Information Security

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI

普通高等学校信息安全"十一五"规划教材

现代密码学

XIANDAI MIMAXUE

许春香　李发根　聂旭云　禹　勇　编著

电子科技大学出版社

PUTONG GAODENG XUEXIAO XINXI ANQUAN "SHIYIWU" GUIHUA JIAOCAI

普通高等学校信息安全"十一五"规划教材

现代密码学

许春香　李发根　聂旭云　禹　勇　编著

电子科技大学出版社

图书在版编目（CIP）数据

现代密码学 / 许春香等编著. —成都：电子科技大学出版社，2008.11

普通高等学校信息安全“十一五”规划教材

ISBN 978-7-81114-519-9

Ⅰ.现… Ⅱ.许… 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（2008）第 152301 号

内 容 提 要

本书为普通高等学校信息安全“十一五”规划教材之一，系统地介绍了现代密码学基础知识，包括流密码、分组密码、公钥密码、数字签名、Hash 函数，同时还介绍了密码学的最新进展。

本书可作为信息安全专业、计算机专业、通信专业本科生、研究生教材，也可以供信息安全技术领域科技人员参考。

普通高等学校信息安全“十一五”规划教材

现代密码学

许春香 李发根 聂旭云 禹 勇 编著

出 版： 电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦 邮编：610051）

策划编辑： 曾 艺

责任编辑： 曾 艺

主 页： www.uestcp.com.cn

电子邮件： uestcp@uestcp.com.cn

发 行： 新华书店经销

印 刷： 成都蜀通印务有限责任公司

成品尺寸： 185mm×260mm **印张** 11 **字数** 275 千字

版 次： 2008 年 11 月第一版

印 次： 2008 年 11 月第一次印刷

书 号： ISBN 978-7-81114-519-9

定 价： 20.00 元

编委会名单

编委会主任

郝玉洁

编委（按姓氏笔画为序）

刘乃琦　许春香　李毅超　佘　堃

周世杰　秦　科　谌黔燕　鲁　珂

学术顾问

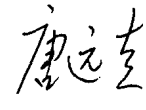
秦志光　李建平　周明天

序言

随着社会信息化的快速发展，信息已成为社会发展的重要资源，围绕着这一资源所展开的全球性的竞争日趋激烈。信息的安全已不再是个人和涉及少数人利益的问题，而是事关部门、公司、企业甚至国家、地区等政治和经济利益的十分重要的问题。信息安全正在作为一种产业快速发展，而与此相悖的是，信息安全人才匮乏，远远不能满足商业、金融、公安、军事和政府等部门的需求。因此，培养信息安全领域的高技术人才已成为我国高等工程教育领域的重要任务。

信息安全是集计算机、通信工程、数学等学科知识为一体的交叉型新学科，对于这一新兴学科的培养模式和课程设置，各高等院校普遍缺乏经验，为此，电子科技大学计算机科学与工程学院信息安全专业的专家、学者和工作在教学一线的老师们，以我国本科高等工程教育人才培养目标为宗旨，组织了一系列信息安全的研讨活动，认真研讨了国内外高等院校信息安全专业的教学体系和课程设置，在进行了大量前瞻性研究的基础上，启动了普通高等院校信息安全“十一五”规划教材的编写工作。该系列教材由 8 本理论教材和 2 本实验教材组成，全方位、多角度地阐述了信息安全技术的原理，反映了当代信息安全研究发展的趋势，突出了实践在高等工程教育人才培养中的重要性，弥补了目前该类教材理论教学内容丰富，而实践教学不成体系的缺点，使其成为该系列教材的特点，也是其成功所在。

感谢电子科技大学信息安全专业的老师们为促进我国高等院校信息安全专业建设所付出的辛勤劳动，相信这套教材一定会成为我国高等院校信息安全人才培养的优秀教材。同时希望电子科技大学的教师们继续努力，为培养更多、更好的信息安全人才，为我国的信息安全事业作出更大的贡献。



