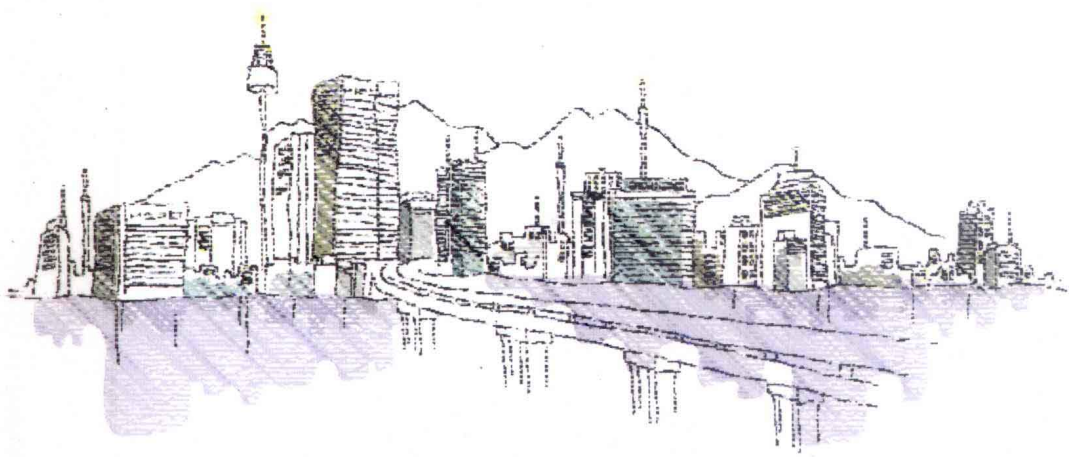
工业和信息化普通高等教育“十二五”规划教材
21世纪高等学校计算机规划教材
21st Century University Planned Textbooks of Computer Science

大学计算机基础

Fundamentals of Computer Science and Technology

段跃兴 主编

- 内容丰富新颖，工作流程由浅入深
- 概念通俗易懂，基础理论实例阐明
- 全书思路清晰，目标明确实用性强



高校系列

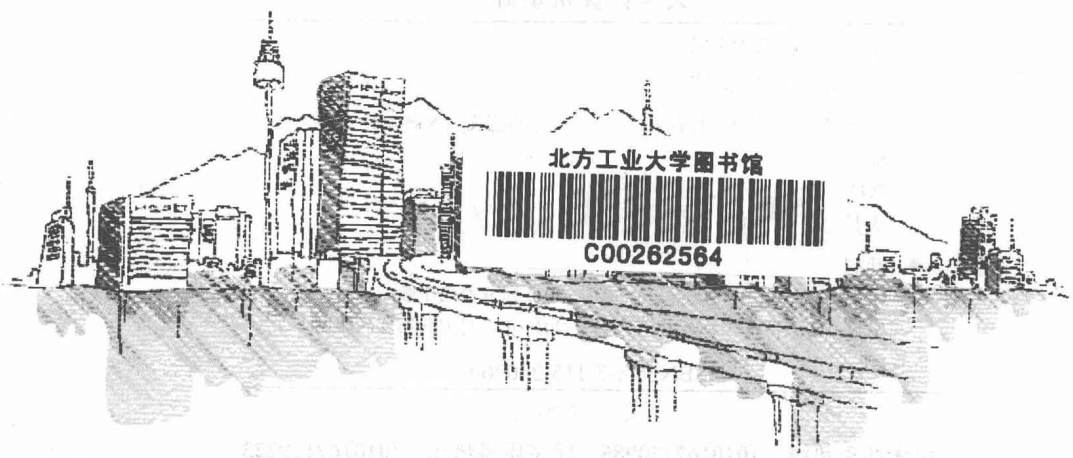
人民邮电出版社
POSTS & TELECOM PRESS

工业和信息化普通高等教育“十二五”规划教材
21世纪高等学校计算机规划教材
21st Century University Planned Textbooks of Computer Science

