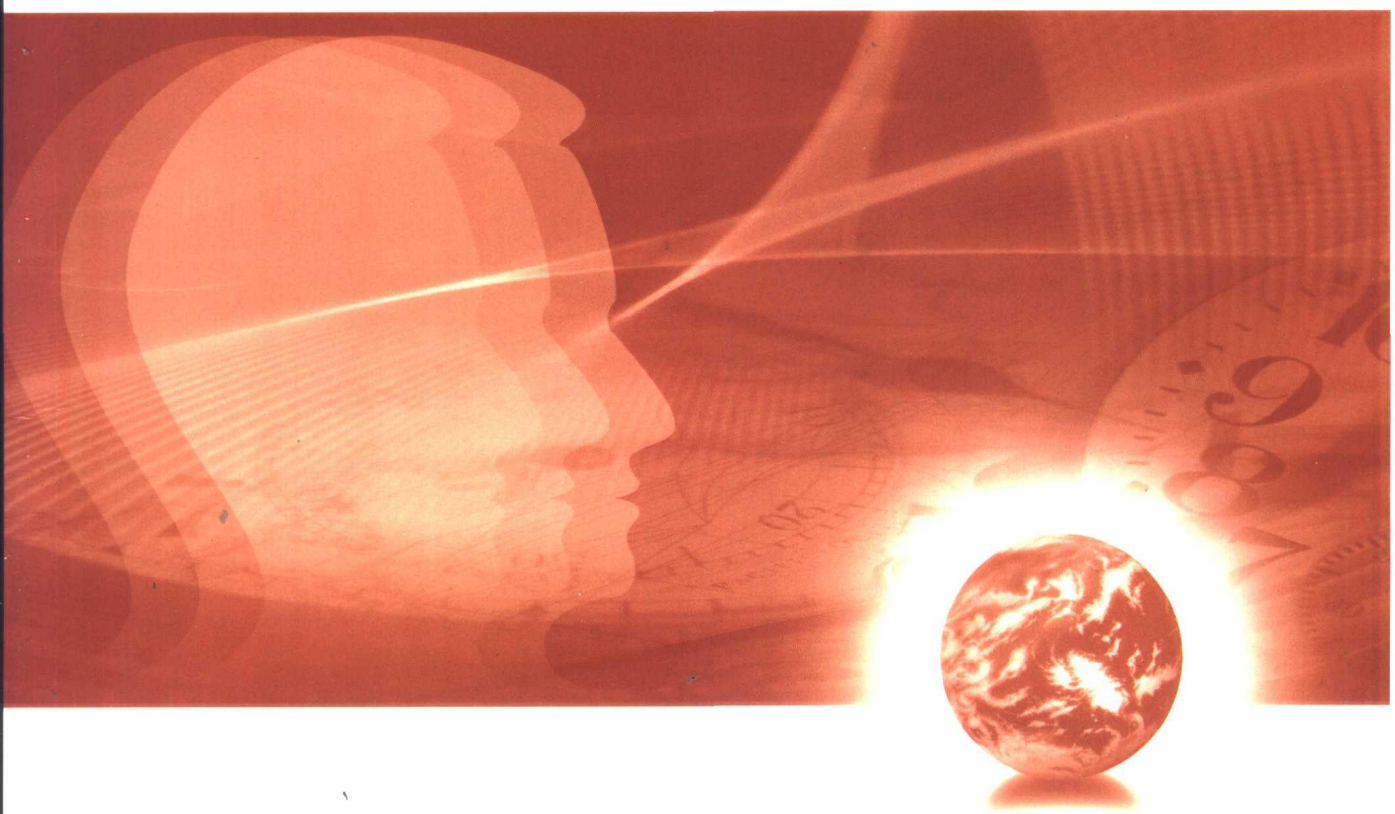
高等院校计算机科学与技术
“十五”规划教材

网络与信息安全教程



林柏钢 编著

机械工业出版社
CHINA MACHINE PRESS

高等院校计算机科学与技术“十五”规划教材

网络与信息安全教程

林柏钢　编著

机械工业出版社

本书围绕网络与信息安全发展前沿的热点问题，比较全面地介绍了网络与信息安全的基本理论和应用实践的最新成果。全书共 12 章，内容包括：绪论、信息安全的基础理论、传统密码、序列密码、分组密码、公钥密码、现代网络高级密码协议、密钥管理技术、通信网络安全保密技术、计算机网络系统集成安全技术、网络安全测试工具与应用技术、电子商务协议与安全管理等内容。全书材料丰富、覆盖面广、可读性强。

