XIANDAI
MIMAXUE
JICHU LILUN YU YINGYONG

现代密码学

基础理论与应用

张键红　编著

电子科技大学出版社

现代密码学基础理论与应用

张键红　编著

电子科技大学出版社

图书在版编目（CIP）数据

现代密码学基础理论与应用/ 张键红编著 . ——成都：
电子科技大学出版社，2011.4
ISBN 978-7-5647-0717-0

Ⅰ. ①密… Ⅱ. ①张… Ⅲ. ①密码学－理论－应用
Ⅳ. ①TN273.4

中国版本图书馆 CIP 数据核字(2010)第 217470 号

内容简介

应用密码技术是电子安全系统的关键技术，它主要实现保密性、完整性和不可否认性。本书包括密码算法、密码协议及使用方面的主要内容：密码学基础、公钥密码算法、数字签名、序列密码、密钥建立、密钥管理、电子邮件安全等。每章附有阅读资料，部分章节配有习题。本书是在讲授多年的讲义的基础上形成的，可以作为高等学校计算机科学、通信工程、信息安全等专业的本科教材，也可以供有关工程技术人员参考。

现代密码学基础理论与应用

张键红　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：朱　丹
责任编辑：辜守义
主　　页：www.uestcp.com.cn
电子邮箱：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×260 mm　　印张 13　　字数 320 千字
版　　次：2011 年 4 月第一版
印　　次：2011 年 4 月第一次印刷
书　　号：ISBN 978-7-5647-0717-0
定　　价：28.00 元

前　言

随着 20 世纪科学技术的发展，特别是信息科学技术的发展，人们的生活已经进入了信息化社会。信息在我们的生活中无处不在，在信息给我们带来便利的同时，我们也面临着一系列重要问题：信息安全吗、可信吗、是真的吗？这与人们的经济利益和个人隐私，也与国家的政治利益和经济利益息息相关。各国政府都非常重视信息和网络安全，信息安全已成为一个世纪性、全球性的研究课题。

当我国的信息安全事业蓬勃发展之际，国家的重视、政府的支持、经济的需要使得我国的信息安全产业得到快速发展。在信息安全产业快速发展的同时，社会对信息安全人才的需求在不断增加，高等教育对信息安全的专业化教育的推进，将对信息安全的发展具有积极促进作用。

本书针对高等院校的信息与计算机类相关专业本科生所开设的课程特点，编者结合近几年在密码学与信息安全方面的教学实践和科研情况，广泛汲取了各类教材的特色而精心编著了本教材。本教材以培养学生对密码学的认知能力为目标，突出密码技术的实用性，尽量避免传统密码教材的数学原理和理论分析而应用性偏弱的局限，并对一些需要数学知识可能过于深奥的知识点，如密码学的信息论基础、序列密码以及密码分析等内容进行了简化，重点选择了一些具有典型意义和常用的密码体制和算法进行介绍，并在每章最后均配一些习题以帮助学生掌握和巩固重要知识点，使其更加易于课堂教学的实施和学生阅读，激发学生潜在的学习积极性。

本教材的主要特色：可读性强、结构合理、强调基础、注重应用，不求面面俱到，力求使学生能够较快掌握密码技术的核心内容。全书共分为 7 章，其具体章节内容安排如下：

第 1 章主要介绍密码技术发展概况以及密码学的基本概念，包括密码学的发展、密码系统的原理、密码系统攻击以及密码体制的分类等内容。

第 2 章介绍密码学的一些相关数学知识和数学困难问题，包括近代代数、计算复杂性和数论方面的基础知识以及入离散对数、大数分解、子集等问题。

第 3 章主要对序列密码进行了介绍，包括序列密码的基本原理及模型、线性反馈移位寄存器 LFSR、基于 LFSR 的序列密码和几种典型序列密码算法，以及序列密码在现实生活中的应用和破译。

第 4 章对几种经典的公钥密码体制的原理、安全性和基本概念进行了介绍，包括 RSA 公钥体制、Merkle-Hellman 背包公钥体制、Rabin 公钥密码体制、ElGamal 公钥系统、McEliece 公钥密码、椭圆曲线密码体制（ECC）和多变量密码的基本原理与应用等内容。