大学计算机基础

Fundamentals of Computer Science and Technology

段跃兴 主编



高校系列

人民邮电出版社
北京

图书在版编目（CIP）数据

大学计算机基础 / 段跃兴主编. -- 北京 : 人民邮电出版社, 2011.9(2011.9 重印)
21世纪高等学校计算机规划教材
ISBN 978-7-115-26026-0

Ⅰ. ①大… Ⅱ. ①段… Ⅲ. ①电子计算机－高等学校－教材 Ⅳ. ①TP3

中国版本图书馆CIP数据核字(2011)第174276号

内 容 提 要

本书以教育部高等学校非计算机专业计算机基础课程教学指导分委员会提出的“关于进一步加强高等学校计算机基础教学的意见”（简称白皮书）中“大学计算机基础”课程的教学大纲为依据，将一线教师多年实际教学经验与计算机领域中的科学知识相结合，以知识上严谨、内容上全面、语言上流畅为目的而精心编写的。

全书共分 8 章，主要内容包括：计算机硬件知识、操作系统、计算机网络、算法与程序设计、多媒体技术、数据库技术和常用软件的介绍。该书内容全面、概念清晰、语言流畅、图文并茂、通俗易懂。通过本书的学习，不但能使当今的大学生较全面地了解计算机系统的基础概念、主要工作流程与工作原理，还能为程序设计、计算机网络、操作系统、数据库应用、多媒体技术及相关的后续课程的学习打下坚实的理论与实践基础，书中所述内容均是学习计算机理论和熟练掌握计算机操作的必备知识。

本书可作为各高等院校非计算机专业计算机基础教学的教材，也可作为计算机爱好者全面、深入学习计算机知识的实用参考书籍。

21 世纪高等学校计算机规划教材

大学计算机基础

◆ 主　　编　段跃兴
责任编辑　邹文波

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
大厂聚鑫印刷有限责任公司印刷

◆ 开本：787×1092　1/16
印张：22.5　　2011 年 9 月第 1 版
字数：596 千字　　2011 年 9 月河北第 2 次印刷

ISBN 978-7-115-26026-0

定价：37.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154
广告经营许可证：京崇工商广字第 0021 号

前　言

20世纪是人类社会极其辉煌的世纪，电子计算机、Internet的出现与迅猛发展使我们的学习、工作、生活发生了日新月异的变化，人类社会迈入了信息化的时代。面对飞速发展的世界我们应该更多地关注科研领域，因为科技力量决定着一个国家现代化进程的脚步。学科中的专业知识与以计算机为核心的信息技术之间的相互渗透越来越紧密相容，极大地促进了科学研究的发展，而这同时也意味着专业知识的学习，需要当今大学生们了解和掌握更多的计算机知识及相应的操作，能否驾驭计算机已成为衡量一个现代人综合素质高低的重要标志之一。

在此背景下，教育部高等学校非计算机专业计算机基础课程教学指导分委员会提出了“关于进一步加强高等学校计算机基础教学的意见”（简称白皮书），在白皮书中正式颁布了“大学计算机基础”课程教学大纲。大纲要求大学生应具备一定的计算机操作应用技能，全面了解计算机系统知识，理解数据库、多媒体中的相关概念，熟悉计算机网络、应用程序的开发流程，最终能搭建起属于自己的专业应用软件系统。为此我们深入研究了课程教学大纲，积极探索当今大学生的学习规律与方式方法，结合多年的教学工作经验，精心编写了此书。其目的就是想使同学们对计算机及其技术能有一个全方位的、正确的认识，培养起良好的信息素养，为今后专业知识的学习奠定坚实的基础，同时也希望此书能在教学环节中起到积极向上的作用。

全书分为8章，在内容组织上由浅入深、循序渐进，力图做到概念准确、重点突出、原理清晰，反映计算机及其技术的基础知识与最新理念。主要内容包括：计算机硬件知识、操作系统、计算机网络、程序设计、多媒体技术、数据库技术和常用软件的介绍。

