密码学

MIMAXUE

宋震　等编著

中国水利水电出版社
www.waterpub.com.cn

MIMAXUE
MIMAXUE

密码学

宋震　等编著

中国水利水电出版社

内 容 提 要

本书是一本面向初学者的密码学书籍。

在本书的前一部分，主要讲述了密码学及密码工程中的一些基础知识，如密码学的基本概念、密码体制的分类以及所用到的数学知识。然后，对各种密码体制的基本概念与原理进行简要的讨论，如古典密码体制、流密码、分组密码体制、公开密钥密码体制等，并详细描述各种密码体制中典型的密码算法过程及其安全性。

本书结构紧凑，语言严谨，论述清晰，条理性强。在内容的安排上由浅入深，详略得当，并且有丰富的算法实例，使理论与实践相结合。适于用作各大专院校相关专业教材。

图书在版编目（CIP）数据

密码学/宋震等编著. —北京：中国水利水电出版社，2002

ISBN 7-5084-1116-1

Ⅰ. 密… Ⅱ. 宋… Ⅲ. 密码—理论 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字（2002）第 037589 号

书　　名	密码学
作　　者	宋震　等编著
出版、发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@public3.bta.net.cn（万水） sale@waterpub.com.cn 电话：（010）68359286（万水）、63202266（总机）、68331835（发行部）
经　　售	全国各地新华书店
排　　版	北京万水电子信息有限公司
印　　刷	北京北医印刷厂
规　　格	787×1092 毫米　16 开本　11.75 印张　253 千字
版　　次	2002 年 7 月第一版　2002 年 7 月北京第一次印刷
印　　数	0001—4000 册
定　　价	18.00 元

凡购买我社图书，如有缺页、倒页、脱页的，本社发行部负责调换

前　言

密码学的研究内容十分广泛。作为一本面向初学者与非专业人员的密码学书籍，本书只讲述密码学及密码工程中的一些基础知识，对各种密码体制的基本概念与原理进行简要的讨论，并详细描述各种密码体制中典型的密码算法过程及其安全性。

本书的组织与结构如下：

第 1 章主要讲述密码学的基本概念、密码体制的分类、密码学的发展历史。

第 2 章将讲述本书讲述内容中一些基础的数学知识，包括数论基础、代数基础、计算复杂性理论基础等内容。

第 3 章介绍古典密码体制中一些典型的密码体制。虽然这些密码体制已经很少使用，但对这些密码体制的讨论将有助于我们理解、构造和分析现代实用的密码。

第 4 章讲述的内容是流密码。流密码将消息以比特（或字符）为单位，逐比特（或字符）对明文进行加密。流密码多用于政府、军方等国家要害部门。深入地了解流密码需要较多的数学理论知识，因此，本书将仅从分类、结构、模型上对流密码进行简单的介绍，并介绍两个典型的流密码算法：A5 与 SEAL。

第 5 章主要讨论分组密码体制。分组密码体制将明文消息划分为一个一个的分组，逐分组地完成加密变换。分组密码是目前在商业领域比较重要而流行的一种加密体制，它广泛地应用于数据的保密传输、加密存储等应用场合。在第 5 章中，本书将介绍分组密码体制的基本概念、典型结构、工作方式，同时，对一些重要且流行的加密算法，如 DES、IDEA、RC5 以及 AES，进行详细地讨论。

第 6 章将介绍公开密钥密码体制。公开密钥密码体制是 1976 年 Diffie 与 Hellman 的《密码学的新方向》一文所提出的一种新的密码体制，该技术为通信安全带来了革命性的变化。本书第 6 章首先分析、讨论了公开密钥密码设计原理，随后介绍了几个目前已经处于实用化阶段的、常用的公开密钥密码算法，包括 RSA、ElGamal、椭圆曲线密码体制等，并对部分算法的实现细节进行了一些讨论。

