要求公开算法并取消其中的法律监听。迫于社会的压力，美国政府曾邀请少数密码专家介绍算法，企图通过专家影响民众，然而收获不大。1995年，美国贝尔实验室的年轻博士M. Blaze攻击EES的法律监督字段，伪造ID获得成功。于是，美国政府宣布仅将EES用于话音加密，不用于计算机数据加密，并且后来又公开了加密算法。于是美国政府于1997年又开始征集新的数据加密标准算法AES。

1994年，美国颁发了数字签名标准DSS（Digital Signature Standard），并实际上成为一种国际标准，许多国际标准化组织都已将DSS颁布为数字签名标准。一些国家已经颁布了数字签名法，从此数字签名有了法律依据。我国也颁布了自己的数字签名标准，并于2004年8月颁布了《电子签名法》。

1997年4月，美国标准和技术研究所（National Institute of Standards and Technology，NIST）开始公开征集DES的替代算法，它被称为高级加密标准（Advanced Encryption Standard，AES），并专门成立了AES工作组。至1998年6月共征集到16个候选算法。于2001年最终被采纳为AES。经过3年多的努力，2000年10月2日，NIST公布了最终的

AES 标准——由比利时密码学家 Joan Daemen 和 Vincent Rijmen 提交的 Rijndael 算法，并于 2001 年 11 月 26 日作为美国新的数据加密标准对外公布。

2001 年 1 月，欧洲委员会从信息社会技术（Information Society Technology，IST）规划中出资 33 亿欧元启动了“新欧洲签名、完整性与加密计划”（New European Schemes for Signatures，Integrity，and Encryption，NESSIE），希望推出一套不仅包括分组密码，还包括流密码、Hash 函数、消息认证码、数字签名和公钥加密等在内的强安全性的密码标准。2003 年 3 月，NESSIE 公布了最终的评估结果，他们把选出的安全算法集称为 NESSIE 算法套件，该套件包括 12 个决选算法和 5 个已经作为标准或即将成为标准的算法，共 17 个算法。日本、韩国等国家也先后启动了类似的计划。

密码学最初只用于解决信息的加密保护问题，用以对抗敌手在信道的窃密行为。随着计算机科学的蓬勃发展，社会已进入信息时代。电子计算机和通信网络的广泛应用，一方面为人们的生活和工作提供了很大的方便，另一方面也提出了许多亟待解决的问题，其中信息的安全性就是一个突出的问题。目前，大量敏感信息需要通过公共通信设施或计算机网络传递，特别是 Internet、局域网和无线通信的广泛应用，以及计算机应用系统（如电子商务、电子政务、电子金融等）的迅速发展，越来越多的个人信息、企业信息、计算机应用系统等需要利用密码技术提供加密保护和真实性认证。一些新的公钥密码体制相继被提出，各种不同应用背景的数字签名方案不断出现，各种有实用价值的密码体制的快速实现受到高度重视，许多密码标准、应用软件和产品被开发和应用。随着其他技术的发展，一些潜在的密码应用价值技术也得到密码学家的重视，出现了一些新的密码技术，如混沌密码、量子密码、生物密码等。现代密码学的应用已不仅仅局限于政治、军事以及外交领域，其商用价值和社会价值也已得到充分的肯定。

1.2 信息安全威胁与信息安全技术

1.2.1 什么是信息安全

信息安全问题在人类社会发展中从古至今都存在。在政治斗争、商业竞争甚至个人隐私保护等活动中，人们常常希望他人不能获知或篡改某些信息，并且也常常需要查验所获得信息的可信性。普遍意义上的信息安全是指实现以上目标的能力或状态。随着人类存储、处理和传输信息方式的变化和进步，信息安全的内涵在不断延伸。当前，在信息技术获得迅猛发展和广泛应用的情况下，信息安全可被理解为信息系统抵御意外事件或恶意行为的能力，这些事件和行为将危及所存储、处理或传输的数据或这些系统所提供的服务的可用性、机密性、完整性、非否认性、真实性和可控性。以上这 6 个属性刻画了信息安全的基本特性和需求，被普遍认为是信息安全的基本属性，其基本含义如下：