二〇〇七年三月十日于香港

唐远炎　国际电子电气工程学会会士（IEEE Fellow）
国际模式识别学会会士（IAPR Fellow）
国际 IEEE SMC 机器学习委员会主席（Machine Learning Committee, IEEE SMC）
《中国高等学校学术期刊》计算机科学分册（Frontiers of Computer Science in China）副主编
国际 SCI 检索刊物《International Journal on Wavelet, Multiresolution, and Information Processing（IJWMIP）》（小波、多尺度分辨及信息处理国际期刊）创办人、主编
国际 SCI 检索刊物《International Journal of Pattern Recognition and Artificial Intelligence（IJPRAI）》（模式识别与人工智能国际期刊）副主编

前言

密码学可以划分为古典密码学和现代密码学，古典密码学可以追溯到古罗马时期，而现代密码学主要是在第二次世界大战以后发展起来的。本书主要讨论现代密码学，为读者掌握和应用现代密码技术打下基础，但为了使读者全面了解密码学的历史，本书在引言中也简单介绍了古典密码学。学习现代密码学并不需要先学习古典密码学作为基础，但熟悉古典密码学对理解现代密码学是有帮助的，建议有兴趣的读者阅读古典密码学的有关专著。

现代密码学的基础体系为第 2 章至第 6 章，包括流密码、分组密码、公钥密码、数字签名、Hash 函数。这个体系又可以分为三个环节：流密码是一个环节，分组密码是一个环节，其余部分属于一个环节。这三个环节联系并不紧密，不能认为前面环节是后面环节的基础，读者在阅读本书时需要注意这个特点。

在本书的基础体系中，流密码技术环节主要讨论序列的随机性、线性移位寄存器以及两个普遍使用的流密码算法 RC4 和 A5；分组密码技术环节主要讨论分组密码的工作模式，第一代公开的、完全说明实现细节的商用密码算法 DES，国际数据加密算法 IDEA，高级加密标准 AES 以及我国官方公布的第一个商用密码算法 MS4；第三个环节主要讨论 RSA、ElGamal 公钥密码、Rabin 公钥密码、椭圆曲线公钥密码算法和 RSA 数字签名等数字签名算法以及 MD5 和 SHA 等 Hash 函数。

密码协议是应用上述基础体系中的密码技术所构建的协议，第 7 章主要讨论几种常用的密码协议。

本书在后续章节即第 8 章、第 9 章和第 10 章讨论了密码学的新方向，包括基于身份的公钥密码、可证明安全理论、量子密码学和 DNA 密码学等。这部分内容可以使读者了解密码技术的最新进展，对于一般了解密码学的读者可以不涉及。

本书可作为信息安全专业本科生、研究生教材，还可以供信息安全技术领域科研人员参考。

笔者衷心感谢郝玉洁等老师，她们的大力推动是本书写作的动力，最后衷心感谢电子科技大学计算机学院领导和同事们在本书编写中给予的支持和帮助。

作　者

2008 年 9 月于电子科技大学

目录

第 1 章　引言

第 2 章　流密码

第 3 章　分组密码

第 4 章 公钥密码

第 5 章 数字签名

目录

第 6 章　Hash 函数

第 7 章　密码协议

第 8 章　可证明安全性理论

第 9 章　基于身份的公钥密码体制

第 10 章 密码学的新方向

第1章

引　言

21 世纪是信息的时代，信息成为社会发展的重要战略资源，信息技术改变着人们的生活和工作方式。在信息时代的今天，任何一个国家的政治、军事和外交离不开信息，经济建设、科学发展和技术进步同样离不开信息，社会的信息化已经成为当今世界发展的主要潮流。计算机和网络技术的快速发展，使得整个社会的信息化程度愈来愈高，拥有更多的信息便意味着在竞争中抢占先机。然而，现代信息技术是一把双刃剑，它一方面给人们带来了巨大的利益，另一方面又给人们带来了潜在的威胁。Internet 的出现和发展为人类交换信息，促进科技、文化、教育和生产的发展，提高人们的生活质量提供了极大的便利。然而，正是因为 Internet 的开放性和无政府性，给不法分子以可乘之机，他们在试图窃取重要情报、倾泻信息垃圾、进行网络诈骗、散发破坏性信息等等，因此，信息安全已经成为世界各国共同关注的一个重要问题。所谓信息安全，是指保护信息及信息系统在信息存储、处理和传输过程中不被非法用户访问或修改，而且对合法用户不会拒绝服务，其中心内容是保护信息的机密性和认证性。