第 5 章对数字签名的原理、攻击类型和不同类型的签名方案进行了介绍，主要介绍了 RSA，DSS 等几种常见的数字签名，以及代理签名、环签名等不同类型的签名。

第 6 章对密钥管理和几种经典的密钥协议进行了介绍，如：密钥的分类，密钥的分配、

公布、生命期和零知识证明技术与密钥协议的攻击类型等。

第 7 章对电子邮件的安全技术进行了介绍，包括 PGP 的工作原理、安全体制，密钥管理以及 MIME/SMIME E 协议的格式、内容、安全功能等，也包含 PGP 软件的安全装、使用。

由于密码学所涉及的数学知识较多，如信息论、概率论、近代代数和数论等方面的数学知识。希望学习本书的读者须具备一定的数学基础知识，学习和了解这方面的数学知识对研究和学习应用密码学是大有帮助的，但即使没有学过这些数学知识也不会影响对本书的阅读和学习。

本书语言通俗易懂，内容丰富翔实，可作为信息安全、计算机科学与技术、信息与计算科学、通信工程、网络工程以及电子商务等信息技术类本/专科专业密码学课程的教材，也适合初学密码学的研究生及从事信息安全、计算机、通信、电子工程等领域的科技人员阅读参考。

本书由北方工业大学图形和模式识别研究所组织编写，全书由邹建成教授和张键红副教授负责组织与统稿工作。第 1、2、7 章由张键红负责编写；第 3 章由苏秀娜负责编写；第 4 章由刘雪负责编写；第 5 章和第 6 章分别由高胜楠和陈华编写。本书的编写还从其他老师和同行的有关著作和教材（包括网站）中得到了帮助，作者在此一并表示由衷的感谢。

尽管作者已尽了最大努力，但由于作者的学识和水平，书中难免有需要商榷之处，诚望读者不吝赐教斧正。笔者的电子邮箱：jhzhang@ncut.edu.cn。

作　者

2010 年 8 月

目　　录

第 1 章　绪　　论

密码学是一种研究密码系统和通信安全的一门科学，最初被运用于军事和政治方面，它具有悠久的历史，但是，它仍是一个年轻而令人兴奋的、不断出现变化和新挑战的领域。在不同时期、不同的环境下，随着不同的需求，它的功能也发生着重要变化，在人们的日常生活中越来越发挥着重要作用。本章将对密码学的发展历史、基本概念、密码体制的分类进行介绍。

1.1　密码学的历史

密码学是一个古老的学科，最早可以追溯到 4000 多年以前。在公元前 5 世纪，古希腊斯巴达出现原始的密码器，用一条带子缠绕在一根木棍上，沿木棍纵轴方向写好明文，解下来的带子上就只有杂乱无章的密文字母。解密者只需找到相同粗细的木棍，再把带子缠绕上去，沿木棍纵轴方向即可读出有意义的明文。这是最早的换位密码术。

后来，在公元前 1 世纪，作为一种简单易行的单字母替代密码，著名的恺撒（Caesar）密码在高卢战争中被广泛应用。

密码破译是随着密码的使用而逐步产生和发展的。1412 年，波斯人卡勒卡尚迪所编的百科全书中载有破译简单代替密码的方法。到 16 世纪末期，欧洲一些国家设有专职的破译人员，以破译截获的密信，使密码破译技术有了相当的发展。1863 年普鲁士人卡西斯基所著的《密码和破译技术》，以及 1883 年法国人克尔克霍夫所著的《军事密码学》等著作，都对密码学的理论和方法做过一些论述和探讨。1949 年美国人香农发表了《秘密体制的通信理论》一文，应用信息论的原理分析了密码学中的一些基本问题。