本书可供电子、计算机、信息安全等专业的本科生、研究生自学使用，也可供网络与信息安全的科技人员与管理人员，以及关心该领域发展的广大读者作为参考书。

图书在版编目（CIP）数据

网络与信息安全教程/林柏钢编著. —北京：机械工业出版社，2004.6
高等院校计算机科学与技术“十五”规划教材
ISBN 7-111-14673-5

Ⅰ. 网… Ⅱ. 林… Ⅲ. 计算机网络—安全技术—高等学校—教材

Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2004）第 056252 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
责任编辑：李利健
责任印制：洪汉军

三河市宏达印刷有限公司印刷 • 新华书店北京发行所发行

2004 年 7 月第 1 版第 1 次印刷
787mm×1092mm　1/16 • 23.5 印张 • 610 千字
0001－5000 册
定价：33.00 元

出 版 说 明

信息技术高度普及的今天，具备一定层次的信息技术素养成为社会素质教育的一个重要目标，由此对高等院校的计算机专业教育提出了更高更新的要求。教育水平提高的关键是教学质量，那么对教学质量有直接影响的教材建设就成为了计算机专业教育的根本，为重中之重。

适逢高等院校计算机专业教育改革的关键时期，为配合相关的教材建设，机械工业出版社会同全国在该领域内享誉盛名、具备雄厚师资和技术力量的高等院校，包括清华大学、上海交通大学、南京大学、电子科技大学、东南大学、西安电子科技大学、解放军理工大学、北京科技大学等重点名校，组织长期从事教学工作的骨干教师，集思广益，对当前高等院校的教学现状开展了广泛而深入的研讨，继而紧密结合当前技术发展需要并针对教学改革所提出的问题，精心编写了这套面向普通高等院校计算机专业的系列教材，并陆续出版。

本套教材内容覆盖了普通高等院校计算机专业学生的必修课程，另外还恰如其分地添加了一些选修课程，总体上分为基础、软件、硬件、网络和多媒体五大类。在编写过程中，对教学改革力度比较大、内容新颖以及各院校急需的并且适应社会经济发展的新教材，优先选择出版。

本套教材注重系统性、普及性和实用性，力求达到专业基础课教材概念清晰、深度合理的标准，并且注意与专业课教学的衔接；专业课教材覆盖面广、深浅适中，在体现相关领域最新发展的同时注重理论联系实际。全套教材体现了教育改革的最新思想，可作为高等院校计算机科学与技术专业的教学用书，同时也是培训班和自学使用的最佳教材。

机械工业出版社

前　言

随着计算机网络技术的迅猛发展和网络系统的深入应用，信息网络的社会化和国际化使人类社会的生活方式发生了重大变化。网络化、数字化应用业务大量涌现，电子商务（EC）、电子政务（EG）、远程教育（DE）、网络银行（NB）、网络媒体（NM）、数字图书馆（DL）等走进了我们的生活中。电子网络已经成为今天的各项社会生活赖以存在的基础设施。在当今社会中，不能想象，没有信息系统支持的邮电、金融、民航、商务等行业如何为客户提供服务。同样不可想象的是，没有信息安全保障的信息系统，将会发生什么样的后果。

因此，网络与信息系统越发展到高级阶段，人类社会对它的依赖性就越强。从某种意义上说，“网络社会”越发达，它遭受攻击的危险性也越大。特别是信息成为社会发展的重要战略资源之后，国际上围绕信息的获取、使用和控制的斗争也愈演愈烈。网络安全、信息安全成为维护国家安全和社会稳定的一个焦点，各国政府、各大企业公司和研究机构都把目光投向网络和信息安全领域，优先发展信息安全产业也成为社会和经济发展的一种主流声音。

另一方面，进入新世纪后，我国的信息安全形势更加严峻。计算机黑客的猖獗、计算机病毒的泛滥、有害内容的恶性传播、国际信息间谍的潜入、网络恐怖活动的威胁、战争的阴影笼罩，以及网络攻击和犯罪活动等等，都呈明显上升趋势。信息化引发的网络信息安全问题，不仅涉及国家的经济安全、金融安全和社会安全，同时也涉及国防安全、政治安全和文化安全。简单地说，网络信息安全最终牵涉到的就是国家安全。