密码技术是保证信息安全的核心技术，密码学能为信息安全提供关键理论和技术支持，在信息安全领域占有极其重要的地位。本教材系统地介绍了密码学的体系结构、基础知识以及在信息安全中发挥着重要作用的各种密码理论和技术。

1.1 密码学的发展历史

密码学，这门古老而年轻的科学，是信息安全的核心技术。回顾密码学的发展，如同翻开一本内容丰富、充满传奇色彩的故事书。人类对密码的研究和应用已有几千年的历史，从 4000 年前的古埃及到 20 世纪的两次世界大战，密码一直扮演着极其重要的角色。

古罗马的凯撒（Caesar）大帝第一次将密码术应用到人类实践中。当时，凯撒大帝利用传信兵与前线的将军们通信，为了防止传信兵中途被抓或者篡改信件，凯撒采用了一种特殊的写信方式：将字母按顺序推后 3 位，即将字母 A 写为 D，将字母 B 写为 E，以此类推。信件写完后，凯撒将信件卷起，在封口滴上厚厚的蜡，在蜡未干以前，压上自己的私印。将军收到信件以后，首先检查蜡封是否完整，蜡印是否为凯撒的印章，然后才拆开信件，按照只有他和凯撒才知道的字母替换规律读信。在现在的密码学教科书上，我们仍然可以找到这种密码方法，即 Caesar 密码。这种密码系统是现代密码系统的雏形，蕴含了信息安全学科所强调的四种基本服务：机密性、认证性、数据完整性和不可抵赖性。

密码学在第二次世界大战期间也发挥了重要作用。1918 年，为了保护银行通信安全，德国人 Arthur Scheribius 发明了第一台被称为 ENIGMA 的非手工编码密码机。第二次世界大战期间，这种密码机的加密通信能力被德国人用于军事，为德军在战争初期的胜利起到了重要作用，让盟军大伤脑筋。后来，波兰人 Marian Rejewski 初步破解了 ENIGMA，随后，英国人 Alan Turing 更是终结了 ENIGMA，盟军随后开发了称为 Colossus 的机器，很多学者认为成功破解 ENIGMA 使得第二次世界大战得以提前一年结束。然而，密码学

作为一门科学则仅仅是近60多年的事情。1948年，Shannon发表了划时代的“通信的数学理论”，宣告了信息论的诞生。随后，Shannon发表了著名的“保密系统的通信理论”一文，用信息论观点对信息保密问题做了全面的论述。该文将密码学的研究纳入科学的轨道，同时，为对称密码学的构建提供直接的理论基础。

为了解决对称密码系统中密钥分发和管理问题，1976年，Diffie和Hellman在他们的经典论文《密码学的新方向》中提出了一种允许通信双方在不安全信道上安全地协商密钥的协议，即著名的Diffie-Hellman协议。在此基础上，他们提出了公钥密码学的概念。因此，这篇经典的论文成为密码学的研究和应用由传统走向现代的标志。虽然他们没有构造出一个具体的公钥密码系统，而只猜测其存在，但是他们的工作引起了密码学界的广泛关注。

1978年，Rivest、Shamir和Adleman提出了著名的RSA公钥密码体制，这是第一个实用的公钥密码体制，由于他们的杰出贡献，获得了2002年图灵奖。30多年来，虽然RSA公钥密码体制经历了风风雨雨，但仍然是目前应用最为广泛的密码体制之一。随后，其他学者和研究人员基于另外的数学困难问题提出了大量的公钥密码算法。其中的代表方案有：基于大整数分解问题的改进的RSA算法和Rabin算法、基于有限域上离散对数问题的ElGamal算法以及近来受到广泛关注的基于椭圆曲线的密码算法等。

近30多年来，公钥密码的研究如雨后春笋，研究学者们相继提出了一系列公钥密码算法，还提出了很多新的概念和应用，如数字签名、认证协议、基于身份的密码系统、数字签密等。在公钥密码领域也逐渐出现了很多研究课题，如具有附加性质的数字签名、门限密码系统、数字签密、基于身份的密码学、密钥管理等。在经历了几千年的历史后，密码学这门古老的艺术现在已经成为一门公开而活跃的学科。

