普 通 高 等 教 育 规 划 教 材

密码学与网络安全技术基础

主　编　汤　惟
副主编　屠立忠
参　编　朱　珣

机 械 工 业 出 版 社

网络安全已经成为网络信息系统开发、建设、应用中必须的支撑技术。本书从信息系统开发、建设、应用的工程实际出发讲述网络安全技术基础，主要内容包括网络安全所需要的现代密码学基本原理和常用加、解密算法，密钥管理、数字签名方法：消息认证协议 Kerberos X.509v3证书；IP安全，E-mail，Web安全等网络系统实用安全技术。最后介绍常用的安全电子交易技术规范 SET和企业安全体系结构 PKI。

本书可作为高等学校计算机、通信等有关专业本科生的教材，也可作为计算机网络、通信工程师的技术参考书和培训教材。

本课程建议学时 40～48学时。

图书在版编目（CIP）数据

密码学与网络安全技术基础/杨义惟主编.—北京：机械工业出版社，2004.1

普通高等教育规划教材

ISBN 7-111-13675-5

Ⅰ.密… Ⅱ.杨… Ⅲ.计算机网络—密码术—高等学校—教材

Ⅳ.TP393.08

中国版本图书馆 CIP数据核字（2003）第 119386号

机械工业出版社（北京市百万庄大街 22号 邮政编码 100037）

策划编辑：王小东 责任编辑：卢若薇 版式设计：冉晓华

责任校对：李秋荣 封面设计：饶 薇 责任印制：路 琳

北京机工印刷厂印刷·新华书店北京发行所发行

2004年 2月第 1版第 1次印刷

787mm×1092mm 1/16·12印张·296千字

定价：17.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

本社购书热线电话（010）68993821，88379646

封面无防伪标均为盗版

普通高等教育应用型人才培养规划教材编审委员会委员名单

主　任：刘国荣　　湖南工程学院
副主任：左健民　　南京工程学院
　　陈力华　　上海工程技术大学
　　鲍　泓　　北京联合大学
　　王文斌　　机械工业出版社
委　员：（按姓氏笔画排序）
　　任淑淳　　上海应用技术学院
　　何一鸣　　常州工学院
　　陈文哲　　福建工程学院
　　陈志强　　华北航天工业学院
　　陈　崚　　扬州大学
　　苏　群　　黑龙江工程学院
　　娄炳林　　湖南工程学院
　　梁景凯　　哈尔滨工业大学（威海）
　　童幸生　　江汉大学

计算机科学与技术专业分委员会委员名单

主　任：黄陈蓉　　南京工程学院
副主任：吴永昶　　上海应用技术学院
委　员：（按姓氏笔画排序）
汤　惟　　江汉大学
沈　涛　　扬州大学
陈文强　　福建工程学院
肖建华　　湖南工程学院
邵祖华　　浙江科技学院
靳　敏　　黑龙江工程学院

序

工程科学技术在推动人类文明的进步中一直起着发动机的作用。随着知识经济时代的到来，科学技术突飞猛进，国际竞争日趋激烈。特别是随着经济全球化发展和我国加入 WTO，世界制造业将逐步向我国转移。有人认为，我国将成为世界的“制造中心”。有鉴于此，工程教育的发展也因此面临着新的机遇和挑战。

迄今为止，我国高等工程教育已为经济战线培养了数百万专门人才，为经济的发展作出了巨大的贡献。但据 IMD1998年的调查，我国“人才市场上是否有充足的合格工程师”指标排名世界第 36位，与我国科技人员总数排名世界第一形成很大的反差。这说明符合企业需要的工程技术人员特别是工程应用型技术人才市场供给不足。在此形势下，国家教育部近年来批准组建了一批以培养工程应用型本科人才为主的高等院校，并于 2001、2002年两次举办了“应用型本科人才培养模式研讨会”，对工程应用型本科教育的办学思想和发展定位作了初步探讨。本系列教材就是在这种形势下组织编写的，以适应经济、社会发展对工程教育的新要求，满足高素质、强能力的工程应用型本科人才培养的需要。