在公元 20 世纪初的第一次世界大战期间，英国破译密码的专门机构“40 号房间”利用缴获的德国密码本破译了著名的“齐默尔曼电报”，促使美国放弃中立参战，改变了战争进程。在第二次世界大战中，波兰人和英国人破译了德国著名的“恩格玛”密码机密码，使德国的许多重大军事行动对盟军都不成为秘密；后来，美国人破译了被称为“紫密”的日本“九七式”密码机密码，使得美军炸死了偷袭珍珠港的元凶日本舰队总司令山本五十六，并且以劣势兵力击破日本海军的主力，扭转了太平洋地区的战局。因此，密码技术在两次世界大战中充当着一个举足轻重的角色。

在 1977 年 1 月 15 日，美国国家标准局颁布了对计算机系统和网络进行加密的数据加密标准 DES（Data Encryption Standard 数据加密标准）并于 1997 年 7 月 15 日生效，这是密码学历史上一个具有里程碑意义的事件。

在 1976 年，当时在美国斯坦福大学的迪菲（Diffie）和赫尔曼（Hellman）两人提出了公开密钥密码的新思想（论文“New Direction in Cryptography”），把密钥分为加密的公钥和

解密的私钥，开辟了公钥密码体制的新纪元。

1969 年，哥伦比亚大学的 Stephen Wiesner 首次提出了“共轭编码”（Conjugate Coding）概念。

1977 年，美国的里维斯特（Ronald Rivest）、沙米尔（Adi Shamir）和阿德勒曼（Len Adleman）提出第一个较完善的公钥密码体制——RSA 体制，这是一种建立在大数因子分解基础上的算法。

1984 年，Bennett.Chareles H，Brassard. Gille 在 Wiesner 的思想启发下，首次提出了基于量子理论的 BB84 协议，由此，量子密码理论就诞生了（注：量子密码不同于以前的密码技术，它是一种可以发现窃听行为、安全性基于量子定律的密码技术，可以抗击具有无限计算能力的攻击）。

1985 年，英国牛津大学物理学家戴维•多伊奇（David Deutsch）提出量子计算机的初步设想，这种计算机一旦造出来，可在 30 秒钟内完成传统计算机要花上 100 亿年才能完成的大数因子分解，从而破解 RSA 运用这个大数产生公钥来加密的信息。

1985 年，美国的贝内特（Bennet）根据关于量子密码术的协议，在实验室第一次实现了量子密码加密信息的通信。尽管通信距离只有 30cm，但它证明了量子密码术的实用性，与一次性便笺密码结合，同样利用量子的神奇物理特性，可产生连量子计算机也无法破译的绝对安全的密码。

1985 年，N.Koblitz 和 V.Miller 把椭圆曲线理论应用到攻钥密码技术中，使得公钥密码技术得到进一步的发展，成为了公钥密码技术研究的新方向。

2003 年，位于日内瓦的 id Quantique 公司和位于纽约的 MagiQ 技术公司，推出了传送量子密钥的距离超越了贝内特实验中 30cm 的商业产品。日本电气公司在创纪录的 150km 传送距离的演示后，在 2004 年向市场推出产品。IBM、富士通和东芝等企业也在积极进行研发。目前，市面上的产品能够将密钥通过光纤传送几十公里。美国的国家安全局和美联储都在考虑购买这种产品。MagiQ 公司的一套系统价格在 7～10 万美元之间。

2001 年 11 月 26 日，美国国家标准与技术研究院（NIST）颁布了一种新的分组加密标准来替代原先的 DES 算法，即高级加密标准（Advanced Encryption Standard，AES），并于 2002 年 5 月 26 日生效。在 2006 年，高级加密标准已然成为对称密钥加密中最流行的算法之一。

2004 年，中国科技大学郭光灿院士领导的中科院量子信息小组在北京与天津之间成功实现了 125km 光纤的点对点的量子密钥分配，解决了量子密码系统的稳定性问题。

2004 年 8 月，在美国加州圣芭芭拉召开的国际密码大会上，中国山东大学的密码专家王小云教授成功地破译了四大著名的密码算法 MD5、HAVAL－128、MD4 和 RIPEMD。不久又破译了被美政府广泛应用的计算机密码系统 SHA-1 密码算法。