该书的特色：一是内容全面、重点突出。从低层硬件知识到应用软件的开发，从单台的微型计算机到组合而成的计算机网络，全书内容基本涵盖了整个计算机及其应用系统的知识点。在每个环节，知识点明确，力争做到以点带面。二是经典内容与新技术相结合。在保证系统整体性的前提下，阐明最基本的工作原理和技术指标，反映了计算机及其技术的较新发展和应用。三是语言通俗易懂，书写流畅。对于计算机系统中的主要工作过程和基本原理，书中用通俗易懂的语言，并尽可能地选用具有代表性的实例来辅助说明，以便加深读者的理解。

本书由从事计算机基础教学多年并具有丰富实践教学经验的教师集体编写而成，第1章由段跃兴执笔、第2章由张晓霞执笔、第3章由杨丽凤执笔、第4章由王星魁执笔、第5章由孟东霞执笔、第6章由任少斌执笔、第7章由丁华执笔、第8章李华执笔。全书由段跃兴统稿，山西大学李德玉教授审稿。

由于编者水平有限，书中难免存在错误和不妥之处，敬请读者批评指正。

编者联系信箱为：dyxty01@163.com

编者

2011年7月

目 录

第 1 章 概论

计算机是 20 世纪人类最伟大的科学技术发明之一，它的出现和发展大大推动了人类科学技术的发展，在短短 50 多年的时间里，计算机及其技术已渗透到社会的各行各业，并取得了巨大成就。计算机已由最初的“计算”工具，演变成了适用于多种领域，并具有获取、存储、传输、处理、表示、控制信息等功能的高科技产品。计算机不仅是现代人类活动中不可缺少的工具，同时对它的认识与掌握也是衡量一个当代高素质人才的重要标准之一。

计算机处理的对象是信息，信息的处理也离不开计算机。用计算机处理信息具有快捷、方便、准确、容量大等特点，计算机的普及使用使信息的数量急剧增加、质量急剧提高，信息的处理更加依赖于计算机，这又进一步地推动了计算机及其技术的发展，信息与计算机就是这样相互依赖相互促进地发展着。本章将从信息、计算机系统的基本概念入手，介绍它们的基本知识、相关特征及应用领域，使读者对信息、计算机系统及其二者的关系有一个初步的了解。

1.1 信息与信息技术

1.1.1 信息的概念

科学技术的发展使人们迈入了信息化时代。早在“十五”规划中，我国就已明确提出了要把推进国民经济和社会信息化工作放在优先的位置，国家的信息化是指在国家统一规划和组织下，在农业、工业、科技、国防及社会生活的各个方面应用现代信息技术，深入开发、广泛利用信息资源，加速实现国家现代化的进程。国家信息化体系的建设包括：信息资源、信息网络、信息技术的应用、信息产业、信息化人才和信息化政策六方面的内容。信息正以不断扩展的含义，渗透到各个科学技术领域以及整个社会当中，人们已认识到信息、材料（物质）、能源（能量）是组成当今社会物质文明的三大要素，信息是一种宝贵的资源。

在科学研究领域，信息论已成为与系统论、控制论等其他学科一样重要的现代科学方法论。那么究竟什么是信息？在国内外公开发行的刊物上对它的解释已达到了 100 余种，众说纷纭，莫衷一是，截止到目前，在专业领域内还没有形成一个严格的、统一的定义。1928 年，哈特莱（Ralph V.L.Hartley）在第 7 期的《贝尔系统技术》杂志上发表了一篇名为《信息传输》的文章，文中首先提出了“信息”这一概念。1948 年信息论奠基人美国科学家香农（C.E.Shannon）在《贝尔系统技术》杂志上发表了一篇名为《通信的数学理论》的长文，该文被认为是信息论诞生的标志，文中对信息的解释是“用以消除随机不确定的东西”。同年控制论创始人美国科学家维纳