1.2 密码学基本概念

密码学是主要研究通信安全保密的学科，它包括两个分支：密码编码学与密码分析学。密码编码学主要研究的是对消息进行变化，以保护信息在信道的传递过程中不被敌手窃取、解读和利用的方法；而密码分析学则恰恰相反，它主要研究如何分析和破译密码。这两个分支既相互对立，又相互促进。

1.2.1 保密通信系统

使用保密通信系统，两个通信伙伴可以保护需要发送的消息，使未授权者不能提取消息。发送方将要发送的消息称为明文，明文被变换成看似没有意义的随机消息，称为密文，这种变化过程称为加密；其逆过程，即由密文恢复出明文的过程称为解密。对明文进行加密时所采用的一组规则称为加密算法，相应的，对密文进行解密时所采用的一组规则称为解密算法。加密和解密算法的操作都是在一组密钥控制下进行的，分别称为加密密钥和解密密钥。传统密码体制所用的加密密钥和解密密钥相同或者从一个密钥容

易推导出另一个密钥，称其为单钥密码体制或对称密码体制。若加密密钥不相同或者从一个密钥难以推导出另一个密钥，则称为双钥密码体制或非对称密码体制。

在信息传输和处理过程中，除了预定的接收人外，还有非授权人，他们通过搭线窃听、电磁窃听、声音窃听等来窃取机密信息，称为截收者或敌手。敌手虽然不知道系统所用的密钥，但是通过分析，有可能从截获的密文推断出相应的明文或密钥，这样的工作成为密码分析。对一个保密通信系统采取截获密文进行分析的攻击称为被动攻击。还有一类攻击称为主动攻击，是指敌手可以采用添加、删除、重放、伪造等篡改手段向系统注入假消息，达到对系统进行攻击的目的。

一个保密通信系统由明文消息空间 M、密文空间 C、密钥空间 K_1 和 K_2、加密算法 $E_{k_1}: M \to C$ 和解密算法 $D_{k_2}: C \to M$ 组成，如图 1-1 所示。对于给定的明文消息 $m \in M$，密钥 $k_1 \in K_1$，加密算法把明文 m 变换成密文 c，即：

$$c = E_{k_1}(m), \quad m \in M, k_1 \in K_1$$

接收方利用解密密钥 k_2 和解密算法 D 对收到的密文进行解密，恢复出明文，即：

$$m = D_{k_2}(c), \quad m \in M, k_2 \in K_2$$

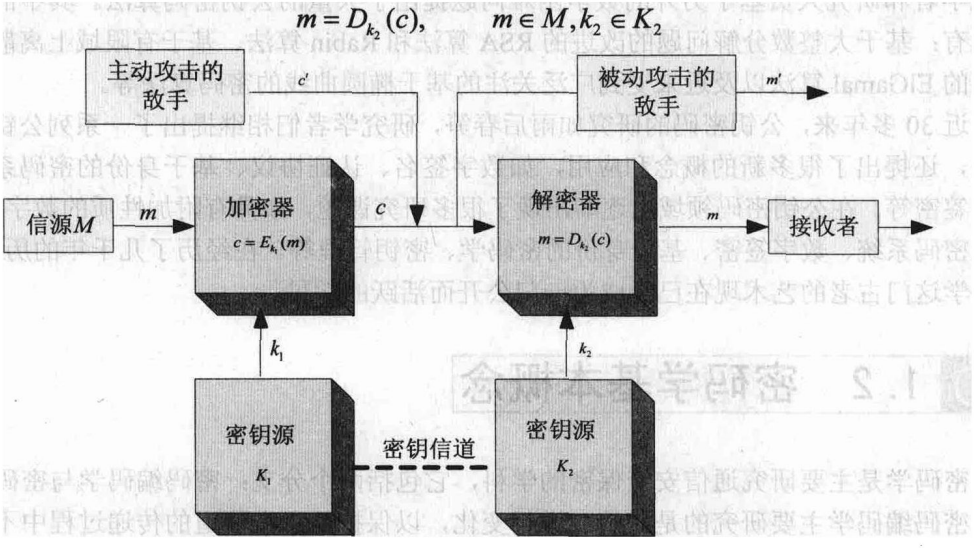


图 1-1　保密通信系统模型

1.2.2 密码体制分类

密码体制的分类有很多种，在此只介绍最常见的一种分类方法。按照加密算法与解密算法所使用的密钥是否相同进行分类，密码体制可以分为单钥密码体制和双钥密码体制。

如果一个保密系统的加密密钥相同，或者虽然不同，但是由其中的一个很容易推导出另一个，这样的密码体制称为单钥密码体制。采用单钥密码体制的系统的保密性主要依赖于密钥的保密性，与算法的保密性无关，算法是公开的，要求由密文和加解密算法得到相应的明文是困难的。根据单钥密码体制的这种特性，单钥加解密算法可由价格低