面对严重的网络与信息安全威胁，加大国家信息化安全保障体系刻不容缓，提高全民的安全防范意识，加速培养网络与信息安全专门人才的目标任重而道远。重视信息安全已成为全社会的共识，研究网络信息安全的现状、规律和发展，研究信息安全基本理论、安全基础设施、安全技术与应用以及安全政策和管理，这是本书的出发点，目的是让读者有所启发，有所收获，有所提高和应用。

网络与信息安全教程一书共分 12 章。各章节主要内容安排是：第 1 章为绪论；第 2 章是信息安全的基础理论；第 3～7 章分别为：传统密码体系、序列密码、分组密码体系、公钥密码体系、现代网络高级密码体系；第 8 章为密钥管理技术；第 9 章介绍网络通信安全保密技术与实现；第 10～12 章依次为：计算机网络系统集成安全技术、网络安全测试工具与应用技术、电子商务协议与安全管理。本书力求紧跟国内外网络与信息安全技术前沿，全面、简单、系统地反映网络与信息安全的理论和实践。

在本书的策划和编写过程中，参阅了国内外有关作者的大量文献和资料，得到了福州大学数学与计算机学院和计算机系统结构研究所有关领导、同事和朋友的大力支持和帮助，研究生洪淼、李国金、李青岩、廖建国、宋永林、林德敬、黄淑宽、陈肇宇、周贵堂等，为本书的出版做了大量的具体工作，在此一并表示衷心的感谢。

本书的部分研究工作得到了国家自然科学基金项目（60172017）和福建省政务信息共享平台安全评估技术研究课题的资助。

由于网络与信息安全的技术发展非常快，本书的选材还有一些不尽如人意的地方，加上笔者学识水平和时间所限，书中难免存在不足之处，敬请广大读者批评指正，以便进一步完善提高。

编　者

目　录

第1章 绪 论

本章将着眼网络与信息安全的整体、宏观和系统层次发展，从最基本的信息与网络安全概念出发，侧重围绕信息安全基本概念（信息安全问题、面临威胁、保密学和保护技术）、网络信息安全体系结构（基本框架、安全机制、安全标准）以及网络信息安全发展等问题作简单介绍。

1.1 信息安全基本概念

1.1.1 信息安全问题

信息无所不在，无所不有。信息作为广义的概念，越来越被人们习惯地理解为：人类在认识世界和改造世界过程中获取的各种数据、消息和知识，以及各种事物间运动差异表现出来的不同状态和方式。不同研究领域对信息的理解是不一样的，比如说，数学上理解信息就是概率论，物理上说信息就是熵概念，通信上的信息就是解除不定度，哲学上谈信息归结为认识论，等等。尽管学术界不同学科对信息的定义有不同的理解，但不管怎样，在人们的日常生活中，信息成了看得见、听得到的东西（当然也包括看不到、听不见的东西）。通俗地说，信息指的就是数据、消息和资讯等一类概念。

当今社会，信息越来越重要。信息不仅是一种宝贵的智力资源，同时也是每个国家重要的战略资源。信息作为一种传播载体和可利用资源，已经深入人心。随着社会的进步发展和不同社会的差异变化，使原本属于中性的“信息”概念，也逐渐显现出它的公开性和保密性两个最基本的主要特性。信息的公开性概念反映出信息的传播属性范围，哪些信息属公众信息，哪些信息属内部信息。公众信息一般理解为非保密性的，内部信息通常理解为带有保密性的。当然，公众信息也并非不具有保密安全性，公众信息和内部信息在某些特定场合和范围中也是有所界定的。比如，在报纸上登载一个工程师的特长档案信息没什么值得大惊小怪，但若公开一个单位、一个系统、一个区域、一个省的整体工程师的特长档案信息那是非常有价值的。信息的安全性特征强调信息保密的安全程度，一般地说，内部信息要求具有保密性或安全性。信息的保密性和安全性就是人们通常所说的“信息安全”的属性范围的概念。

何谓“信息安全”？其实，它指的就是在网络环境下信息系统中的数据受到指定保护，不因偶然和恶意的原因而遭到破坏、更改、泄漏，使信息系统能连续、可靠、正常地运行，或因破坏后还能迅速恢复正常使用的安全过程。信息安全反映出有用信息的本身使用价值以及在收集、存储、传送、交换、加工处理过程中的保密程度要求。信息安全也说明信息本身价值的安全和信息技术安全两个层面。只要信息属于个人、企业、国家的使用价值范围，以及它的保护外延性，就说明信息本身需要保证安全性。其次，对保护信息对象的操作，不论是具体的信息内容，还是特定的信息体系，都需要信息安全技术来保证。对国家而言，信息安全就是确保社会信息化状态和信息技术体系不受外来侵袭和破坏。