第 7 章主要讨论单向散列函数。单向散列函数是不可逆的密码体制，它可以被用作防止主动攻击以保证明文消息的完整性，另外它还用于数字签名等领域。第 7 章阐述了单向散列函数的基本概念、技术要求、基本设计方法等，并讨论了目前使用比较广泛的几种散列函数，如 MD5 与 SHA-1 等，最后，该章还介绍了使用了密钥的单向散列函数的一些有关概念与算法。

第 8 章将讲述数字签名。数字签名是密码学应用的一个重要方面，数字签名广泛地被用于身份认证、数据完整性、不可否认性及匿名性等安全实践中。数字签名可分为普通签名与

应用于具有特殊要求场合的特殊签名，本书只对普通签名进行一些介绍。该章在介绍数字签名的基本概念及基于公开密钥密码算法构建数字签名方案的基本原理之后，讨论了一些常用的数字签名体制，如 RSA 签名体制、ElGamal 签名体制、DSS 数字签名标准等。

第 9 章主要讨论了密码系统中密钥管理问题。密钥是整个密码系统的核心，密钥管理系统是整个密码系统的安全基础之所在。密钥管理系统不仅与技术方面的因素有关，人及管理制度等非技术因素也在密钥管理系统中占有重要的地位。在第 9 章中，作者将主要从技术方面的因素，包括密钥管理组织结构、密钥生成、密钥分配、密钥协商等，讨论密钥管理的有关问题。

最后，需要强调说明的是，作为一本密码学的基础入门性书籍，本书略过了许多对于初学者而言可能略显困难的知识，例如：密码学的信息论基础、M 序列与 m 序列的分析等；另外，除了分析密码体制安全性时可能会涉及到部分密码分析知识外，作者也有意略去密码分析不提。这是因为这部分知识需要的数学知识可能会过于深奥。最后，本书有意只选择了部分常用的、流行的密码体制进行讲述，对于一些虽然也经常提起、但在实践中并不经常使用的密码体制略去不讲，感兴趣的读者可以查阅其他相关书籍获得进一步知识。

在本书编写过程中，我们得到了很多朋友的支持，袁阳、刘宝宏、邓鸿、刘斌、贾永东、黄治国、周照鹏、罗豪、周进光等对本书的材料搜集与整理做了很多工作。技术的研究和发展是无止境的，虽然作者已竭尽全力，但书中仍难免有错误或疏漏的地方，欢迎读者朋友提出来，与我们探讨。我们的 E-mail 地址是：ybbi@sina.com

编者

2002 年 6 月

目　　录

第 1 章　绪论

密码的历史极为久远，其起源可以追溯到远古时代，人类有记载的通信密码始于公元前400 年。

虽然密码是一门古老的技术，但自密码诞生直至第二次世界大战结束，对于公众而言，密码始终处于一种未知的黑暗当中，常常与军事、机要、间谍等工作联系在一起，让人在感到神秘之余，又有几分畏惧。

信息技术的发展迅速改变了这一切。随着计算机和通信技术的迅猛发展，大量的敏感信息常常通过公共通信设施或计算机网络进行交换，特别是 Internet 的广泛应用、电子商务和电子政务的迅速发展，越来越多的个人信息需要严格保密，如：银行账号、个人隐私等。正是这种对信息的秘密性与真实性的需求，密码学才逐渐揭去了神秘的面纱，走进公众的日常生活当中。

本章主要介绍密码学的基本概念、密码体制的分类、密码学的发展历史。

1.1　密码学的基本概念

密码学主要是研究通信安全保密的学科（虽然密码学也广泛应用于存储加密等领域，但一般认为密码学主要应用服务于通信过程），它包括两个分支：密码编码学和密码分析学。密码编码学主要研究对信息进行变换，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，而密码分析学则与密码编码学相反，它主要研究如何分析和破译密码。这两者之间既相互对立又相互促进。

密码的基本思想是对机密信息进行伪装。一个密码系统完成如下伪装：某用户（加密者）对需要进行伪装的机密信息（明文）进行变换（加密变换），得到另外一种看起来似乎与原有信息不相关的表示（密文），如果合法的用户（接收者）获得了伪装后的信息，那么他可以从这些信息中还原得到原来的机密信息（解密变换），而如果不合法的用户试图从这种伪装后信息中分析得到原有的机密信息（密码分析者），那么，要么这种分析过程根本是不可能的，要么代价过于巨大，以至于无法进行。

