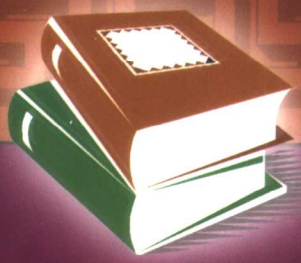
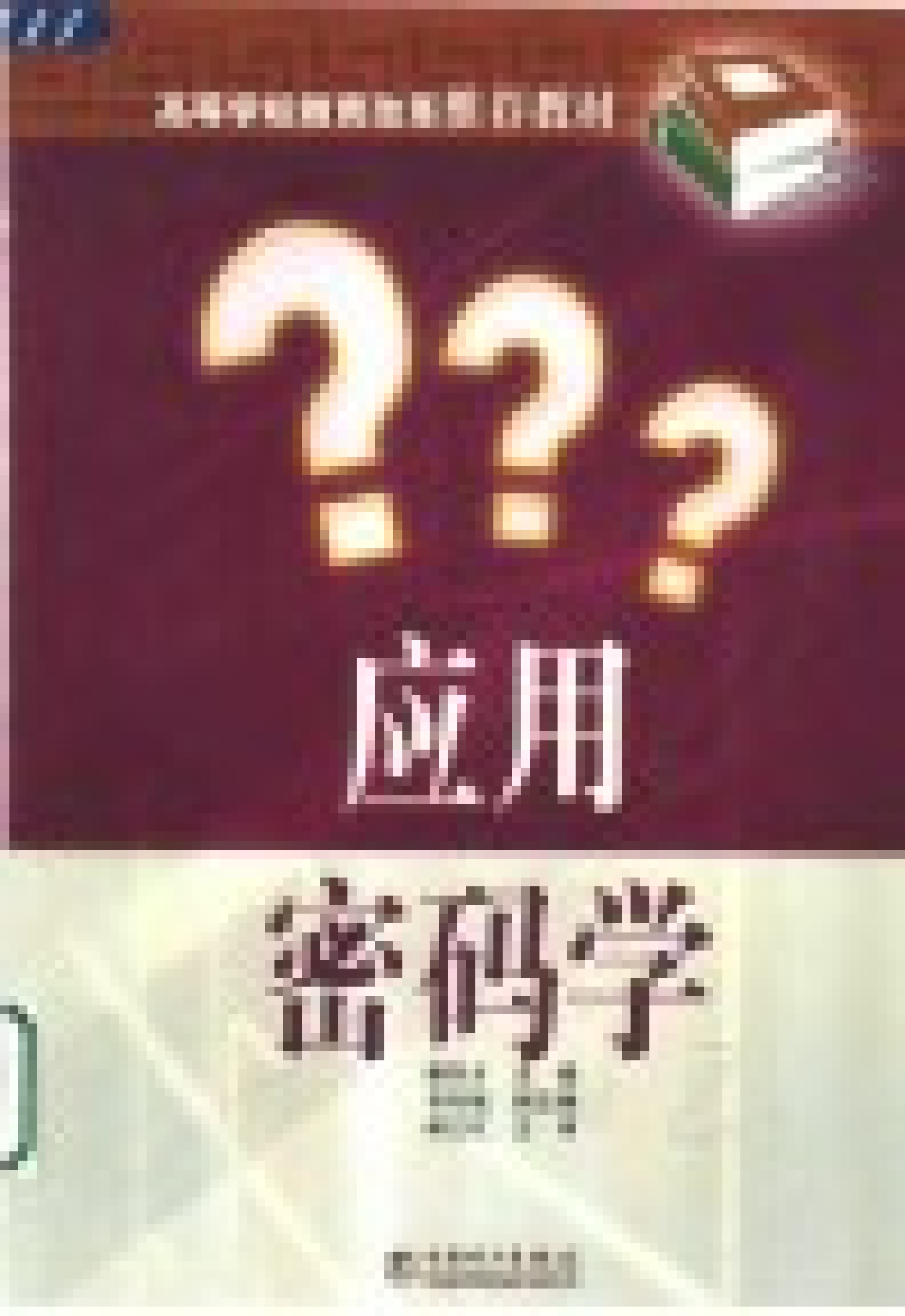
高等学校教育改革推荐教材