廉的芯片来实现。密钥可由发送方产生，然后通过安全的信道发送给接收方。单钥密码体制对明文消息的加密有两种方式，一种是明文消息按字符逐位地加密，称为流密码或序列密码；另一种是将明文消息分组，逐组地进行加密，称为分组密码。

如果一个保密系统的加密和解密分别使用不同的两个密钥，并且由加密密钥推导出解密密钥是计算上不可行的，这样的密码体制称为双钥密码体制，由 Diffie 和 Hellman 于 1976 年首先提出来。采用双钥密码体制的每个用户都有一对选定的密钥，一个是公开的，可以像电话号码一样进行注册公布，称为公钥；另一个是秘密的，称为私钥，因此，双钥密码体制又称为公钥密码体制。

1.2.3 密码攻击

敌手主要使用以下三种攻击手段对密码体制进行攻击。

1．穷举攻击

穷举攻击是对密码体制的一种最基本的攻击，又称为蛮力攻击，是指敌手依次试遍所有可能的密钥对所获密文进行解密，直至得到正确的明文；或者先确定一个密钥，然后对所有可能的明文进行加密，直到得到目标密文。从理论上来讲，对任何实用的密码体制，只要有足够的资源，都可以用穷举攻击将其攻破。1997 年 6 月 18 日，美国科罗拉多州以 Rocket Verser 为首的一个工作小组宣布，通过网络，利用数万台计算机，历时 4 个多月，通过穷举攻击攻破了 DES，这是穷举攻击的一个很好的例子。

2．统计分析攻击

统计分析攻击是指敌手通过分析密文和明文的统计规律来攻击密码系统，这种攻击曾经为密码破译作出过很大的贡献，许多古典密码体制都可以通过分析密文字母和字母组的出现概率和其他统计规律而被破译。抵抗这种攻击的方法是在密文中消除明文的统计特性。

3．数学分析攻击

数学分析攻击是指敌手针对加解密算法的数学特征和密码学特性，通过数学求解的方法来破译密码。根据敌手所拥有的数据资源来分类，有以下四种攻击方式：惟密文攻击、已知明文攻击、选择明文攻击和选择密文攻击。表 1-1 给出了不同类型的攻击以及敌手所掌握的不同资源。

表 1-1　数学分析攻击类型

攻击类型	敌手拥有的资源
惟密文攻击	加密算法；截获的密文
已知明文攻击	加密算法；截获的密文；某些明文—密文对
选择明文攻击	加密算法；截获的密文；自己选择的明文和由密钥生成的相应密文
选择密文攻击	加密算法；截获的密文；自己选择的密文和相应的由该密文解密得到的明文

惟密文攻击时，敌手获得信息最少，敌手仅根据公开的加密算法和截获的密文对密码系统进行破译，这对敌手很不利，因此，这类攻击最容易抵抗。已知明文攻击中的敌手除了拥有加密算法和截获的密文外，还知道某些明文—密文对。如果对一篇散文加密，敌手可能对其中的消息含义知之甚少。然而，如果对很特别的信息加密，敌手也许知道消息中的一部分。在选择明文攻击中，敌手能够自己选择明文并获得相应的密文，这是对敌手比较有利的一种攻击，因为敌手可以根据自己的需要选择密文。在选择密文攻击中，敌手可以根据需要选择密文，并能获得相应的明文，这是对敌手最有利的攻击，这种攻击的敌手具有最强大的攻击能力。