1.2 密码学的基本概念简介

密码学是研究密码的编制和密码破译的技术科学。研究密码变化的客观规律，并应用于编制密码来实现秘密通信，称为密码编码学（Cryptography）；应用于破译密码以获取通信情报的或伪造一个假消息使得能通过密码系统验证的，称为密码破译学（Cryptanalysis）。其总

称为密码学。

一个密码系统是通信双方按约定的法则进行明文（plaintext）和密文（ciphertext）进行特殊变换的一种保密手段。依照这些约定的法则，发送者通过加密钥（K）把明文转换为密文，这个过程称为加密变换（encryption permutation）；接收者利用解密钥（K′）把密文恢复为明文，这个过程称为解密变换（decryption permutation）。图 1-1 所示表明了这个过程。

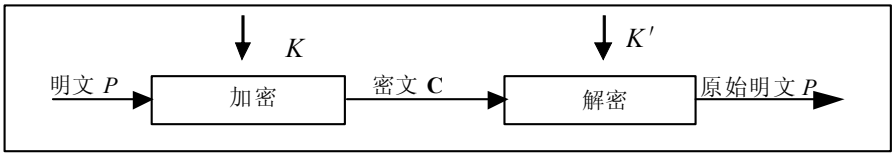

图 1-1　加密和解密模型

在通常情况下，明文用 M（消息）或 P（明文）表示，它可能是比特流（文本、位图、图像、数字化的语音流或数字化的视频图像）。至于涉及计算机时，P 是简单的二进制数据流，明文可被传送或存储。无论在哪种情况，M 表示待加密的消息。

密文通常用 C 表示，它也是二进制数据流，有时和 M 一样大，有时稍大（通过压缩和加密的结合，C 有可能比 P 小些；然而，单单加密通常达不到这一点）。加密函数 E 作用于 M 得到密文 C，用数学表示为：

$$E（M）=C$$

相反地，解密函数 D 作用于 C 产生 M

$$D（C）=M$$

先加密后再解密消息，原始的明文将恢复出来，下面的等式必须成立：

$$D（E（M））=M$$

从数学的角度来讲，一个密码系统就是一族映射，它在密钥的控制下将明文空间中的每一个元素映射到密文空间上的某个元素。这族映射是由密码方案确定，具体使用哪一个映射是根据不同密钥的选择而决定的。

在实际应用中，一般把密码方案与密钥共同看成控制密码系统的“密钥”，只不过密码方案是固定的“密钥”，密钥是系统的可变“密钥”。将“密钥”中的固定部分与可变部分区分开来对于密码分析以及密钥管理等具有重要意义。

图 1-1 所示是理想情况下的加解密模型，但是在现实生活中，通信信道是开放的，可能存在着一个入侵者来攻击该模型，因此，实际的加解密模型必须考虑存在攻击的情况。那么存在攻击者的加解密模型就变为如图 1-2 所示。