# 应用密码学

蔡乐才　主　编
张仕斌　副主编
郝文化　主　审

中国电力出版社
www.infopower.com.cn


???
应用
遥测学

高等学校教育改革推荐教材

# 应用密码学

蔡乐才　主　编
张仕斌　副主编
郝文化　主　审

中国电力出版社
www.infopower.com.cn

## 内容提要

本书是按照高等本科院校的培养目标和基本要求，并结合作者多年来教学经验和工程实践的基础，为实施教学改革，使密码学技术面向应用实践，而编写的一本应用密码学技术基础教材。本书在详细介绍密码学的基本概念及分类的基础上，介绍了目前应用较多的密码学技术。全书的内容涵盖两个方面：一方面介绍了密码学理论，其中对常见密码算法，如 DES、RSA、IDEA 和 AES 等进行了详细的介绍和分析，以便于密码算法的分析、设计和应用；另一方面，为了突出密码学的实际应用，结合目前信息处理和信息传输中比较典型的密码算法应用，如数字签名、身份识别和电子货币等，进行了实例分析，建立了密码算法应用系统的基本架构，并就应用中可能存在的密码算法性能问题进行了详细的分析和描述，对于密码学的分析研究和应用研发起到了很好的参考作用。本书在每章后均配有理论巩固题和上机实战题，实现了教与学的统一。

本书语言通俗易懂，内容丰富翔实，突出了以实例为中心的特点，既可作为大学本科院校计算机科学与技术专业、网络工程专业、信息安全及其相关专业的教学用书，也可作为广大密码学爱好者自学应用密码学技术时的参考用书。

## 图书在版编目（CIP）数据

应用密码学 / 蔡乐才主编. —北京：中国电力出版社，2005

高等学校教育改革推荐教材

ISBN 7-5083-2959-7

I.应... II.蔡... 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（2004）第 127870 号

**责任编辑**：逄积仁

**丛 书 名**：高等学校教育改革推荐教材

**书　　名**：应用密码学

**出版发行**：中国电力出版社

地　　址：北京市三里河路 6 号　　邮政编码：100044

电　　话：（010）68358031（总机）　　传　　真：（010）68316497，88383619

本书如有印装质量问题，我社负责退换

服务电话：（010）88515918（总机）　　传　　真：（010）88518169

E-mail：infopower@cepp.com.cn

**印　　刷**：汇鑫印务有限公司

**开本尺寸**：185×260　　**印　　张**：13.75　　**字　　数**：305 千字

**书　　号**：ISBN 7-5083-2959-7

**版　　次**：2005 年 2 月北京第 1 版

**印　　次**：2005 年 2 月第 1 次印刷

**印　　数**：0001—5000 册

**定　　价**：21.00 元

# 序

党的十六大以来，举国上下都在贯彻人才强国战略。特别是在我国加入 WTO、面临经济转轨的形势下，我国高等教育事业紧扣世界教育发展的脉搏，已从精英教育走向大众教育，进入迅猛发展的时期。

21 世纪是信息技术高度发展的信息时代，要求大学生具有更加丰富的信息技术知识和更强的应用信息技术的能力。选好一本教材，对提高计算机类专业的教学质量至关重要。在确定课程体系以后，最重要的工作就是根据教学要求编写出高质量的教材。在教材建设中，我们提倡百花齐放、推陈出新，经过实践考验，形成公众认可的精品，从而以推动教学质量的提高。

受出版社委托，我们邀请了一些相关高校的教师，召开了一次别具风格的“新形势下高等院校系列教材建设研讨会”，共同研究了国内外高等教育的教学现状与发展趋势，介绍了当前国内高等院校计算机类专业的教学状况与教材建设情况，探讨了新形势下高等院校的教材建设问题，强调了教材要“体现实用性，突出院校自身教学特点，老师易教，学生易学”的编写原则。

在有关专家、教授的亲切指导和热心支持下，在相关高校计算机学院（系）院长（主任）与骨干教师的热情参与下，教材编委会和众多作者在总结了教材建设上多年探索和实践的基础上，广泛汲取了各类成功教材的有益经验，分析了广大学生的承受能力和学习心得，并听取了计算机界教育专家们建议，博采各家所长，精心打造本套教材。本套教材以培养学生的应用能力为目的，突出实用性，突破了传统教材中理论与实践脱节、偏深、偏难的现象，易于实施教学，发掘学生的潜在学习积极性，能让学生在最短的时间内，全面系统地掌握计算机技能。