在网络发展的今天，共享信息成为一种基本需求。信息安全实质上主要体现为网络信息安全，这使得信息安全的概念所赋予的范围更广，内容更丰富，系统更复杂。因此，网络上的信

息安全从个人财产档案信息、企业的商业机密到国家信息化建设（包括国防信息现代化建设）等等相关的信息安全内容都至关重要。忽略信息安全问题，只把安全机制建立在物理安全机制上是远远不够的。尤其对国家来说，信息安全事关大局，切不可掉以轻心。

1.1.2 信息安全面临威胁

由于计算机网络技术的飞速发展，依赖计算机网络系统完成传送、存储和处理信息的作用明显加强。网上银行、网上市场、网上电子商务、网上电子政务等形式层出不穷。网上数据流、信息流和资金流已成为当今网络世界不可缺少的主要部分。随之而来的网络信息安全问题也更加突出。面临的主要威胁表现为：

1. 通信传输威胁

这是反映信息在计算机网络系统的通信过程中面临的一种严重的威胁，体现出数据流通过程的一种外部威胁。常见的攻击手法主要有：截获、中断、伪造和篡改等。

- 截获——攻击者可从网络上窃听他人的通信内容；
- 中断——攻击者有意中断他人在网络上的通信内容；
- 伪造——攻击者任意伪造信息在网络上向攻击目标传送；
- 篡改——攻击者故意篡改传送过程中的真实信息。

2. 存储攻击威胁

存储攻击威胁通常是指存储在计算机系统或服务器、数据库中的数据信息面临的一种严重攻击威胁，体现出数据存放中的一种常见的内部威胁。其攻击手法主要有：数据窃取、变更、重放和抵赖攻击等。对数据的窃取和变更形式，攻击者可从计算机硬盘和数据库中窃取有用的数据信息。攻击者可能利用计算机系统硬件设备的电子辐射了解系统的内部信息，也可能利用非法用户进入计算机系统，窃取或变更内部信息资料。对人为因素的破坏案件，近几年都呈明显上升趋势，而且人为的恶意攻击隐蔽性很强，具有更大的危害性。

对于抵赖攻击行为，恶意攻击者否认信息的原始性存储资料，造成信息真实性的混乱。这在电子资金交易场合尤为突出。

3. 信息系统威胁

正因为信息系统已成为国家的重要战略资源，信息技术体现在国防上就是一种现实的战斗力。因此，从某种意义上说，控制信息权与反控制信息权是一场没有硝烟的战争。来自信息系统的威胁主要有：信息战、软件攻击、黑客与病毒攻击，以及安全缺限等。

（1）信息战

它指不择手段地获取信息控制权的一种攻击方式。由于获取信息控制权已经提升为衡量一个国家战略资源的能力，因此信息战就演变为一种国家行为的恶意攻击威胁。攻击目标主要是军事指挥通信系统、能源、运输、金融等与国家政治、经济、文化、国防密切相关的信息系统。20 世纪 90 年代和 2003 年的两场伊拉克战争就是一例，美军在伊拉克实施的“沙漠风暴”行动期间，迅速摧毁伊方关键的通信中心，使伊方处于被动的战略境地。

（2）软件攻击

它指对计算机系统的软件进行攻击的一种方式，易对整个信息系统造成巨大损失。软件攻击包括：软件删除（比如信息文件有意删除）、软件漏洞修改（诸如病毒感染破坏，设置秘密陷门，信息转移泄漏等）、软件复制盗窃等。

（3）安全缺限

它主要指构筑信息系统的软硬件安全缺限。硬件方面包括计算机设备、通信链路、网络产品、网络结构、电磁辐射等缺限，构成了网络信息系统的潜在威胁；软件方面包括软件程序漏洞、操作系统漏洞、数据库漏洞、TCP/IP 协议漏洞、网络软件漏洞以及登入口令设置漏洞等等，都是潜在的安全缺限威胁。

据不完全统计分析，1998 年公安部有关部门受理网络犯罪案件仅 100 多起，1999 年增至 400 多起，2000 年剧增为 2700 多起，2001 年增加到 4500 多起，比 2000 年上升 70%，2002 年又上升到 6600 多起，而且仅 2003 年上半年就有 4800 多起，比同期上升 77.1%。