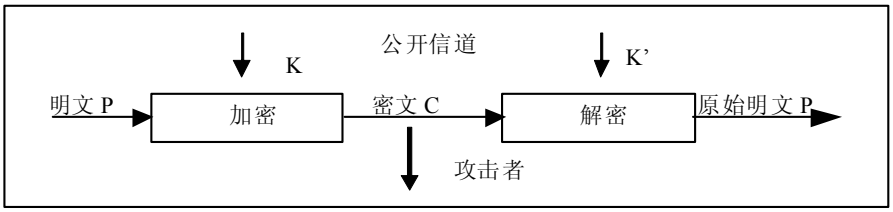

图 1-2　加密和解密模型

一般而言，一个密码系统依据其应用可以提供以下功能：

1）秘密性（privacy）：一个非法的用户不能从一个密文中恢复明文。

2）鉴别性（authenticity）：消息的接收者应该能够确认消息的合法来源，攻击者不可能伪装成他人来欺骗接收者。

3）完整性（Integrity）：消息的接收者应该能够验证在传送过程中消息没有被篡改，入侵者不可能用假消息代替合法消息。

4）不可否认性（Nonrepudiation）：发送者事后不可能虚假地否认他发送的消息。

在传统的密码学中，往往注重消息的秘密性。但是近代密码学认为信息的鉴别性、完整性和不可否认性在现实生活中的应用比秘密性更重要。

1.3 密码系统设计的理论基础和攻击类型

密码系统设计的理论为混淆（confusion）与扩散（diffusion），最早是由 C.E.Shannont 提出的。其主要目的是为了抵抗对手对密码体制的统计分析，在设计分组密码中，可以充分利用扩散和混淆来有效地抵制对手从密文的统计特性中推测出明文或密钥。 一般密码体制的实现的方式是先混淆，再扩散，最后再进行反混淆。

扩散是指更改任何明文（或信息）的单个位元均会影响到所有其他的密文（或签名章）位元，这样可以隐蔽明文的统计特性。当然，理想的情况是让明文中的每一个位元的变化影响密文中的所有位元。因此，扩散特性是密码学安全的主要核心所在。

混淆就是将密文与密钥之间的统计关系变得尽可能复杂，使得对手即使获取了关于密文的一些统计特性，也无法推测密钥，使用复杂的非线性代替变换可以达到比较好的混淆效果，而简单的线性代替变换得到的混淆效果则不理想。乘积和迭代有助于实现扩散和混淆。选择某些较简单的受密钥控制的密码变换，通过乘积和迭代可以取得比较好的扩散和混淆效果。

密码技术的安全理论包括无条件安全（unconditional security）与有条件安全（conditional security）。无条件安全是指经过理论（theoretical）及正规化（formal）程序证明安全性，其大多以 Random Oracle 作为证明的基础。主要由于密文没有泄露足够多的明文信息，因此，无论计算能力有多大，都无法由密文唯一确定明文。例如，仅处理一个位元或计算基本单位 one-time pad。有条件安全是指破解方法已知，但在计算复杂度上不可行，即给定可用的处理速度及存储器，还是很难在合理时间内破解出结果。例如，一些著名的数学难题，如因数分解（factorization）、离散对数（discrete logarithm）与椭圆曲线（elliptic curve）等。

一个密码系统破译复杂度评估主要包括数据复杂度（data complexity）、计算复杂度（computation complexity）、存储复杂度（memory complexity）与成本效益度量（cost effective）。数据复杂度方面是指所需的数据量大小与数据结构本身所具有的复杂度；计算复杂度是指所需的处理器能力或所需的计算时间的大小；存储复杂度是指破译该密码系统所需的存储量的大小（包括 main memory 与 disk memory）；成本效益度量是指所花费人力、物力成本与所获得效益的比较。

根据破译的程度，密码系统破译可分为完全破解（total break）、全域推断（global inference）、局部推断（local inference）与信息推断（information inference）。具体解释如下：

- 安全破解：可以得到密钥（尤其是私钥）或完全掌握密钥产生算法或计算出任一组合法下的公钥/私钥对。
- 全域推断：找到一个替代的密码演算法并可以得到原先演算法所产生的任何相同结

果。

- 局部推断：可以从某一个局部密文中去推导出所对应的明文，例如填字游戏。
- 信息推断：可以从一些密文中去推断出有关明文或密钥的信息（可能并没有得到真正的密钥或密文）。

下面我们将介绍密码破译的不同分析方法。

- 唯密文攻击（ciphertext-only attack）：已知一些密文和加解密算法，攻击者可以从中推导出所有的明文或密钥，或从某一个密文中推导出所对应的明文。
- 已知明文攻击（known-plaintext attack）：已知一些明文和密文对，攻击者可以从中推导出密钥，或利用这些明文—密文对应关系从某一个密文中推导出所对应的明文。注：在明文攻击中，攻击者对其所拥有的明文-密文对里的明文没有选择和控制权力。
- 选择明文攻击（chosen-plaintext attack）：已知一些预先选择好的明文和相对应的密文，攻击者可以从中推导出密钥，或从某一个密文中推导出所对应的明文。
- 自适应选择明文攻击（adaptive chosen-plaintext attack）：攻击者不仅仅可以预先选择明文，而且还可以根据先前选择的明文得到对应的密文来调整将要选择的明文。显然，该攻击比选择明文攻击更强。
- 选择密文攻击（chosen-ciphertext attack）：在未知密钥或私钥的前提下，可以选择密文并得到对应的明文，利用选择的密文和明文的对应关系可以推导出某一个密文所对应的明文。
- 选择密钥攻击（chosen-key attack）：可以从某些已知密钥中获得密钥的产生关系，进而可以得到某一公钥对应的私钥。
- 穷密钥搜索（exhaustive key search attack）：在理论上很简单，对每个密钥进行测试，计算复杂度决定于密钥空间的大小。
- 暴力攻击（human force attack）：以人为暴力手段迫使密钥持有人交出密钥。