航天工程的先驱、美国加州理工学院的马·卡门教授有句名言：“科学家研究已有的世界，工程师创造未有的世界。”科学在于探索客观世界中存在的客观规律，所以科学强调分析，强调结论的惟一性。工程是人们综合应用科学（包括自然科学、技术科学和社会科学）理论和技术手段去改造客观世界的实践活动，所以它强调综合，强调方案优缺点的比较并做出论证和判断。这就是科学与工程的主要不同之处。这也就要求我们对工程应用型人才的培养和对科学研究型人才的培养应实施不同的培养方案，采用不同的培养模式，采用具有不同特点的教材。然而，我国目前的工程教育没有注意到这一点，而是：①过分侧重工程科学（分析）方面，轻视了工程实际训练方面，重理论，轻实践，没有足够的工程实践训练，工程教育的“学术化”倾向形成了“课题训练”的偏软现象，导致学生动手能力差。②人才培养模式、规格比较单一，课程结构不合理，知识面过窄，导致知识结构单一，所学知识中有一些内容已陈旧，交叉学科、信息学科的内容知之甚少，人文社会科学知识薄弱，学生创新能力不强。③教材单一，注重工程的科学分析，轻视工程实践能力的培养；注重理论知识的传授，轻视学生个性特别是创新精神的培养；注重教材的系统性和完整性，造成课程方面的相互重复、脱节等现象；缺乏工程应用背景，存在内容陈旧的现象。④老师缺乏工程实践经验，自身缺乏“工程训练”。⑤工程教育在实践中与经济、产业的联系不密切。要使我国工程教育适应经济、社会的发展，培养更多优秀的工程技术人才，我们必须努力改革。

组织编写本套系列教材，目的在于改革传统的高等工程教育教材，建设一套富有特色、有利于应用型人才培养的本科教材，满足工程应用型人才培养的要求。

本套系列教材的建设原则是：

1．保证基础，确保后劲

科技的发展，要求工程技术人员必须具备终生学习的能力。为此，从内容安排上，保证学生有较厚实的基础，满足本科教学的基本要求，使学生日后具有较强的发展后劲。

2）突出特色，强化应用

围绕培养目标，以工程应用为背景，通过理论与工程实际相结合，构建工程应用型本科教育系列教材特色。本套系列教材的内容，结构遵循如下 9字方针：知识新、结构新、重应用。教材内容的要求概括为：“精”、“新”、“广”、“用”。“精”指在融会贯通教学内容的基础上，挑选出最基本的内容、方法及典型应用；“新”指在将本学科前沿的新进展和有关的技术进步新成果、新应用等纳入教学内容，以适应科学技术发展的需要。妥善处理好传统内容的继承与现代内容的引进。用现代的思想、观点和方法重新认识基础内容和引入现代科技的新内容，并将这些按新的教学系统重新组织；“广”指在保持本学科基本体系下，处理好与相邻以及交叉学科的关系；“用”指注重理论与实际融会贯通，特别是注入工程意识，包括经济、质量、环境等诸多因素对工程的影响。

3）抓住重点，合理配套

工程应用型本科教育系列教材的重点是专业课（专业基础课、专业课）教材的建设，并做好与理论课教材建设同步的实践教材的建设，力争做好与之配套的电子教材的建设。

4）精选编者，确保质量

遴选一批既具有丰富的工作实践经验，又具有丰富的教学实践经验的教师担任编写任务，以确保教材质量。

我们相信，本套系列教材的出版，对我国工程应用型人才培养质量的提高，必将产生积极作用，会为我国经济建设和社会发展作出一定的贡献。

机械工业出版社颇具魄力和眼光，高瞻远瞩，及时提出并组织编写这套系列教材，他们为编好这套系列教材做了认真细致的工作，并为该套系列教材的出版提供了许多有利的条件，在此深表衷心感谢！