准确地说，一个密码系统由明文空间、密文空间、密码方案和密钥空间组成。

（1）加密的信息称为明文。明文的全体称为明文空间。一般情况下，明文用 M（或 m，即消息，Message）或 P（或 p，即明文，PlainText）表示。明文是信源编码符号，可能是文本文件、位图、数字化存储的语音流或数字化的视频图像的比特流。我们可以简单地认为明文是有意义的字符流或比特流。

（2）密文是经过伪装后的明文，全体可能出现的密文的集合称为密文空间。一般情况下，密文用C（或c，即Cipher，密码）表示，它也可以被认为是字符流或比特串。

（3）密码方案确切地描述了加密变换与解密变换的具体规则。这种描述一般包括对明文进行加密时所使用的一组规则（称为加密算法，其对明文实施的变换过程称为加密变换，简称为加密）的描述，以及对密文进行还原时所使用的一组规则（称为解密算法，其对密文实施的变换过程称为解密变换，简称为解密）的描述。

（4）加密和解密算法的操作通常在称为密钥的元素（分别称为加密密钥与解密密钥）控制下进行。密钥的全体称为密钥空间。一般情况下，密钥用K（或k，即Key，密钥）表示。密码设计中，各密钥符号一般是独立、等概出现的，也就是说，密钥一般是随机序列。

通常将加密变换记为$E(k,\cdot)$，解密变换记为$D(k,\cdot)$或$E^{-1}(k,\cdot)$，式中k表示密钥（有时，加密变换与解密变换还可分别被简记为$E_k(\cdot)$与$D_k(\cdot)$）。加密变换与解密可以统称为密码变换。密码变换一般是复杂的非线性变换（而非线性变换），这是因为，如果密码变换是线性变换的话，那么，我们可以很容易地通过已知明文攻击解方程确定密码变换。

从数学的角度来讲，一个密码系统是一族映射，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。这族映射由密码方案确定，具体使用哪一个映射由密钥决定。

可以将密码方案与密钥共同看作控制密码变换的“密钥”，只不过密码方案是固定的“密钥”，而密钥是变换的“密钥”。将“密钥”中固定的部分（密码方案）与变化的部分（密钥）区分开来对于密码分析以及密钥管理等具有重大的意义。

另外，在密码系统所处的环境中除了接收者外，还有非授权者（或称攻击者），它们通过各种方法来窃听（例如，非授权者可采用电磁侦听、声音窃听、搭线窃听等方法直接得到未加密的明文或加密后的密文；这种对密码系统的攻击手段称为被动攻击）和干扰信息（例如非授者采用删除、更改、增添、重放、伪造等手段主动地向系统注入假消息；这种对密码系统的攻击手段称为主动攻击）。

对一个密码系统的被动攻击将损害明文信息的机密性，即需要保密的明文信息遭到泄露；而对一个密码系统的主动攻击将损害明文信息的完整性，即通信时的接收方所接收到的信息与发送方所发送的信息不一致。保证信息机密性的方法是使用密码算法进行加密，而保证信息完整性的方法是使用鉴别与认证机制，数字签名与散列函数（鉴别码）即属于鉴别与认证机制。