总之，信息安全威胁类型很多，无法一一列举。归结我国信息安全现状的威胁，主要是下面几点应引起我们的重视：

- 信息与网络安全的防护能力相对欠缺，安全漏洞仍然不少；
- 基础信息产业相对薄弱，与国外同行业相比差距还比较大；
- 国内具有知识产权的信息与网络安全产品相对缺乏，而且安全功能急待提高；
- 信息安全管理力度还要加强，法律法规滞后现象急待解决；
- 信息犯罪形势依然严峻，有效打击犯罪行为的技术手段和人为监管都应注重实效；
- 全社会的信息安全意识急待提高，加强教育，加紧培训专门安全人才刻不容缓。

1.1.3 网络信息安全特征与保护技术

1．信息安全特征

保证信息安全，最根本的就是保证信息安全的基本特征发挥作用。因此，下面先介绍信息安全的五大特征。

（1）完整性（integrity）

它指信息在传输、交换、存储和处理过程保持非修改，非破坏和非丢失的特性，即保持信息原样性，使信息能正确生成、存储、传输，这是最基本的安全特征。

（2）保密性（confidentiality）

它指信息按给定要求不泄漏给非授权的个人、实体或过程，或提供其利用的特性，即杜绝有用信息泄漏给非授权个人或实体，强调有用信息只为授权对象使用的特征。

（3）可用性（availability）

它指网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并能投入使用。可用性是衡量网络信息系统面向用户的一种安全性能。

（4）不可否认性（Non-Repudiation）

它指通信双方在信息交互过程中，确信参与者本身，以及参与者所提供的信息的真实同一性，即所有参与者都不可能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

（5）可控性（controllability）

它指对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性，即网络系统中的任何信息要在一定传输范围和存放空间内可控。除了采用常规的传播站点和传播内容监控这种形式外，最典型的如密码的托管政策，当加密算法交由第三方（或任何方）管理时，必须严格按规定可控执行。

2. 信息安全保护技术

网络信息安全强调的是通过技术和管理手段，能够实现和保护消息在公用网络信息系统中传输、交换和存储流通的保密性、完整性、可用性、真实性和不可抵赖性。因此，当前采用的网络信息安全保护技术主要是两个类型：主动防御技术和被动防御技术。

（1）主动防御保护技术

主动防御保护技术一般采用数据加密、身份鉴别、存取控制、权限设置和虚拟专用网络等技术来实现。

1）数据加密。密码技术被公认为是保护网络信息安全的最实用方法。对数据最有效的保护就是加密,因为加密的方式可用不同手段来实现。

2）身份鉴别。身份鉴别强调一致性验证，验证要与一致性证明相匹配。通常，身份鉴别包括：验证依据、验证系统和安全要求。

3）存取控制。存取控制表征主体对客体具有规定权限操作的能力。存取控制的内容包括：人员限制、访问权限设置、数据标识、控制类型和风险分析等。它是内部网络信息安全的重要方面。

4）权限设置。规定合法用户访问网络信息资源的资格范围，即反映能对资源进行何种操作。

5）虚拟专用网技术。使用虚拟专用网（VPN—Virtual Private Network）或虚拟局域网（VLAN）技术。VPN 技术就是在公网基础上进行逻辑分割而虚拟构建的一种特殊通信环境，使其具有私有性和隐蔽性。VPN 也是一种策略，可为用户提供定制的传输和安全服务。

（2）被动防御保护技术

被动防御保护技术主要有防火墙技术、入侵检测系统、安全扫描器、口令验证、审计跟踪、物理保护及安全管理等。

1）防火墙技术。防火墙是内部网与 Internet（或一般外网）间实现安全策略要求的访问控制保护，是一种具有防范免疫功能的系统或系统组保护技术，其核心的控制思想是包过滤技术。

2）入侵检测系统。IDS（Intrusion Detection System）就是在系统中的检查位置执行入侵检测功能的程序或硬件执行体，可对当前的系统资源和状态进行监控，检测可能的入侵行为。