编委会主任
湖南工程学院院长　刘国荣教授

前　言

本书是机械工业出版社组织编写的普通高等教育应用型本科计算机专业规划教材之一。

网络信息安全已经成为网络信息系统建设、维护中必须的支撑技术。本书从信息系统开发、建设、应用的工程实际出发讲述网络安全技术基础。主要内容包括网络安全所需要的现代密码学基本原理和常用加解密算法，密钥管理，数字签名方法；消息认证协议 Kerberos X.509v3证书；IP安全，E-mail Web安全等网络系统实用安全技术。最后介绍常用的安全电子交易技术规范 SET和企业安全体系结构 PKI。

网络信息安全理论与技术涉及安全需求和策略、基本技术、基础设施和安全服务体系诸多问题，不仅内容庞杂，而且发展十分迅速。新理论产生快，应用系统的复杂性极其安全需求日益增长，新的技术应用层出不穷。本书从信息安全的核心技术——密码学基础理论入手，力图深入浅出地介绍网络信息安全相关的基本理论和工程实践需要的实用技术，同时尽可能地反映该领域的最新发展。

本书可作为高等学校应用型本科计算机、通信工程等有关专业教材，也可作为计算机网络、通信工程师的技术参考书和培训教材。

本书第1、2、3、4章由汤惟执笔，第7、8、9章由屠立忠执笔，第5、6章由朱□编写。汤惟负责全书统稿。

华中科技大学计算机科学与技术学院博士生导师、中国教育科研网（CERNET）专家委员会委员、CERNET华中地区网络中心主任李之棠教授作为本书主审，他在百忙中对本书进行了十分仔细的审阅，对全书结构、内容提出了指导性意见和建议。本书编写得到江汉大学和南京工程学院的领导和同志们的大力支持和帮助。在此对所有关心和支持本书出版的领导、导师和同志们表示衷心地感谢。

由于编者水平有限，书中出现的错误和不当之处，敬请读者指正。

编者

2003年10月于武汉

目　录

第 1章　概　　论

计算机安全包括计算机系统的实体安全和系统中存储的数据（信息）的安全。计算机安全的根本目的是保护计算机信息系统的真实性、完整性和机密性。计算机技术与数字通信技术的结合，使网络成为现代信息系统的基本运行环境。基于 TCP/IP的各类网络系统及其互联所实现的共同特征是开放互联、资源共享、分布式处理。计算机信息系统在为各种组织机构和个人所有信息的交换、共享、处理带来极大方便的同时，网络信息安全事故也时有发生。的确，网络信息系统的安全已经成为信息技术研究的重要课题。在网络环境下，为实现数据机密通信、用户身份认证、信任关系建立等，现代密码学理论和方法得到广泛应用，是我们理解、掌握、应用网络安全机制，实现安全服务必需的基本理论。

本章讨论网络信息系统面临的主要威胁，介绍密码学的基本概念。由此给出网络安全的基本概念和网络安全基本模型。

1.1　网络安全面临的威胁及网络应提供的安全服务

1.1.1　网络安全面临的威胁及存在的问题

（1）来自用户的非授权访问　网络安全面临的威胁之一是来自用户的非授权访问。一个组织机构的网络系统，来自用户的威胁是指对网络内部信息的故意或者非故意非授权访问，这里，用户包括网络内部用户和网络外部的访问者。恶意软件主要指计算机病毒、蠕虫等，通常认为它们来自网络外部。因此对网络安全的威胁可以分为内部威胁和外部威胁。以下是用户非授权访问攻击网络的典型例子：

① 用户 A向用户 B传送敏感数据（如支付工资记录）。这些数据被用户 C在浏览内部网时“偶然”获取，或者进行非授权更改。

② 对公司心怀不满或者已被解雇的雇员利用其尚未被注销的权限对网络内部的敏感数据进行复制或者删除、更改。

③ 用户 B假冒网络管理员 A向终端 C发出授权消息，终端 C接受该消息并认为是管理员 A发出，因此实施相应授权操作。

④ 以非法窃取网络内部信息或者破坏网络资源为目的黑客入侵。

（2）病毒恶意软件对网络的入侵　病毒类恶意软件入侵网络系统的渠道和方式通常包括：

① 陷门：陷门是指进入程序的秘密入口，具体实现方式可以是某些特定的输入口令或者用户识别码（ID），或者是一个不可能事件序列激活的程序段。掌握陷门的人可以不经过安全认证和授权访问系统资源，恶意程序可以通过陷门植入系统。