如果非授权者借助窃听到的密文以及其他一些信息通过各种方法推断原来的明文甚至密钥，这一过程称为密码分析或密码攻击。从事这一工作的人称作是密码分析员或密码分析者。

这样，一个保密系统可以完整地表示为如图1-1所示的模型。

如果密码分析者可以由密文推出明文或密钥，或者由明文和密文可以寻求密钥，那么就称该密码系统是可破译的。相反地，则称该密码系统不可破译。

当称一个密码系统是不可破译的，具有两种不同的含义：

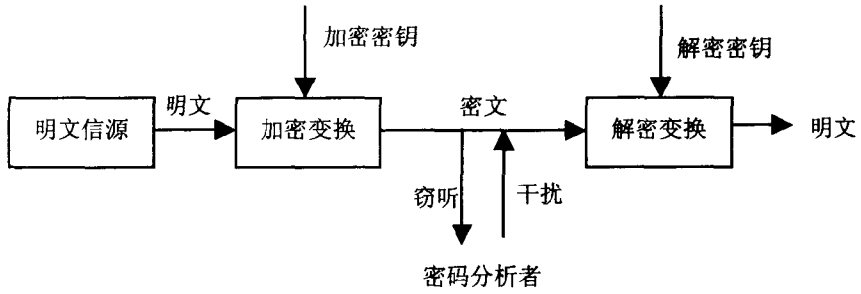

图 1-1 密码系统示意图

对于一个密码系统来说，若攻击者无论得到多少密文也求不出确定明文的足够信息，这种密码系统就是理论上不可破译的，称该密码系统具有无条件安全性（或完善保密性）。

构建无条件安全的密码体制是可能的。如下的密码体制（常被称为“一次一密”密码）已经被证明是无条件安全的：

不失一般性，假设明文、密文与密钥都是二元数字序列，即

$$\text{明文}\ m=(m_1,m_2\cdots,m_L)$$

$$\text{密钥}\ k=(k_1,k_2\cdots,k_R$$

$$\text{密文}\ c=(c_1,c_2\cdots,c_S)$$

其中，m_i（$1\le l\le L$）、k_i（$1\le i\le R$）与 c_j（$1\le j\le S$）均为 0、1 数字。

令 $L=R=S$，并假定明文空间与密钥空间统计独立，且密钥 k 为一随机数字序列。

定义加密变换为：

$$c=E_k(m)=m\oplus k$$

其中 $m\oplus k$ 表示明文 m 与密钥 k 按位模 2 加（按位异或），此时，$c_l=m_l\oplus k_l$，$1\le l\le L$。

解密变换为：

$$m=D_k(c)=c\oplus k$$

其中，$c\oplus k$ 表示密文 c 与密钥 k 按位模 2 加（按位异或），此时，$m_l=c_l\oplus k_l$，$1\le l\le L$。

因此，解密变换确实可以还原加密过的密文。

可以证明，如上的密码体制是无条件安全的（由于证明中使用了信息论的有关知识，我们在此不再给出详细的证明过程）。

若一个密码系统原则上虽可破译，但为了由密文得到明文或密钥却需付出十分巨大的计算，而不能在希望的时间内或实际可能的经济条件下求出准确的答案，这种密码系统就是实际不可破译的，或称该密码系统具有计算安全性（或实际保密性）。衡量不可破译性的尺度叫保密强度。对于任何一个密码系统，如果达不到理论上不可破译，就必须达到实际不可破译。

实际不可破译的密码系统的保密强度必须与这个密码系统的应用目的、保密时效要求和当前的破译水平相适应。有时对保密性可能只要求持续一小段时间，例如，发起进攻的战斗命令只需要在战斗打响前严格保密；或者要求攻击者无法使用低于明文本身价值的代价破译。

一个密码系统的实际安全性牵涉到两方面的因素：

（1）所使用的密码算法的保密强度。

密码算法的保密强度取决于密码设计的水平、破译技术的水平以及攻击者对于加密系统知识的多少。密码系统所使用的密码算法的保密强度提供了该系统安全性的技术保证。

（2）密码算法以外不安全的因素。

即使密码算法能够达到实际不可破译，攻击者也可能不通过对密码进行破译的途径，而是通过其他的各种非技术手段（例如用金钱收买密钥管理人员等）攻破一个密码系统。

因此，密码算法的保密强度并不等价于密码系统整体上的安全性。一个密码系统必须同时完善技术与制度要求，才能保证整个系统的安全。

本书仅讨论影响一个密码系统安全性的技术因素，即密码算法本身。对于一个密码算法的保密强度，一般我们采取对密码进行分析，从而获得其是否可破译或破译需要花费多少资源的相关信息的方法来衡量。