（N.Wiener）在《控制论》一书中指出“信息就是信息，既不是物质也不是能量”，专门强调了信息是区别于物质与能量的第三类资源。近代信息管理和信息系统学科认为信息是“事物之间相互联系、相互作用的状态描述”，是“客观世界各种事物变化和特征的反映”。上述定义都比较抽象，采用现实的方式来理解信息时，有几个具有代表性的定义：

- 信息是有一定含义的数据，是用来描述客观世界的知识；
- 信息是对决策或行为有现实或潜在价值的数据；
- 信息是经过加工后的数据，是事物存在或运动状态的表达；
- 信息是数据的含义，数据是信息的载体。

由此可见，数据和信息是两个既有联系又有区别的概念。从广义上讲，信息是一组被加工成特定形式的数据；而数据是可以记录、通信和识别的符号，这种“数据”对使用者来说是有确切含义的，具有实际价值并对当前和未来的活动能产生一定的影响；或表达了现实世界中某种实体的特征。人们通过对信息多年的研究，发现信息有别于其他事物的本质属性主要表现在以下几方面。

① 时效性。信息有着非常强的时效性。一条信息在某一个时刻的使用价值非常高，但过了这一时刻可能就一文不值了，如金融信息、战争信息等。信息的价值同时还取决于使用者的需求及对信息的理解、认识和利用能力。

② 相对性。一条对某人或某群体非常有价值的信息，对其他人或群体可能就毫无价值或价值不大。

③ 共享性。信息可以被多个用户共享，从而得到充分的利用。

④ 传递性。信息可以通过多种形式迅速传输，如计算机网络、电话、广播、书报杂志、磁带光盘等。信息的可传输性优于物质和能源，信息只有通过传播，才能实现共享，才能充分发挥其应有的作用，加速社会的发展。

⑤ 可压性。可以把信息作浓缩处理，即进行集中、综合与概括而又不丢失信息本义的处理。我们现在已经面临着一个如汪洋大海般的信息社会，不剔除无用信息、减少冗余信息，我们将会被“大海”淹没。

1.1.2 信息技术及其应用

现代信息技术是指应用信息科学原理和方法有效利用信息资源的技术体系。一般来讲，信息技术（Information Technology，IT）是指在信息的识别、采集、存储、传输、检索、加工及处理过程中所使用的技术。从内容上看它主要包括计算机技术、通信技术、微电子技术、多媒体技术、自动控制技术、视频技术、遥感技术等。计算机技术是信息技术的核心，离开了计算机技术及其应用，现代信息技术就无从谈起；微电子技术是信息技术的基础，因为芯片是微电子技术的结晶，是计算机的核心部件；通信技术的发展加快了信息传递的速度，从传统的电报、无线电广播、电视到现代的移动电话、卫星通信都离不开通信技术；计算机技术和通信技术紧密相连，是现代信息技术的重要组成部分，二者也是计算机网络的主要组成内容。

信息从采集、存储、传输到后面的分析、加工与处理，要经历多个环节，一般情况下，按工作流程中基本环节的不同，信息技术还可分为信息获取技术、信息传输技术、信息存储技术、信息加工技术及信息标准化技术。信息获取技术包括信息的搜索、感知、接收、过滤等，如电子显微镜、电子望远镜、遥感气象卫星、各种传感器、Internet 上的各种搜索引擎中的技术等。信息传输技术指跨越空间共享信息的技术，按传输的方向又可分为不同的类型，如单向传递与

双向传递技术，单通道传递、多通道传递与广播传递技术。信息存储技术指跨越时间保存信息的技术，如印刷术、照相术、录音术、录像术、缩微术、磁盘术、光盘技术等。信息加工技术是对信息进行描述、分类、排序、转换、浓缩、扩充、创新等的技术。信息加工技术的发展已有两次突破：从人脑信息加工到使用机械设备（如算盘，标尺等）进行信息加工，再发展为使用电子计算机与网络进行信息加工。信息标准化技术是指使信息的获取、传递、存储、加工各环节有机衔接，以及提高信息交换共享能力的技术，如信息管理标准、汉字字符的编码标准、语言文字的规范化等。