② 逻辑炸弹：逻辑炸弹是最早出现的恶意程序之一，它通常嵌于合法程序中并设定“触发条件”。典型的触发条件包括特定机器日期时间，对特定文件的访问，特定用户的进入等。一旦条件满足，逻辑炸弹便被触发——激活程序变更系统状态，修改系统数据甚至全部

文件，造成终端或者服务器系统或者整个网络瘫痪。

3 特洛伊木马：特洛伊木马来自古希腊传说，借指隐藏在正常程序中的代码段。当程序被调用时，这些隐藏代码将执行一些附加功能，例如间接实现非授权访问，删除用户文件等。

4 病毒：病毒通常是隐藏在正常文件中的代码段或者是隐藏在系统外存特定区域的完整程序。病毒与逻辑炸弹、特洛伊木马有相似的破坏作用，其区别是它具有可传染性：病毒可以通过修改程序实现对自身的复制或者变异复制，在网络环境下通过数据交换实现传播。

5 蠕虫：蠕虫程序指通过网络连接实现自身的传播病毒代码。网络蠕虫利用网络连接传播的方法包括电子邮件、远程登录、远程执行等。其传播过程可以是：搜索远程主机地址表；建立与远程系统的连接；将自身复制到远程系统并激活运行。

（3 在电子商务系统中，通过网络相互联系的用户之间可能存在的问题

1 公司的客户通过网络发出确认一笔交易的消息，随后否认他已发出的消息。或者反过来，公司否认通过网络所收到的消息，或者声称收到消息的时间无效。

2 公司利用客户的一次性授权通过网络多次从客户账户中划款。或者客户利用公司一次性交易授权在网络上实施多笔交易。

3 用户 A和用户 B通过网络相识，由于没有相互的实体联系，因此不能确认彼此身份的真实性，从而无法实施交易。事实上互联网中的确存在各种身份假冒和欺诈行为。

（4 网络安全所受到的攻击 数据通信是实现各种网络服务的主要途径，正常的网络通信如图 1.1.1a所示。以上安全威胁事例归结起来构成对网络安全的如下攻击（见图 1.1.1b～e）。

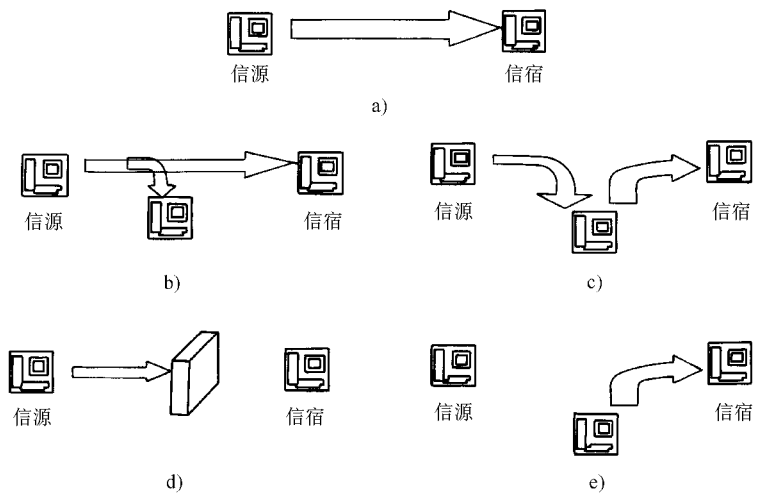

图 1.1.1 网络安全所受到的攻击

1 窃听：如对文件或者程序的非授权复制，在通信信道中进行监听等。窃听构成对系统信息机密性的攻击。

2 篡改：如对文件中的数据实施非授权修改、添加、删除，替换程序实现的功能，对网络中传送消息内容的更改等。篡改是对系统或者用户信息完整性的攻击。

3 阻断：如切断通信信道，破坏文件系统或者存储介质，改变用户 ID使其不可访问等。阻断是对网络资源可用性的攻击。

(4) 拒绝服务：如一个实体可能抑制所有发送给用户 A的消息。另一种可能的拒绝服务则是使得网络系统崩溃，或者通过滥发消息使特定服务器等网络设备过载，不能响应正常服务，或者降低正常服务功能的水平。拒绝服务攻击的也是网络资源的可用性，属于阻断攻击的一种方式。