本套教材作为“新形势下高等院校系列教材”，突出体现了以下特色：

（1）各高校领导十分重视，热心于本套教材的建设，并鼓励教师积极参与，热切希望本套教材真实地反映各高校教学水平、教学特点和最新教研成果；

（2）教材的整个编写过程，自始至终得到有关专家和教授热心、真诚的指导与关怀；

（3）根据各高校与老师的实际需要，与出版社共同规划，共同建设、共同完善教材体系与内容，体现开放与互动交流的宗旨。

这套教材在写法上体现了理论与实践相结合，相关的知识点讲解清晰、透彻，注重教学实际，力求科学实用，符合教学习惯，语言通俗易懂，内容丰富翔实，既注重基本理论及使用方法的深入剖析，又注重实例与技巧的融会贯通。各章后附有课后理论与上机练习，满足学生需要，亦为教师的课堂教学及上机指导提供了有益的参考与帮助。

这套教材是“新形势下高等院校系列教材”，是一种新的尝试。“新”，就会有许多值得修改的地方。本套教材面向各高校，对有志于参与本套教材编写或修改的教师来说是开放的，各学校可以根据自己的特点和教师的特长加以修订和补充。我们热烈欢迎更广泛的学校、教师或作者共同热心参与，更好地规划和完善这套“新形势下高等院校系列教材”。

全国高等学校计算机教育研究会理事长　袁开榜

# 前　言

信息在社会中的地位和作用越来越重要，信息已成为社会发展的重要战略资源，社会的信息化已经成为当今世界发展的潮流和核心。同时，信息的安全问题也成为人们关注的焦点。信息的安全问题是与密码学紧密联系在一起的，从二战以后公开的密码学研究爆炸性地增长，特别是密码学的计算机应用已经深入到越来越多的行业领域，并发挥着越来越重要的作用。在此背景下，应用密码学逐渐成为高等院校各专业的一门重要专业基础课程或选修课程，针对高等院校计算机科学与技术专业、网络工程专业、信息安全及其相关专业学生，我们经过认真收集和整理素材，精心编写了这本与最新密码学理论研究成果和应用同步的《应用密码学》一书。

本书以注重密码学基础知识，注重实际操作，注重密码学应用为中心，主要讲授密码学的基本概念及分类，介绍目前应用较多的密码学技术及应用。主要目的是让计算机科学与技术专业、网络工程专业、信息安全及其相关专业的学生，掌握和了解密码学的概念、基本原理及应用技术，能够利用密码学作为本学科的学习与研究工具，适应信息化社会的发展，更好地在信息化社会生活、工作和学习。

## 主要内容

本书共分为 10 章。第 1 章主要介绍了密码学的发展；第 2 章主要介绍了古典密码学中的单表体制和多表体制的密码系统，包括古典密码体制中的基本加密运算、典型的古典密码体制，以及对古典密码体制的破译方法；第 3 章主要介绍了密码学的相关数学知识；第 4～6 章主要介绍了现代密码学中的分组密码、公钥密码、流密码等典型密码体制；第 7～10 章主要介绍了密码学的应用，包括密钥管理、数字签名、身份识别和电子货币等。在每章的开头都列出了本章所要求掌握的知识点，为了方便读者在学完本章后，检验学习成果和加深对本章内容的理解和掌握，本书在每章的最后都给出了相应的实践检验题。

## 特点

本书用模块化方式深入浅出地讲解了密码学的基础知识，以及密码学应用的重点与难点。全书重点突出、主次分明、结构清晰、逻辑性强，每章都有知识点、概述、实践检验等配套内容。使读者能够在充分掌握密码学基础知识的同时，掌握密码学应用技术，将其尽快运用到实际工作中，从而实现教与学的结合、统一。

## 适应对象

本书语言通俗易懂，内容丰富翔实，突出了以实例为中心的特点，既可作为大学本科院校计算机科学与技术专业、网络工程专业、信息安全及其相关专业的教学用书，也可作

为广大密码学爱好者自学应用密码学技术时的参考用书。

## 编写分工

本书由蔡乐才负责统稿和审校工作。由蔡乐才、张仕斌、陈超、赵攀担任全书的编写工作，黎仁国、曹海、张弘参与了本书的校阅工作。郝文化负责全书的审订工作。其中，由蔡乐才参与编写第 1、4、5、6、8 章，张仕斌参与编写第 2、9 章，陈超参与编写第 2、4、8、9、10 章，赵攀参与编写第 3、5、6、7 章。同时，参与本书编排的还有邹素琼、王安贵、陈郭宜、程小英、谭小丽、卢丽娟、刘育志、吴淬砺、赵明星、贺洪俊、李小平、史利、张燕秋、周林英、黄茂英、李力、李小琼、李修华、田茂敏、苏萍、巫文斌、邹勤、粟德容等，在此表示衷心感谢。