21世纪是信息化的社会，在社会信息化的过程中，实践证明只有通过建立强大的信息基础设施，才能使信息资源得到广泛而快速的传递与使用，从而带动和促进社会各行各业的快速发展。信息技术的普及使用深刻影响和改变着人们的生活及工作方式，对当今社会的发展产生了巨大的影响。这主要体现在以下几个方面。

（1）信息高速公路

1993年3月美国率先提出了“国家信息基础结构”（National Information Infrastructure，NII）即我们所说的“信息高速公路”，它是由通信网、计算机系统、信息资源、终端设备和用户构成的，是覆盖了整个国家的一个高速的、双向交互式的信息网络。通过这个网络，可以把政府机关、社会团体、企业、家庭、学校、医院等一一连接起来，为每个单位及公民提供“随时随地随意的”丰富多彩的各种信息服务，从而满足人们在生产、工作、生活和交往中的信息交流和需求，极大地提高工作和生产效率，改善了生活质量，促进了社会的进步。我国在这方面建设了中国公用分组交换网（ChinaPAC）、中国公用数字网（ChinaDDN）、中国教育和科研计算机网（CERNET）、中国公用计算机互联网（ChinaNET）等网络。

（2）远程教育

现代远程教育是应用计算机网络技术和多媒体技术，在数字化环境下进行交互式学习的过程，它涵盖了信息源、网络传输、多媒体终端和网络教学管理四大部分。现代远程教育体系用计算机网络来承载和传播包括图、文、声、像在内的覆盖全部教学内容的教学信息，与用户形成交互式教学模式，实现实时的可视化远程授课、授课点播、同步课业辅导、远程讨论交流、交互咨询答疑等功能，突破了课堂教学和课本教学信息单一化的局限，充分开发和利用信息资源，将多学科、多层次的丰富信息传递给学生。这种开放式教育网的建立，能有效地发挥各种教育资源的优势，有利于全方位培养人才，有利于学习者全面发展，进而形成一个终身学习体系，为社会每一个成员的学习提供机会和平台。

远程教育有两种基本模式：

① 以群体为基础的远程教育：它指的是通过音频、视频或卫星等把分散于不同地方的教师和学习者联系到远处的网络教室中，我国的电视大学系统就是以群体为基础的远程教育方式；

② 以个体为基础的远程教育：这种体制的主要特征是能科学地为个别学生准备远程教材，以及为在远程学习的学生设计学习辅助系统。互联网的飞速发展，为以个体为基础的远程学习创造了条件。

（3）远程医疗

远程医疗目前主要是指人们运用计算机、通信、医疗技术与设备，通过数据、文字、语音和图像资料的远距离传送，来实现专家与病人、专家与医务人员之间异地“面对面”的会诊。在医学专家和病人之间建立起了崭新的合作关系，使病人在原地、原医院即可接受远地专家的会诊并在其指导下进行治疗和护理，这样既可以节约医生和病人大量时间和金钱，同时还能使病人

享受到专家级的治疗。远程医疗除包括远程医疗会诊外，还包括远程医学教育、远程多媒体医疗/保健咨询系统等。实现远程医疗不仅需要解决医疗或临床等医学问题，还需要解决计算机技术、数据通信、计算机网络、数据库等其他各方面问题，需要专业人员把它们应用、集成到医疗网络系统中。