(5) 假冒：对系统信息真实性的攻击。如假冒合法用户插入系统，编造虚假信息发送给信宿。前面在（3）的 2）中所举事例原则上也是假冒，但由于它是将已获取的合法授权越权使用，通常称为重放。

对安全的攻击又可分为被动攻击和主动攻击。窃听属于被动攻击，攻击者的目标是获取传输中的信息或者监视网络通信。监视网络通信的目的包括测定信源、信宿地址，获取用户 ID，通过分析通信流量、发生频率猜测通信性质等。被动攻击不会导致数据的任何改变，较难检测，抵御此类攻击的重点是预防。

主动攻击涉及传输数据的更改或者虚假信息的产生，这类攻击包括篡改、假冒、重放和拒绝服务。预防主动攻击是十分困难的，但可以检测该类攻击，识别篡改、假冒、重放，对主动攻击破坏的网络资源进行有效恢复。

1.2.2 网络信息系统应提供的安全服务

根据网络可能受到的攻击，一个安全的网络信息系统应该能够提供以下安全服务：

(1) 机密性服务 将系统中的敏感信息进行秘密存储或者传输，保证消息的机密性。根据消息内容的结构，可以将保密服务实施在不同层次上。最广义的保密服务是在特定时间段内保护两个用户之间传输的所有消息不发生泄露。也可以对消息中的不同字段实施不同级别的保护，这种方式实现起来更为复杂，代价较高。消息保密的另一种类型即防止敌手实施对通信流的分析，这要求对通信链路上传输的数据包源、目的地址、长度、发送频率进行保护或者伪装。

(2) 完整性服务 一个面向连接的完整性服务是确保收到的消息与发送的消息完全一致，没有被篡改、插入、重放、重排或者延迟。因此面向连接的完整性服务用于保护消息流免受篡改和拒绝服务。无连接的完整性服务则仅仅指保护消息不被篡改。如同消息保密，完整性服务也可以实施在不同层次上，如整个消息流、单个消息或者消息中的特定字段。

(3) 真实性服务 消息认证用于保证消息的真实性。在消息单向传输中，认证的功能是使消息的接收者相信消息确实来源于该消息所声明的信源。在双向传输中，认证服务涉及通信双方。在连接发起时，认证服务确保通信双方的身份的真实性。在连接建立后认证服务还应该保证该连接不被第三方假冒插入。

(4) 不可抵赖服务 不可抵赖服务用于防止通信双方抵赖（否认）已经发送或者接收的消息。用户 A的消息 M发出给用户 B，用户 B接收到 M后能够证实 M确实是用户 A发出的；同理，用户 A也能够证实 M确实已经被用户 B接收。

(5) 访问控制 在网络环境中，访问控制的目的是限制用户对网络资源非授权访问。每个试图访问网络的实体都必须识别其身份，身份得到鉴别后即可获得为其定制的访问权限。同时还应该对各合法用户的访问权限实施授权、保密、变更、收回等管理。

以上网络安全服务的有效实现需要数学、信息、通信、计算机网络等诸多学科技术领域的综合。它涉及到网络安全体系和协议、密码学理论、信息分析、安全检测、应急处理技术等，其中密码学是网络安全的基础理论和关键技术。

1.2 密码学基本概念

1.2.1 密码通信模型

(1) 密码通信的概念 为防止敌手窃听，发送者将待发送消息进行变换、隐藏后再通过信道发送给接收者，确信窃听者即便获取信道中传输的数据，也不能从中析取原始消息。这里待发送的消息称为明文，对明文进行变换、隐藏其内容的过程称为加密；经过加密的消息称为密文，将密文转换为明文的过程称为解密。图 1.2 给出密码通信的基本过程。