## 配套服务

为充分展现本书编写特点，帮助读者深刻理解本书编写意图与内涵，进一步提高对本书教学的使用效率，我们建立了本书使用指导联络方式，它是读者与编者之间交流沟通的桥梁。欢迎读者将图书使用过程中的问题与各种探讨、建议反馈给我们，本书作者将竭诚为你服务，联系方式 E-mail：bojia@bojia.net。

同时，为了便于多媒体教学，我们为读者提供了本书配套的电子教案，为老师教学提供有益的参考和帮助。请登录网址：http://www.bojia.net，在网站下载专区免费下载。

作　者

2005 年 1 月

# 目　录

# 第1章　密码学概述

**知识点：**

- 密码系统模型
- 密码学的基本概念
- 密码体制的分类
- 凯撒密表
- 密码学的发展及应用

**本章概述：**

本章将从密码学的基本概念着手，阐述密码学中最基本的概念。并在此基础上，介绍密码系统模型，分析密码系统的基本组成、影响因素及基本原理。最后，通过对凯撒密表的具体分析，进一步明确密码、密码体制的概念及构成要素和基本结构框架，为后续章节的学习奠定基础。

## 1.1　密码学的基本概念

密码的历史极为久远，其起源可以追溯到几千年以前，人类有记载的通信密码始于公元前400年。有人说，第一次世界大战是化学家的战争，第二次世界大战是物理学家的战争，如果未来发生战争将是数学家的战争，其核心是信息战中的军事密码学问题。虽然密码学是数学的一个分支，但密码学的应用将会对人类的方方面面产生巨大的影响。

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，它始终让人在感到神秘之余，又有几分畏惧。因为它常常与军事、机要、间谍等工作联系在一起。

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。

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他人窃取、解密和利用的方法，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。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的信息中分析得到原有的机密信息，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。

1. 密码系统的组成

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）明文空间。待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，Plain Text）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，可以简单地认为明文是有意义的字符流或比特流。

（2）密文空间。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，即密码，Cipher）表示，它也可以被认为是字符流或比特串。

（3）密码方案。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）密钥空间。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，即密钥，Key）表示。密码设计中，各密钥符号一般是独立、等概率出现的，也就是说，密钥一般是随机序列。

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），他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（例如非授权者采用删除、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）。

2. 密码系统模型

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。从事这一工作的人被称作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。

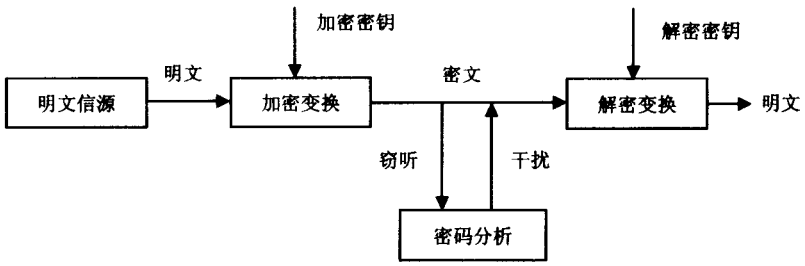



图 1-1　密码系统模型

3. 不可破译密码系统

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时候，具有两种不同的含义：

（1）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，如下面的密码体制（常被称为“一次一密”密码）已经被证明是无条件安全的。

假设明文、密文与密钥都是二元数字序列，即

$$\text{明文 } m=(m_1,\ m_2,\ \cdots,\ m_L)$$

$$\text{密钥 } k=(k_1,\ k_2,\ \cdots,\ k_R)$$

$$\text{密文 } c=(c_1,\ c_2,\ \cdots,\ c_S)$$

式中：$m_l$ $(1\leqslant l\leqslant L)$、$k_i(1\leqslant i\leqslant R)$与 $c_j(1\leqslant j\leqslant S)$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