（1）可用性（Availability），是指即使在突发事件下，依然能够保障数据和服务的正常使用，如网络攻击、计算机病毒感染、系统崩溃、战争破坏、自然灾害等。

（2）机密性（Confidentiality），是指能够确保敏感或机密数据的传输和存储不遭受未授权的浏览，甚至可以做到不暴露保密通信的事实。

（3）完整性（Integrity），是指能够保障被传输、接收或存储的数据是完整的和未被篡

改的，在被篡改的情况下能够发现篡改的事实或者篡改的位置。

（4）真实性（Authentication），也称可认证性，是指能够确保实体（如人、进程或系统）身份或信息、信息来源的真实性。

（5）非否认性（Non-repudiation），是指能够保证信息系统的操作者或信息的处理者不能否认其行为或者处理结果，这可以防止参与某次操作或通信的一方事后否认该事件曾发生过。

（6）可控性（Controllability），是指能够保证掌握和控制信息与信息系统的基本情况，可对信息和信息系统的使用实施可靠的授权、审计、责任认定、传播源追踪和监管等控制。

1.2.2 信息安全威胁

所谓信息安全威胁，是指某人、物、事件、方法或概念等因素对某些信息资源或系统的安全使用可能造成的危害。一般把可能威胁信息安全的行为称为攻击。在现实中，常见的信息安全威胁有以下几类。

（1）信息泄露，指信息被泄露给未授权的实体（如人、进程或系统），泄露的形式主要包括窃听、截收、侧信道攻击和人员疏忽等。其中，截收泛指获取保密通信的电波、网络数据等。侧信道攻击是指攻击者不能直接获取这些信号或数据，但可以获得其部分信息或相关信息，而这些信息有助于分析出保密通信或存储的内容。

（2）篡改，指攻击者可能改动原有的信息内容，但对信息的使用者并不能识别出被篡改的事实。在传统的信息处理方式下，篡改者对纸质文件的修改可以通过一些鉴定技术识别修改的痕迹，但在数字环境下，对电子内容的修改不会留下这些痕迹。

（3）重放，指攻击者可能截获并存储合法的通信数据，以后出于方法的目的重新发送它们，而接收者可能仍然进行正常的受理，从而被攻击者所利用。

（4）假冒，指一个人或系统谎称是另一个人或系统，但信息系统或其管理员可能并不能识别，这可能使得谎称者获得了不该获得的权限。

（5）否认，指参与某次通信或信息处理的一方事后可能否认这次通信或相关的信息处理曾经发生过，这可能使得这类通信或信息处理的参与者不承担应有的责任。

（6）非授权访问，指信息资源被某个未授权的人或系统使用，也包括被越权使用的情况。

（7）网络与系统攻击，由于网络与主机系统不免在设计或实现上的漏洞，攻击者可能利用它们进行恶意的侵入和破坏，或者攻击者仅通过对某一信息服务资源进行超负荷的使用或干扰，使系统不能正常工作，后面一类攻击一般被称为拒绝服务攻击。

（8）恶意代码，指有意破坏计算机系统、窃取机密或隐蔽地接受远程控制的程序，它们由怀有恶意的人开发和传播，隐蔽在受害方的计算机系统中，自身也可能进行复制和传播，主要包括木马、病毒、后门、蠕虫、僵尸网络等。

（9）灾害、故障与人为破坏，信息系统也可能由于自然灾害、系统故障或人为破坏而遭到损坏。

以上威胁可能危及信息安全的不同属性。信息泄露危及机密性；篡改危及完整性和真实性；重放、假冒和非授权使用危及可控性和真实性；否认直接危及非否认性；网络与系统攻击、灾害、故障与人为破坏危及可用性；恶意代码依照其意图可能分别危及可用性、机密性和可控性等。