在这种对密码算法的分析当中，一般我们假设密码攻击者了解密码方案的全部知识，可以得到相当数量的密文，知道明文的统计特性和密钥的统计特性，但不知道每一密文 c 所用的特定的密钥 k，这时整个密码系统的安全性全部寄托于密钥的保密之上（这一假设称为 Korchoffs 假设，即“一切秘密寓于密钥之中”）。虽然如果密码分析者或敌手不知道所使用的密码系统，那么破译密码将更难，但我们不应该把密码系统的安全性建立在敌手不知道所使用的密码系统这个前提之下。换句话说，密钥（而不是密码系统的其他组成）是整个密码体制的核心所在。

设计一个密码算法的目的是其保密强度可以在 Kerckhoff 假设下达到安全性要求。在此假设下，常用的密码攻击可以分为以下几类：

（1）惟密文攻击：分析者有一个或一些密文（理论上不可破译的密码与实际不可破译的密码都是针对惟密文攻击而讲的）。

（2）已知明文攻击：分析者有一些明文及对应的密文。

（3）选择明文攻击：分析者可以选择一些对攻击有利的特定明文，并产生对应的密文。

（4）选择密文攻击：分析者可以选择一些攻击有利的特定密文，并得到对应的明文。

上述每种攻击的目的是决定所使用的密钥。这四种攻击类型的强度按序递增，惟密文攻击是最弱的一种攻击，选择密文攻击是最强的一种攻击。如果一个密码系统能够抵抗选择密文攻击，那么它当然能够抵抗其余三种攻击。

“一次一密”密码体制在惟密文攻击下是安全的（无条件安全的密码系统在惟密文攻击下具有绝对的安全性），但是，“一次一密”不能抵抗已知明文攻击，这是因为密钥 k 可由明文 m 和密文 c 进行模 2 加获得。

由于“一次一密”密码无法抵抗已知明文攻击，这就要求每发送一条消息都要产生一个新的密钥，密钥必须通过一个安全的信道传送到消息的接收端，这给密钥管理带来了很大的难度。因此，“一次一密”密码很不实用，且具有很大的局限性。但是，由于这种密码体制能够提供很高的安全性（如果密钥管理的安全性能够得到保证的话），在某些军事或外交场合似乎仍然在使用它。

从上面的讨论中，我们还可以得到如下的对密码系统的基本要求：

（1）密码系统的密钥空间必须足够地大；这是因为，如果密钥空间小的话，攻击者可以采用已知明文甚至惟密文攻击（这时需要判断解密文得到的结果是否有意义，例如是否满足一定的数据结构要求或是否具有语义上的意义）穷举整个密钥空间从而攻破密码系统（这也正是为什么许多密码体制无法继续保持其安全性的因素之一）。

（2）加密与解密过程必须是计算上可行的，必须能够被方便地实现与使用。

（3）整个密码系统的安全性系于密钥上，即使密码方案被公布，在密钥不泄露的情况下，密码系统的安全性也可以得到保证。

另外，对密码系统还存在一些其他的要求，例如：能够抵抗已出现的一些攻击方法；加密后得到的密文长度与明文长度的比值（可称为消息扩展因子）最好是 1（即最好是密文与明文等长，这样不带来额外的传输）等。

1.2 密码体制的分类

密码体制的分类方法有很多，常用的几种分类方法有：

（1）根据加密算法与解密算法所使用的密钥是否相同，或是否能简单地由加（解）密密钥求得解（加）密密钥，可以将密码体制分成对称密钥密码体制（也叫单钥密码体制、秘密密钥密码体制、对称密码体制）和非对称密钥密码体制（也叫作双钥密码体制、公开密钥密码体制、非对称密钥密码体制）。

如果一个保密系统的加密密钥和解密密钥相同，或者虽然不相同、但由其中的任意一个可以很容易地得知另外一个，所采用的就是对称密钥密码体制。本书所介绍的 A5、SEAL、DES、IDEA、RC5、AES 等都是对称密钥密码体制的一些例子。使用对称密钥密码体制时，如果有能力加密（或解密）就意味着必然也有能力解密（或加密）。