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

式中：$m\oplus k$ 表示明文 $m$ 与密钥 $k$ 按位模 2 加（按位异或），此时，$c_l=m_l=k_l$，$1\leqslant l\leqslant L$。解密变换为

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

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

因此，解密变换确实可以还原加密过的明文。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，因此不再给出详细的证明过程）。

（2）若一个密码系统理论上虽可破译，但是由密文得到明文或密钥却需要付出十分巨大的代价，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安全性（或实际保密性）。衡量不可破译性的尺度被称为保密强度。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。有时对保密性的要求只持续一小段时间，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花费低于明文本身价值的代价破译。

4. 密码系统的安全性

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的了解程度。密码系统所使用的密码算法的保密强度是该密码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（$k$）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，一般采取对密码进行分析的方法来确定，即分析密码是否可破译或破译需要花费多少资源等相关信息，进而衡量密码算法的保密强度。

在这种对密码算法的分析当中，一般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依靠密钥的保密性（这一假设称为 Korchoffs 假设，即“一切秘密寓于密钥之中”）。虽然密码分析者或攻击者在不知道所使用的密码系统时，破译密码将更加困难，但不应该把密码系统的安全性建立在攻击者不知道加密者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。

5. 常用密码系统的攻击

设计一个密码算法的目的是其保密强度可以在 Korchoffs 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）唯密文攻击：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唯密文攻击而言的）。

（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对攻击有利的特定密文，并得到对应的明文。

上述攻击的目的是决定所使用的密钥。这 4 种攻击类型的强度按序递增，唯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，那么它就能够抵抗其余 3 种攻击。

“一次一密”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仍然在使用它。

6. 密码系统的基本要求

从上面的讨论中，还可以得到如下对密码系统的基本要求：

（1）密码系统的密钥空间必须足够大。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唯密文攻击（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如下。

1. 对称密钥密码体制和非对称密钥密码体制

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**（也称作单钥密码体制、秘密密钥密码体制、对称密码体制）和**非对称密钥密码体制**（也叫做双钥密码体制、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，那么该系统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。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，并且由加密密钥不能推导出解密密钥，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。

对称密钥密码体制是基于复杂的非线性变换实现的，非对称密钥密码体制一般是基于

数学上某个难以实现的方法来进行加密的。由于后者的安全程度大小与现实的计算能力具有密切的关系，因此，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，比如它适用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，等等。

2. 流密码和分组密码

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。

流密码是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；分组密码是将明文消息分组（每个分组含有多个字符），然后对每一组进行加密，本书所介绍的 DES、IDEA、RC5、AES 等即为分组密码算法。

3. 单向函数密码体制和双向变换密码体制

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和双向变换密码体制。

单向函数密码体制是一类特殊的密码体制，其性质是可以很容易地把明文转换成密文，但再把密文转换成正确的明文却是困难的（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的某些环节（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考虑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，在此将不再进行详细介绍。

人们经常使用的基本分类方法是第一种分类方法。同时，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，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对密码学进行介绍的，并在此基础上分别介绍了密码学在数字签名、电子货币等方面的应用。

## 1.3 密码学的发展历史

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以前。密码学的发展大约可分为 3 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、隐写术及古代的行帮暗语和一些文字猜谜游戏等都是古代加密方法。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流通，已体现出了密码学的若干要素，但只能限制在一定范围内使用。

古罗马随笔作家修托尼厄斯在他的作品中披露，凯撒常用一种“密表”给他的朋友写信. 这里所说的密表，在密码学上称为“凯撒密表”。用现代的眼光来看，凯撒密表是一种相当简单的加密变换，它是把明文中的每一个字母用它在字母表中位置后面的第 3 个字母代替。古罗马文字就是现在所称的拉丁文，其字母就是我们从英语中熟知的那 26 个拉丁字母。因此，凯撒密表就是用 D 代 a，用 E 代 b，…，用 z 代 w，注意：用 A 代 x，用 B 代 y，C 代 z。这些代替规则也可用一张表格来表示，所以叫“密表”，如表 1-1 所示。

表 1-1　凯撒密表

| 明文 | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 密文 | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