到目前为止，能抵制穷举搜索攻击的安全密钥长度是：在对称密钥系统中密钥长度为128 比特；在公钥密码系统中密钥长度为 1024 或 2048 比特。表 1-2 所示为密钥长度对应表。

表 1-1　密钥长度的对照表

对称密钥系统	公钥密码系统
56 bits	384 bits
64 bits	512 bits
80 bits	768 bits
112 bits	1792 bits
128 bits	2304 bits

上面所述的每种攻击的目的决定所使用的密钥。这几种攻击类型的强度是逐步递增的，唯密文攻击是一种最弱的攻击。

“一次一密”的密码体制在唯密文攻击下是安全的（无条件安全的密码系统在唯密文攻击下是绝对安全的），但是，它却不能抵制已知明文攻击。这是因为密钥 K 可以由明文 M 和密文 C 进行模 2 运算获得。

由于“一次一密”密码体制无法抵制已知明文攻击，所以就要求每发送一条信息就要产

生一个新的密钥，那么，就需要一个密钥本来保存这些密钥；同时，这个密钥本必须通过一个安全的信道传送到信息的接收端，这给密钥管理带来了很大的难度。虽然“一次一密”密码使用起来不方便，且有很大的局限性，但是，由于它能提供很高的安全性，“一次一密”乱码本在今天仍有应用场合，主要用于高度机密的低带宽信道。美国和苏联之间的热线电话据传就是用“一次一密”乱码本加密的。许多苏联间谍传递的消息也是用“一次一密”乱码本加密的。

由此可知，我们要设计一个安全的密码系统必须满足以下要求：

（1）密码系统的密钥空间必须足够大：因为，如果密钥空间不够大的话，一个攻击者可以采用已知明文甚至唯密文攻击穷举整个密钥空间从而可以攻破整个密码系统。注：在攻击时，攻击者通过判断解密密文所获得的明文是否有意义来判断攻击是否成功。

（2）加密与解密过程必须在多项式时间内完成，使得用户能够方便地实现和使用。

（3）密码系统的安全性取决于密钥，当密码算法被公开而密钥没有被泄漏的情况下，整个密码系统还是安全的。

另外，对密码系统还存在一些其他要求，如：能够抵抗已经出现的一些攻击方法； 加密后得到的密文长度与明文的长度的比值尽可能地接近 1；对于不同级别的密码系统，选择合适的密钥长度。