如果一个保密系统把加密和解密的分开，加密和解密分别用两个不同的密钥实现，并且由加密密钥推导出解密密钥是计算上不可行的，则该系统所采用的就是非对称密钥密码体制（公开密钥密码体制）。采用非对称密钥密码体制的每个用户都有一对选定的密钥，其中一个是可以公开的，一个由用户自己秘密保存。本书中所介绍的 RSA、ElGamal、椭圆曲线密码等都是非对称密钥密码体制的典型代表。

对称密钥密码体制基于复杂的非线性变换实现；非对称密钥密码体制一般基于某个数学上难的问题实现。由于后者的安全程度与否与现实的计算能力具有密切的关系，因此，我们

常常认为后者的保密强度似乎比前者更弱，但后者也具有前者所不具备的一些特性，它适应于开放性的使用环境，密钥管理问题相对简单，可以方便、安全地实现数字签名和验证。

（2）根据密码算法对明文信息的加密方式，可分为流密码和分组密码。

流密码逐位地加密明文消息字符（如二元数字），本书中介绍的 A5、SEAL 即为流密码算法；分组密码将明文消息分组（每个分组含有多个字符），逐组地进行加密，本书所介绍的 DES、IDEA、RC5、AES 等即为分组密码算法。

（3）按照是否能进行可逆的加密变换，又可分为单向函数密码体制以及人们通常所指的双向变换密码体制。

单向函数是一类特殊的密码体制，其性质是可以容易地把明文转换成密文，但再把密文转换成原来的明文却是困难的（有时甚至是不可能的）。单向函数只适用于某种特殊的、不需要解密的场合（如密钥管理和信息完整性鉴别技术）以及双向变换密码算法中某些环节（绝大多数情况下，总是要求所使用的密码算法能够进行可逆的双向加解密变换，否则接收者就无法把密文还原成明文）。典型的单向函数包括 MD4、MD5、SHA-1 等。

另外，关于密码体制的分类，还有一些其他的方法，例如按照在加密过程中是否注入了客观随机因素可以分为确定型密码体制和概率密码体制等，在此我们不再进行详细介绍。

我们最经常使用的基本分类方法是第一种分类方法。同时，我们还将对称密钥密码体制再区分为流密码与分组密码（由于大多数现有的公开密钥密码体制都属于分组密码，所以非对称密钥密码体制不再区分流密码与分组密码）。最后，一般我们还将单向函数作为单独的一种密码体制列出。本书也正是按照这样的分类方法逐类对密码学进行介绍的。

1.3 密码学的发展历史

密码学的发展大约可分为三个阶段：古代加密方法、古典密码和近代密码。

古希腊墓碑的名文志、隐写术以及黑帮行话都是古代加密方法，这种加密方法已体现了密码学的若干要素，但只能限制在一定范围内使用。

古典密码一般采用手工或机械变换的方式实现，它比古代加密方法更复杂，但其密钥变化量仍然比较小。古典密码时期的密码系统已经初步呈现出当代密码系统的雏形。古典密码的加密方法一般是文字置换，使用手工或机械变换的方式实现。古典密码的代表密码体制主要有：单表代替密码、多表代替密码及转轮密码。Caesar 密码就是一种典型单表加密体制；多表代替密码有 Vigenere 密码、Hill 密码；著名的 Engima 密码是第二次世界大战中使用的转轮密码。

1949 年 Claude Shannon 发表了《保密系统的信息理论》，1976 年 W.Diffie 和 M.Hellman 发表了《密码学的新方向》，这两篇重要的论文和 1977 年美国实施的《数据加密标准（DES）》，标志着密码学的理论与技术的划时代的革命性变革，宣告了近代密码学的开始。近代密码学与计算机技术、电子通信技术紧密相关。在这一阶段，密码理论蓬勃发展，密码算法设计与