3）安全扫描器。它可自动检测远程或本地主机及网络系统的安全性漏洞点的专用功能程序，可用于观察网络信息系统的运行情况。

4）口令验证。它利用密码检查器中的口令验证程序查验口令集中的薄弱子口令。防止攻击者假冒身份登入系统。

5）审计跟踪。它对网络信息系统的运行状态进行详尽审计，并保持审计记录和日志，帮助发现系统存在的安全弱点和入侵点，尽量降低安全风险。

6）物理保护与安全管理。它通过制定标准、管理办法和条例，对物理实体和信息系统加强规范管理，减少人为管理因素不力的负面影响。

1.1.4 网络信息安全与保密学

在网络信息安全基本特征中关键的问题是保密性。确保信息的保密安全，主要就是使用密码技术，因为密码技术是信息安全技术中的核心技术，它推进和加速了保密学理论的发展。

保密学（Cryptology）是研究信息系统安全保密的科学，从技术的角度说，保密学就是密码学。它是研究密码系统或通信安全的一门科学。其主要内容包括两个方面：密码编码学（Cryptography）和密码分析学（Cryptanalytics）。密码编码学是对信息进行编码，保证消息保

密性和隐蔽性以及认证性的一门学问；而密码分析学是研究分析密码破译或验证消息真伪的学问。密码编码学和密码分析学共同组成密码学。

密码学的历史既古老又年轻，随着人类社会战争的延续和通信发展的需要，为了保护真实信息，采用伪装后再传递的做法，逐步演变产生了密码技术，以后慢慢形成一门独立学科，而且逐步变成计算机科学、通信技术和信息领域中一门具有生命力的主要学科。在这里，科学技术发展和社会竞争（主要是战争）的刺激推动了密码学的发展。因为密码技术的基本思想是伪装信息，尽可能地隐蔽和保护所需要的消息，使未授权者无法理解真实含义。现代的信息伪装技术各种各样，常用的伪装方法就是对信息进行一组可逆的数学变换，变成密文后在信道中传输。还原伪装的方法就是通过解密方法恢复信息的原样性。

下面对密码学的有关概念作初步介绍。

在一个密码系统中，伪装前的原始信息（或消息）称明文（plaintext），伪装后的信息（或消息）称为密文（ciphertext），伪装过程称为加密（encryption），其逆过程，即由密文恢复出原明文的过程称为解密（decryption）。实现消息加密的一组伪装规则（或数学变换）称为加密算法（Encryption Algorithm），对密文进行解密时所采用的一组恢复伪装规则（或数学反变换）称为解密算法。加密算法和解密算法的操作通常都是在一组密钥（key）的控制下进行的，分别称为加密密钥和解密密钥，这个过程如图 1-1 所示。通过各种手段窃取信息机密过程称为窃密，利用技术分析或破解所截获的密文，并用来推断出明文或密钥的过程称为密码分析（cryptanalysis）。

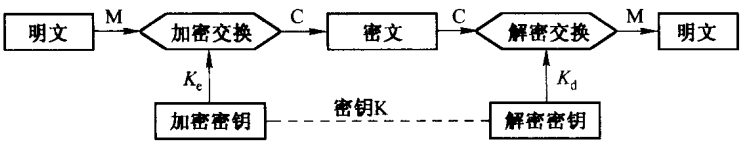


图 1-1　信息伪装的加、解密过程示意图

进一步分析密码体制可以发现，当 $K_e=K_d$ 时，习惯上称为单密钥密码体制或对称密码体制（one－key or symmetric cryptosystem），传统密码体制即属于这种类型，特点是：加密密钥和解密密钥相同，由其中一个很容易推出另一个。算法简单易实现，但密钥管理相对困难。而当 $K_e \neq K_d$ 时，通常称为双密钥密码体制或非对称密码体制（Two－key or Asymmetric cryptosystem），现在流行的公开密钥密码体制即属此类型，特点是：K_e，K_d 不一样，计算 K_d 时无法由 K_e 推出，即使将 K_e 公开，也不影响 K_d 的安全。因此，特别适合计算机网络和分布式计算机系统应用。算法复杂，难实现，但密钥管理相对容易。

密码学发展迅速，加密技术手段也不断出现，有关其他更多的概念将在后续章节中介绍。

信息保密作用是伪装后的信息可以存储在计算机文件中，也可以流通在计算机网络中，即使此时信息遭受窃取或某种原因破坏而泄漏，未授权者也无法理解真实的含义，此时保密便起到保护信息的真实性而不泄密的作用。

作为密码理论的重要发展，主要经历了密码技术发展的四个阶段：

- 第一阶段（1949 年前）：密码学发展初期阶段，未形成一门独立的学科；
- 第二阶段（1949 年～1976 年）：密码学形成学科阶段，以 1949 年 Shannon 发表的“保密通信的信息理论”为标志；
- 第三阶段（1976 年后）：密码学新体制形成与发展阶段，以 1976 年 Diffie 和 Hellman 发