1.4 密码体制的分类

密码体制从原理上可分为私用密钥加密技术（对称加密）和公开密钥加密技术（非对称加密）。

（1）对称密码体制 symmetric cryptosystem

对称密码体制是一种传统密码体制，也称为私钥密码体制。在对称加密系统中，加密和解密采用相同的密钥。因为加解密密钥相同，需要通信的双方必须选择和保存他们共同的密钥，各方必须信任对方不会将密钥泄密出去，这样就可以实现数据的机密性和完整性。因此，单钥体制系统的安全性取决于密钥的安全性，与算法的安全性无关。根据单钥密码体制的这种特性，一般单钥加解密算法可以通过低费用的芯片来实现。对于具有 n 个用户的网络，需要 n（n－1）/2 个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大、分布很广时，密钥的产生、分配、保存、销毁就成了问题，处理不好会严重影响系统的安全性。对机密信息进行加密和验证随报文一起发送报文摘要（或散列值）来实现。比较典型的算法有 DES（Data Encryption Standard 数据加密标准）算法及其变形 Triple DES（三重 DES）；GDES（广义 DES）；欧洲的 IDEA；日本的 FEALN、RC5 等。DES 标准由美国国家标准局提出，主要应用于银行业的电子资金转帐（EFT）领域。DES 的密钥长度为 56bit。Triple DES 使用两个独立的 56bit 密钥对交换的信息进行 3 次加密，从而使其有效长度达到 112bit。RC2 和 RC4 方法是 RSA 数据安全公司的对称加密专利算法，它们采用可变密钥长度的算法。通过规定不同的密钥长度，C2 和 RC4 能够提高或降低安全的程度。对称密码算法的优点是计算开销小、加密速度快，是目前用于信息加密的主要算法；它的局限性在于它存在着通信的贸易双方之间确保密钥安全交换的问题。此外，某一贸易方

有几个贸易关系，他就要维护几个专用密钥。它也没法鉴别贸易发起方或贸易最终方，因为贸易双方的密钥相同。另外，由于对称加密系统仅能用于对数据进行加解密处理，提供数据的机密性，不能用于数字签名，因而，人们迫切需要寻找新的密码体制。

（2）非对称密码体制 asymmetric cryptosystem

非对称密码体制也叫公钥加密技术，是由 Diffie 和 Hellman 于 1976 年首次引入的，该技术就是针对私钥密码体制的缺陷被提出来的。在公钥加密系统中，加密和解密是相对独立的，并且加密和解密使用的是两把不同的密钥，加密密钥（公开密钥）可以向公众公开，谁都可以使用，解密密钥（秘密密钥）只有解密人自己知道，非法使用者根据公开的加密密钥无法推算出解密密钥，因此，称为公钥密码体制。如果一个人选择并公布了他的公钥，另外任何人都可以用这一个公钥来对消息加密并以密文的形式把消息传送给那个人。私钥是秘密保存的，只有私钥的拥有者才能利用私钥对密文进行解密。公钥密码体制的算法中最著名的代表是 RSA 系统，此外还有：背包密码、McEliece 密码、Diffe_Hellman、Rabin、零知识证明、椭圆曲线、EIGamal 算法等。公钥密钥的密钥管理比较简单，并且可以方便地实现数字签名和验证，但算法复杂，加密数据的速率较低。公钥加密系统不存在对称加密系统中密钥的分配和保存问题，对于具有 n 个用户的网络，仅需要 2n 个密钥。公钥加密系统除了用于数据加密外，还可以实现数字签名功能实现用户身份的认证。公钥加密系统可提供以下功能：A.、机密性（Confidentiality）：保证非授权人员不能非法获取信息，通过数据加密来实现；B．确认（Authentication）：保证对方属于所声称的实体，通过数字签名来实现；C．数据完整性（Data integrity）：保证信息内容不被篡改，入侵者不可能用假消息代替合法消息，通过数字签名来实现；D．不可抵赖性（Non-repudiation）：发送者不可能事后否认他发送过消息，消息的接受者可以向中立的第三方证实所指的发送者确实发出了消息，通过数字签名来实现。可见公钥加密系统满足信息安全的所有主要目标。

非对称密码体制功能相当强大，似乎它的强大使得对称密码体制显得微不足道了，但是，非对称密码体制所带来的是不自由和高计算的代价。在非对称密码算法中所需要的计算量比一般的对称加密算法如 DES 或 AES 计算量多几个幂的数量级。一种重要的原则是非对称密码适合数据量不大的加密，对称密码适合数据量大的加密，因此，在应用中，对称密码用来加密所要传送的信息，而非对称密码用来传递加密信息的对称钥。