分析互相促进，出现了大量的密码算法和各种攻击方法。另外，密码使用的范围也在不断扩张，而且出现了许多通用的加密标准，促进了网络和技术的发展。

目前，由于计算机网络技术的迅速发展，由计算机网络通信而带来的网络安全问题引起了人们的普遍关注，作为网络安全基础理论之一的密码学引起了人们的极大关注，吸引着越来越多的研究人员投入到密码领域的研究当中；同时，由于现实生活当中的实际需要以及计算技术的发展变化，密码学的每一个研究领域都出现了许多新的课题、新的方向。例如：在分组密码领域，由于 DES 已经无法满足高保密性的要求，美国于 1997 年 1 月开始征集新一代数据加密标准（即高级数据加密标准，Advanced Encryption Standard，AES）。目前，AES 的征集已经选择了比利时密码学家所开发的 Rijndael 算法作为标准草案，并正在对 Rijndael 算法作进一步评估。AES 征集活动使国际密码学界又掀起了一次分组密码研究高潮。同时，在公开密钥密码领域，椭圆曲线密码体制由于其安全性高、计算速度快等优点引起了人们的普遍关注，许多公司与科研机构都投入了对椭圆曲线密码的研究当中。目前，椭圆曲线密码已经被列入一些标准作为推荐算法。另外，由于嵌入式系统的发展、智能卡的应用，这些设备上所使用的密码算法由于系统资源本身的限制，要求密码算法可以以较小的资源快速实现，这样，公开密钥密码的快速实现成为了一个新的研究热点。最后，随着其他技术的发展，一些具有潜在密码应用价值的技术也逐渐得到了密码学家的重视，出现了一些新的密码技术，例如，混沌密码、量子密码等，这些新的密码技术获得了极大的重视，并在逐步地走向实用化。

现代密码学的研究内容十分广泛，对现代密码学的最新进展进行描述已经大大超出了本书作者的能力，感兴趣的读者可以参考一些相关资料获得一些信息。

第2章　数学基础

密码学是一门交叉学科，特别地，它在很大程度上是一门应用数学学科。密码学中涉及到数论、代数、计算复杂性理论、组合数学等多种数学知识。

本章将介绍密码学中一些基础的数学知识，包括数论基础、代数基础、计算复杂性理论基础等内容。需要特意加以说明的是，密码学所涉及的数学知识十分地广阔，这里所介绍的只是密码学中所涉及到的部分数学基础，同时，本书还将一些与特定的密码体制密切相关的数学知识留在讨论这些密码体制时再进行详细介绍。

2.1　数论基础

数论是研究整数性质的一个数学分支，它同时也是密码学的基础学科之一。在本节中，我们将介绍一些在本书中使用到的有关数论基础知识，其中一些密码算法密切联系的数论知识将放在相关的章节中详述。

全体整数所组成的集合通常用 Z 表示，即

$$Z=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}。$$

2.1.1　整除

定义 2.1.1　设 $a,b\in Z$，$a\neq 0$。如果存在 $q\in Z$ 使得 $b=aq$，那么就说 b 可以被 a 整除，记作 $a\mid b$，且称 b 是 a 的**倍数**，a 是 b 的**因数**（或称**约数、除数、因子**）。b 不能被 a 整除可以记作 $a\nmid b$。

由定义及乘法运算的性质，立即可推出整除关系具有下面的性质（注意：符号 $a\mid b$ 本身包含了条件 $a\neq 0$）。

（1）$a\mid a$；

（2）如果 $a\mid b$ 且 $b\mid c$，则 $a\mid c$；

（3）设 $m\neq 0$，那么 $a\mid b$ 与 $am\mid bm$ 等价；

（4）如果 $a\mid b$ 且 $a\mid c$，则对所有的 $x,y\in Z$，有 $a\mid bx+cy$；

（5）设 $b\neq 0$，如果 $a\mid b$，那么 $|a|\leq|b|$。

另外，由定义我们可以知道，一个整数 $a\neq 0$，它的所有倍数是

$$qa,\quad q=0,\pm 1,\pm 2$$

这个集合是完全确定的。零是所有非零整数的倍数。但对于一个整数 $b\neq 0$，关于它的因