（4）电子商务

所谓电子商务（E-business）是利用计算机技术、网络技术和远程通信技术，实现整个商务（买卖）过程的电子化、数字化和网络化，是在计算机网络上开展的商务活动。当企业要将它们的主要业务，通过企业内部网（Intranet）、外联网（Extranet）以及互联网（Internet）与企业的客户、供销商、其他合作伙伴以及员工直接相连时，其中发生的各种活动就是电子商务。从宏观上讲，电子商务是信息技术的一种崭新应用，是通过电子手段建立起的一种新经济秩序，它不仅涉及计算机技术、数据通信、计算机网络、信息安全和商业交易本身，而且涉及诸如金融、税务、工商等社会其他层面。从微观角度说，电子商务是各种具有商业活动能力的实体（生产企业、商贸企业、金融机构、事业单位、个人消费者等），利用计算机信息网络进行的各项商业活动。

（5）电子政务

电子政务主要指政府工作的电子化和网络化，是政府机构应用计算机技术和网络通信技术对传统政府事务进行的改革。它将政府的管理和服务工作进行集成处理，并在互联网上实现政府工作流程的优化组合。通过电子政务的实施，政府事业单位能超越时空与部门分隔的限制，全方位地向社会提供优质、规范、透明、符合国际水准的管理和服务。

1.1.3 信息安全

信息是一种资源，就像日常中的其他资产一样有着自身的价值，信息安全就是指如何来保护信息以免受到来自各方面、各个层次的威胁。这里有两层含义：一是数据（信息）的安全，二是信息系统的安全。数据安全是指对所处理的数据要保证其机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。而信息系统的安全是指构成信息系统三大要素的安全，即信息基础设施安全、信息资源安全和信息管理安全。信息系统的安全性是采用 4A 的完善程度来衡量的，分别为用户身份验证（Authentication）、授权（Authorization）、审计（Accountability）和保证（Assurance）。对用户身份的验证，是指在用户获取信息、访问系统资源之前对其身份进行确认和验证，以保证用户自身的合法性；针对不同的用户进行授权，可使用户能够以合适的权限合法地访问各种不同的信息及系统资源；审计是对各种安全性事件的检查、跟踪和记录，它提供了信息系统安全事件的证明和根据；保证的作用在于确保系统的安全策略以及信息被准确、完整地理解和解释，在意外故障、自然灾害中信息不被破坏与丢失。任何未经授权的访问或故意侵入系统，窃取、篡改和破坏系统资源，都将会削弱、破坏信息系统的处理能力，侵犯个人隐私、危及企事业单位利益甚至泄露国家的安全机密。

在当今的信息社会中，信息、网络、计算机三者相互渗透、相互依赖、相互制约，它们已经成为了不可分割的一个整体。信息的采集、加工、存储是以计算机为载体的，而信息的存储、传输、处理、发布则是依赖计算机网络。由于本书定位于讲授计算机基础知识，面向本科教育，所以我们所讲的信息安全主要是指计算机网络安全，二者没有加以严格区别。计算机网络安全是对在分布式的网络环境中进行传输、存储、处理的信息提供安全保护，防止信息被窃取、篡改及非法操作。计算机网络是在 7 层协议共同作用下完成工作的，从安全的角度看各层都能提供一定的

安全手段，但在不同的层次上其提供的安全措施又不相同。如在网络层可使用防火墙技术，而在数据链路层，点对点的通信是采用加密和解密技术。从另一个角度看，计算机网络安全是计算机安全在网络环境下的扩展和延伸。而所谓计算机安全，是指为数据（信息）处理系统而建立和采取的技术与安全管理措施，以保护计算机硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露。

由于信息是在开放式的网络环境中处理的，其不安全因素相应地会增多。网络安全比独立的计算机安全更加困难和复杂，针对这一情况，国际标准化组织 ISO 已制定了《信息处理系统开放系统互连基本参考模型第 2 部分——安全系统结构》，即 ISO7498—2 标准。它确定了五大类信息安全服务，分别为数据保密（Data Confidentiality）、用户身份验证（Authentication）、数据完整性（Data Integrity）、不可否认性（Non-Repudiation）、访问控制（Access Control）。为了实现上述服务，需要有相应的安全机制作为保障，针对具体的技术手段，ISO7498—2 提供了八大安全机制，分别为数据加密、数字签名、访问控制、数据完整性机制、鉴别、通信业务填充机制、路由控制、公证机制。在本小节的第 3 部分中我们将会对数据的加密和数字签名作一简单介绍。