（3）非密钥体制 no-key cryptosystem

在这种体制中，通常是为了实现消息或身份的认证或随机化，常用的方法有 one-way 函数、随机产生器、MAC 码等。它们一般在密码系统中作为一个模块来实现功能。

因此，根据实现方法的不同，密码系统的分类如图 1-3 所示。

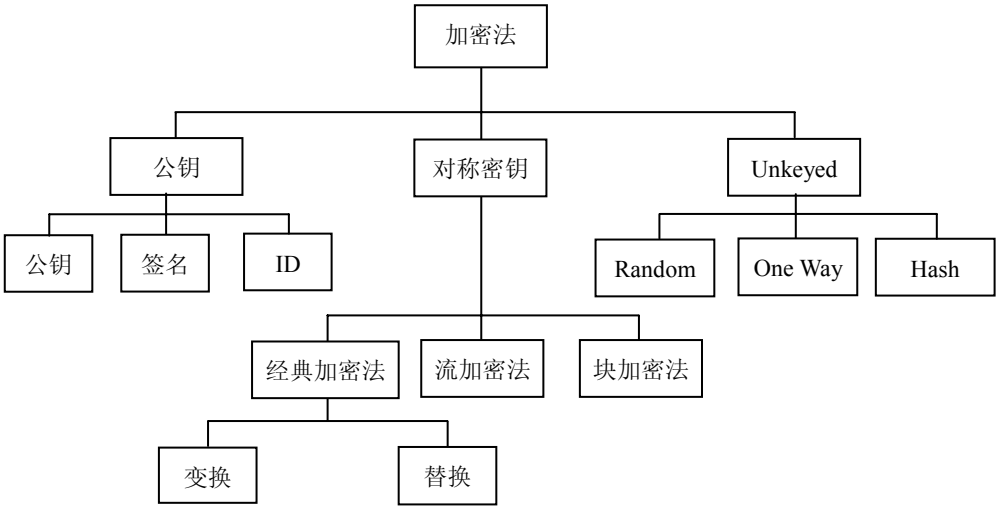

图 1-3　密码系统的分类

上面所提到的密码体制的安全性大多是基于计算数学困难的问题，随着量子计算机研究的发展将会对传统的密码体制构成巨大的威胁。如何构造更安全的能够抵制量子计算机攻击的密码成了现在人们研究的另一个重要问题，这就出现了后量子密码体制。2006 年 5 月，在比利时召开了第一届抗量子密码学会议，针对公钥密码应对量子计算机的挑战主要有以下三个策略：

1）采用不能转换成离散傅立叶变换的数学难题来建立公钥体制。

2）用量子密码来替代传统的公钥密码体制。然而，建立量子密码系统需要较大的代价，并且它不能实现传统密码的所有功能。

3）用对称密码的签名来取代公钥密码的签名。

针对第一类策略，目前，抗量子计算的公钥密码主要有以下三种类型：

①NTRU 公钥密码体制　目前，相对成熟的抗量子计算的公钥密码是由美国数学家 Hoffstein、Pipher 和 Silverman 在 1998 年发明的。它的加密使用基于多项式代数和对数 p，q 约化模的混合系统，而解密使用基于概率论的非混合系统。NTRU 的安全性基于多项式、不同模混合运算的相互作用和从一个非常大的维数格中寻找最短向量的困难性。但至今 NTRU 尚未获得广泛的应用，其原因在于：首先是它的安全性还没有获得充分认同，其签名的安全性远远低于加密的安全性，不适合应用于网络信任体系；其次是知识产权的障碍，NTRU 公司在多个国家注册了基础性专利，我国大范围使用也涉及专利障碍。

②OTU2000 公钥密码体制　最初的设计思路由 Okamoto、Tanaka 和 Uchiyama 在 2000 年提出，具体技术方案由日本 NTT 实验室开发。其缺点是产生密钥需要计算离散对数，从而需要用量子计算机来解决密钥生成问题，因此，目前的可行性不够。

③MQ 公钥密码体制　即多变量二次多项式公钥密码体制（Multivariate Quadratic Polynomials in Public Key Cryptosystem），它基于有限域上的多变元二次多项式方程组的难解性。MQ 是一大类各具特色的公钥密码算法的统称。最早的 MQ 算法发表于 1985 年，由于早期的 MQ 算法被破译，使得一直受到冷落。2000 年以后，出于抗量子计算攻击的考虑，