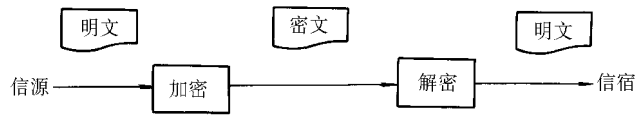

图 1.2 密码通信的基本过程

在计算机通信中，可以认为明文 M是按照某种格式表示文本、图形、语音、视频图像等信息的位序列，也可看作以字节为单位的分组数据块流。经过加密，M转换为一种使得窃听者不可解析的数据编码，即密文 C，它也是二进制数据。这里明文 M与密文 C原则上应该一一对应。因此，加密过程是一个函数 C = E(M)。解密可以看作加密函数 E的反函数 M = D(C) = D(E(M))。

密码算法（有时简称密码）是指用于加密和解密的一对数学函数 E(·)、D(·)。研究如何构造密码算法，使窃听者在合理的时间和代价下不能破译密文，以获取原始明文消息的理论和方法称为密码编码学。与之对应的，研究在未知密码算法前提下，对获取的密文进行分析、破解，从中获取原始明文消息的理论和方法称为密码分析学。

给定密码算法 E、D，在未知 D的前提下，试图构造算法 D′，使得对任何由 E加密的密文 C = E(M)，都有 D′(C) = D(C) = M。这种企图我们称为对密码算法的攻击，如果这种 D′找到了，则称该密码算法被破解了。完整的密码学包括密码编码和密码分析两方面。

密码通信系统中，明文消息所有可能取值集合称为明文消息空间，密文所有可能取值集合称为密文消息空间。一个密码通信系统中，如果已知明文消息空间和密文消息空间（这通常容易办到，因为实际应用中明文消息空间和密文消息空间都是有限集合），则该系统中的任何密码算法原则上都是可以破解的，问题是破解的时间和代价。对给定密码算法的攻击难度通常被称为该密码算法的强度。一个安全的密码通信系统要求敌手在合理的时间和代价内不可能破解其密码，或者说其密码具有足够的强度。

早期密码系统的安全性通常基于其密码算法的机密性，即密码算法是秘而不宣的。这种保密机制存在两个根本性缺陷：

其一，这种密码系统不能适于用户数量不断变化的组织。因为如果其中某个用户离开该组织或者密码算法被泄露，则该系统所有用户必须更换密码算法。

其二，其安全性无从确认，也不能够标准化。因为算法本身是机密的，因此不能被密码学家研究分析。也不能采用流行的硬件或者软件产品实现，因为窃听者可以从市场上购买这些产品进行学习分析。

现代密码学认为密码算法是一组依赖于“密钥”的函数族，该函数族的构造是公开的。一切秘密都在密钥中。

例 1.1 明文消息 M：Network Security is of extreme importance in the information system

选择密钥 k：Jianghan University，由该密钥确定字符替换表

A	B	C	D	E	F	G	H	I	J	K	L	M	N
J	I	A	N	G	H	U	V	E	R	S	I	T	Y
O	P	Q	R	S	T	U	V	W	X	Y	Z	_	
!	B	C	D	F	K	L	M	O	P	Q	X	Z	

得 M对应的密文 C：

YGKO! DSZFGALDEKQZEFZ! HZGPKDGTGZETB! DKJYAGZEYZKVGZEYH! DTJKE! YZFQFKGT

这里替换表的构成是由密钥 k＝“ Jianghan University”中不重复的字符依次对应“ abcdefghi郾 jklmn”，“ o”对应“ !”，密钥 k中未出现字母依次对应“ pqrstuvwxyz”，空格符“ _ ”对应“ Z”。解密既将替换表上、下行颠倒即得。按照这种办法，替换表的构造方法一样。当“密钥”字符串 k取值不同时，替换表取值不同，从而确定一对具体的加、解密算法。

例 1.2.2 逻辑异或密码算法。由逻辑异或的运算性质，此方法描述如下：

给定明文序列 m＝ {m_1，m_2，…，m_n}，密钥 k，这里 m_i、k均为存储字。

加密：$c_i = m_i \oplus k$　　$i=1, 2, \cdots, n$

解密：$m_i = c_i \oplus k$　　$i=1, 2, \cdots, n$

此方法的容易由程序实现：

```
XOR_cipher( int length, char key, char * m, char * d);
蛐蛐是长度为 length的明文字符序列，c为对应密文输出，key是“密钥”
{
for( i=0; i< length; i++) d[ ] =m[ ]⊕ key 蛐蛐⊕表示按位异或
}
```