一个密码体制，如果无论敌手截获了多少密文和用什么手段进行攻击，都不能攻破，则称这样的密码体制是绝对安全的或者无条件安全的。无条件安全的密码体制在理论上是存在的，这就是著名的一次一密密码体制。然而，由于密钥管理的困难性，一次一密密码体制是不实用的。Shannon 指出，仅当密钥至少和明文一样长时，才能达到无条件安全。也就是说，除了一次一密密码体制以外，再无其他的绝对安全的密码体制。因此，加密算法只要满足以下两条准则之一就可以：

（1）破译密文的代价超过被加密信息的价值。

（2）破译密文所花费的时间超过信息本身的生命期。

满足以上两个准则的加密算法被称为计算安全。

1.3 古典密码体制

虽然从现在来看，很多古典密码是很不安全的，但是古典密码的设计思想对现代密码的设计仍有一定的借鉴作用，本节将介绍古典密码学的两大主要方法：代替密码和置换密码，并介绍几种著名的古典密码体制。

1.3.1 置换密码

在置换密码体制中，明文中的字或字母被重新排列，字或字母本身不变，但位置发生了改变，形成密文，又称为易位密码。最简单的易位密码是采用报文倒置法，即将报文按字的顺序依次倒置，并截成固定长度的字母组，形成密文，例如：

明文：never accept failure no matter how often it visits you

密文：uoys tisi vtin etfo wohr etta mone ulia ftpe ccar evne

倒置法是简单的易位密码，经不起攻击。

1.3.2 单表代替密码

代替密码是把明文中的每一个字符替换成密文字母表中的另一个字符，并使用密钥 K 与之进行运算，得到密文；接收者对密文进行逆运算就可以恢复出明文，代替密码主要

包括单表代替密码、多表代替密码和多名代替密码。本节将介绍几种典型的单表代替密码。

在单表代替密码中，只使用一个密文字母表，并且用密文字母表中的一个字母来代替一个明文字母表中的一个字母。设 A 和 B 分别为含 n 个字母的明文字母表和密文字母表：

$$A=\{a_0,a_1,\cdots,a_{n-1}\}$$

$$B=\{b_0,b_1,\cdots,b_{n-1}\}$$

定义一个由 A 到 B 的一一映射 $f:A\to B$：$f(a_i)=b_i$。

设明文 $M=(m_0,m_1,\cdots,m_{n-1})$，则密文 $C=(f(m_0),f(m_1),\cdots,f(m_{n-1}))$，下面介绍几种具体的单表代替密码。

1．加法密码

加法密码的映射函数为：

$$f(a_i)=b_i=a_j$$

$$j=i+k(\mathrm{mod}\,n)$$

其中，$a_i\in A$，k 是满足 $0<k<n$ 的正整数。

古罗马的凯撒大帝发明了著名的 Caesar 密码，其实质是一种加法密码，取 $k=3$，其密文字母表就是把明文字母表循环右移 3 位后得到的字母表。例如：

$$A=\{A,B,C,D,\cdots,W,X,Y,Z\}$$

$$B=\{D,E,F,G,\cdots,Z,A,B,C\}$$

明文：MING TIAN BA DIAN ZHAN DOU

密文：PLQJ WLDQ ED GLDQ CKDQ GRX

2．乘法密码

乘法密码的映射函数为：

$$f(a_i)=b_i=a_j$$

$$j=ik(\mathrm{mod}\,n)$$

其中，k 与 n 互素。因为仅当 $(k,n)=1$ 时，才存在两个整数 x、y，使得 $xk+yn=1$，此时，$xk=1(\mathrm{mod}\,n)$，进而 $i=xj(\mathrm{mod}\,n)$，这样才能正确解密。

3．仿射密码

乘法密码和加法密码相结合便构成仿射密码，其映射函数为：

$$f(a_i)=b_i=a_j$$

$$j=k_0+ik_1(\mathrm{mod}\,n)$$

其中 $(k_1,n)=1$ 且 $0<k_0<n$。

更复杂的多项式密码可以这样构造：

$$f(a_i)=b_i=a_j$$

$$j=k_0+ik_1+\cdots+i^{t-1}k_{t-1}+i^tk_t(\mathrm{mod}\,n)$$

其中 $(k_i,n)=1$，$i=1,2,\cdots,t$，且 $0<k_0<n$。

4．密钥短语代替密码

这种密码选用一个英文短语或者单词串作为密钥，称为密钥字或密钥短语，例如