例如，有这样一个拉丁文句子：

Omnia Gallia est divisa in Partes tres.（高卢全境分为 3 部分。）

用凯撒密表加密后，就成为密文：

RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV

如果不掌握其中奥妙，不知道凯撒密表，就不知所云。

那么，在公元前 54 年，凯撒就是用这种密码给西塞罗写信的吗？有趣的是，密码界对这一点却持否定态度，因为密码学历史上还记载着凯撒使用的另一种加密方法：把明文的拉丁字母逐个代之以相应的希腊字母，这种方法看来更贴近凯撒在《高卢战记》中的记叙。显然，哪一个拉丁字母应该代之以哪一个希腊字母，事先都有约定，凯撒知道，西塞罗也知道，不然的话，西塞罗收到密信后，也会不知所云。

凯撒的这种加密方法也可用一张表格表示。比方说，用希腊字母代替拉丁字母，通常有如表 1-2 所示的代替规则。

表 1-2　另一种可能的凯撒密表

| 明文 | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 密文 | α | β | ε | δ | φ | γ | η | ι | γ | κ | λ | μ | ν | ο | ρ | θ | ξ | σ | τ | π | υ | ω | χ | ψ | ζ | |

对于上述凯撒密表的密码变换分析，“密码”所包含的基本要素如下：

（1）凯撒密表必须有其加密的对象——明文集合，即所有用拉丁语明确表达的语句。

（2）明文经凯撒密表加密后变换成的密义，都是一个由拉丁字母组成的字符串，这说明其密文集合就是由所有这样的字符串组成的。

（3）凯撒密表有密钥 3。但是，这个 3 并不是本质的，它也可以是 4，5 等。因此，这里可以有一个密钥集合，它的元素是 0，1，2，…，25。集合中不同的密钥决定着不同的变换。

（4）密钥集合中各个密钥所决定的加密变换也组成了一个集合，虽然这些加密变换是不相同的，但却有一个共同的算法——后移。

（5）同样，也有一个解密变换集合，相应地也有一个共同的算法——前移。密钥集合中的一个密钥（如 3），作为加密的共同算法“后移”的一个参数，决定了一个具体的加密变换“后移 3”。同样，它也决定了一个具体的解密变换“前移 3”，从而使两个变换互为逆变换。

而一个密码体制，是指由如下 5 个部分组成的一个系统：

- 明文集合$\mu$；
- 密文集合$\pi$；

- 密锁集合 $K$;
- 加密变换集合 $E$ 及其加密算法 $e$;
- 解密变换集合 $D$ 及其解密算法 $d$。

$K$ 中的任一个密钥 $k$，既作为加密算法 $e$ 的参数决定了 $E$ 中的一个加密变换 $e_k$: $\mu \to \pi$，同时又作为解密算法 $d$ 的参数决定了 $D$ 中的一个解密变换 $d_k$: $\pi \to \mu$。并且 $e_k$ 与 $d_k$ 互为逆变换，即对明文集合中的任一个明文语句 $M$，恒有 $d_k(e_k(M)) = M$。

总的来说，所谓的“密码”，是指“密码体制”在不引起混淆的情况下，一个密钥已具体给定的密码体制。

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。Caeser 密码就是一种典型的单表加密体制，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。古典密码主要应用于政治、军事及外交等领域，可以说，自从有了战争，就有了保密通信。交战双方都为了保护自己的通信安全、窃取对方的情报而研究各种信息加密技术和密码分析技术。

在 1949 年之前，密码技术基本上可以说是一门技巧性很强的艺术，而不是一门科学。在这一时期，密码专家常常是凭借直觉和信念来进行密码设计和分析，而不是推理证明。

1949 年，Claude Shannon 发表了“保密系统的信息理论（Communication Theory of Secrecy Systems）”，为密码学奠定了坚实的理论基础，使密码学成为一门真正的科学。但从 1949 年至 1975 年，密码学的理论研究工作进展不大。1976 年 W. Diffie 和 M. Hellman 发表了“密码学的新方向（New Directions in Cryptography）”，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是可能的，从而开创了公钥密码学的新纪元。1977 年，美国国家标准局（National Bureau of Standards）正式公布了数据加密标准 DES（Data Encryption Standard），将 DES 算法公开，从而揭开了密码学的神秘面纱。从此，密码学的研究进入了一个崭新的时代，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，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。因此，密码学理论和技术已成为信息科学和技术中的一个重要研究领域。随着密码理论蓬勃发展，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，随着计算机网络的迅速发展，特别是近年来电子商务的兴起，现代密码学的应用范围也在不断扩张，已不仅仅局限于政治、军事及外交等领域，其商用价值和社会价值也已得到了充分的肯定。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