对于例 1.2.1，如果知道明文是英文短语，则通过英文字母频率分布不难导出字符替换表。对于例 1.2.2，即使考虑增加位串 k的长度使破解稍稍困难些，专业密码分析家也能够在几分钟内解决问题。但以上例子给出现代密码学的一些基本概念：

给定明文消息空间 M，密文消息空间 C，加密算法 E_k：M→C，解密算法 D_k：C→M。对任意明文消息 m∈M加密：c＝E_k(m)　解密：m＝D_k(d)。这里，当加密函数 E取定后，密文 c的值依赖于明文 m和密钥 k，k的所有可能取值的集合称为密钥空间 K。因此该密码系统可以记为(M，C，K，E_k，D_k)，如图 1.2.3所示。具有实际保密意义的密码系统应该满足以下要求：

1) 系统的保密性不依赖于算法，仅依赖于密钥，即算法可以公开，一切秘密在密钥中。

2) 加密、解密算法适用于密钥空间中的所有元素。

3) 从截获的密文或者若干已知密文蛐明文对推出密钥或者任意明文，在计算上实际是不可行的。

4) 解密密钥 k是由加密密钥 k惟一确定的。由 k确定 k很容易，由 k确定 k通常在计算上不可行。

5) 系统便于实现和使用。

(2) 密码编码系统的制定

1) 加密算法的操作类型：实现明文转变为密文的基本策略是替代和置换。替换是将明

文中的每个元素（位、字节、数据块等）映射为另一个元素；置换是将明文中元素进行重排。通常一个加密算法可以分为若干阶段，每个阶段都是替代和置换的混合使用。原则上每个阶段都是可逆转的。

2）密码系统中使用的密钥个数：图 1-3a所示的系统中，加密、解密采用同一密钥，这如同关门、开门用同一把钥匙。这种系统称为单钥密码或者对称密码系统。单钥密码系统的优点是算法处理效率较高，通常宜于硬件实现。问题是密钥传送和管理十分困难：密钥必须通过另外的秘密信道传送或者分发。

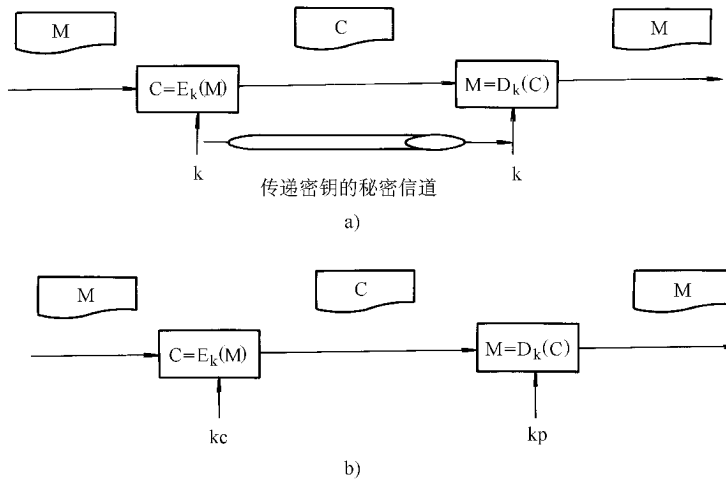

图 1-3 密码系统

a）单钥密码系统 b）公钥密码系统

一个具有 n个用户的系统，如果要求保证其中任意两个用户之间通信的机密性，每个用户应该保持（n－1）个密钥，整个系统必须有效管理 n(n－1)/2个密钥，这些密钥管理本身就是系统安全隐患。

Diffie和 Hellman在 1976年引入公钥密码系统的思想：对明文的加密和解密采用不同的密钥。

$$C=E_{kc}(M)$$

$$M=D_{kp}(C)=D_{kp}(E_{kc}(M))$$

发送者 A向接收者 B发送保密消息 m的过程如下：

1）A首先向 B索取加密 kc（公钥），或者从某个可信的第三方获取；

2）A使用密钥 kc对明文 M加密后发送密文 c；

3）B收到 c后使用密钥 kp（私钥）对密文 c解密。

这样的通信系统中，每个用户可以将自己的加密密钥公开，解密密钥保密。这种密码系统中密钥管理安全性较高，不需要传递密钥的秘密信道，通常称为公钥密码系统，其基本模型见图 1-3b。

3）明文加密处理方式：将明文看作明文基本元素流，连续地对每个元素进行加密处理，每处理一个输出一个。这种方式称为流密码。流密码是传统密码编码学中常见的一种密码系统。如果将明文中连续的若干元素看作一个组块，加解密处理以组块为单位。这种处理方式

称为分组密码。现代密码学推荐使用分组密码，认为其抗攻击强度高于流密码。

1.2.2 密码分析简介

密码分析的前提是在未知密钥的前提下试图通过密文得到明文 M或者系统密钥。密码攻击者所使用的攻击策略依赖于密码算法和攻击者可以得到的信息，常用的密码攻击类型如表 1.2.1所示。这里认为密文是可以获取的，密码算法是已知的。

表 1.2.1 密码系统攻击类型

攻击类型	密码攻击者已知的信息
惟密文攻击	加密算法、待破译的密文
已知明文攻击	加密算法、待破译的密文
	一段或者多段已知明文-密文对
选择明文攻击	加密算法、待破译的密文
	攻击者选择的明文消息以及对应的密文
选择密文攻击	加密算法、待破译的密文
	攻击者选择的密文消息以及相应解密的明文段

惟密文攻击是最困难的。这时攻击者只已知加密算法和消息密文，攻击者的任务是尽可能恢复已知密文对应的明文。当然，最好是推出加密消息的密钥。惟密文攻击可以表述为：

已知：$C_1=E_k(M_1)$，$C_2=E_k(M_2)$，…，$C_i=E_k(M_i)$

推出：M_1，M_2，…，M_i；或者找出密钥 K和一个算法 D′，使得对任意 $C=E_k(M)$，可以推导 $M=D_k'(C)$。

已知明文攻击是指攻击者除可以得到密文外，还可能获取若干已知明文-密文对应段。例如某份已解密报告和该报告的密文副本，或者知道密文中一定含有某个特定消息模式（如公司名称、文件类型标识等）。攻击者的任务是根据这些已知明文-密文对推导出密钥或者一个解密算法，此算法可以对用同一密钥加密的任何消息密文解密。已知明文攻击可以表述为：

已知：M_1，$C_1=E_k(M_1)$，M_2，$C_2=E_k(M_2)$，…，M_i，$C_i=E_k(M_i)$

推出：密钥 K，或者一个算法 D′，使得对任意 $C=E_k(M)$，可以推导 $M=D_k'(C)$。

选择明文攻击是指攻击者能够在对象系统中插入攻击者自己选择的明文消息，然后截获、分析这些消息的密文，从中推导出密钥或者一个解密算法，此算法可以对用同一密钥加密的任何消息密文解密。选择明文攻击可以表述为：

已知：攻击者选择的 M_1，$C_1=E_k(M_1)$，M_2，$C_2=E_k(M_2)$，…，M_i，$C_i=E_k(M_i)$

推出：密钥 K，或者一个算法 D′，使得对任意 $C=E_k(M)$，可以推导 $M=D_k'(C)$。

选择明文攻击的另一个更有效的方法是攻击者不仅能够选择被加密的明文，而且能够基于以前加密的结果修正这个选择，这种方法被称为自适应选择明文攻击。

选择密文攻击是指选择特定的密文，利用解密算法导出对应明文，攻击者的任务是推出密钥：

已知：C_1，$M_1=D_k(C_1)$，C_2，$M_2=D_k(C_2)$，…，C_i，$M_i=D_k(C_i)$

推出：K

选择密文攻击通常用于公开密钥算法。这种攻击的另一种方式是攻击者利用密钥之间相