1. 信息安全标准

（1）我国的信息安全标准

1999 年我国正式颁布了《计算机信息系统安全保护等级划分准则》，即国标 GB17895—1999，并于 2001 年 1 月 1 日起实施。该准则将网络信息系统安全分为 5 个等级：自主保护、系统审计保护、安全标记保护、结构化保护和访问验证保护。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等，这些指标涵盖了不同级别的安全要求。

（2）TCSEC 标准

1985 年美国国防部公布了《可信任计算机标准评估准则 TCSEC，Trusted Computer System Evaluation Criteria》，TCSEC 最初主要作为军方标准使用，1987 年以后延伸到了民用企业领域。TCSEC 将信息安全分为 4 个方面：安全政策、可说明性、安全保障和文档，将计算机系统的可信程度划分为 7 个安全级别，从低到高依次为 D1、C1、C2、B1、B2、B3 和 A1 级。

（3）ITSEC 准则

欧洲信息技术安全评估规则 ITSEC1.2（Information Technology Security Evaluation Criteria）是由欧洲委员会于 1991 年在英、法、德、荷四国研究成果的基础上提出的。ITSEC 以超越 TCSEC 为目的，首次提出信息安全的保密性、完整性、可用性概念，把可信计算的概念提高到可信信息技术的高度。与 TCSEC 不同，ITSEC 并不把保密措施直接与计算机功能相联系，而是只叙述技术安全的要求，把保密作为安全增强功能。此外，TCSEC 把信息的保密作为安全的重点，而 ITSEC 则把信息的完整性、可用性与保密性作为同等重要的因素。ITSEC 定义了从 E0 到 E6 的 7 个安全等级。

（4）信息技术安全评价通用准则（CC）

为适应全球 IT 市场、推动全球信息化发展，国际标准化组织（ISO）从 1990 年开始着手编写国际通用信息安全标准评估准则。在 TCSEC 的基础上，经美国、加拿大、英国、法国、德国和荷兰等国家的共同努力，1996 年公布了具有统一标准、能被广泛接收的信息技术安全通用准则（Common Criteria，CC）。1999 年 12 月 ISO 正式将 CC2.0 接纳为国际标准 ISO15408。CC 是目前最全面的信息技术安全评估准则。CC 参照了 ITSEC 的主要特征，将功能需求分为 11 类 63 族，将保障分为 7 类 29 族。

实际中单靠技术来解决信息安全问题是不现实的，因为信息安全不仅仅是一种技术问题，它更是相关业务和管理的问题，实践证明仅靠技术解决不了安全问题，因此还必须有相关的信息安全管理国际标准。

（5）信息安全管理国际标准

1993 年 1 月，英国标准协会（British standards institution，BSI）成立了信息安全行业工作小组。1995 年 2 月，英国标准协会制定的信息安全管理体系标准 BS7799—1 发布。BS7799—1 对信息安全的控制范围、安全准则、安全管理等要素做出了规范性的表述。随后，ISO（国际标准化组织）和 IEC（国际电工委员会）成立了一个联合技术委员会 ISO/IEC JTC 1。该委员会以 BS7799—1 为蓝本，并对 BS 7799—1 做了 23 处修改后，制定了信息安全的国际标准 ISO/IEC 17799 草案。2000 年 12 月，国际标准 ISO/IEC 17799 正式出版。它旨在帮助各种类型和规模的组织实施并运行有效的信息安全管理体系，从而增强企业识别、防止、减少和控制组织信息安全风险的能力。ISO/IEC 17799 标准的内容涉及 10 个领域，36 个管理目标和 127 个控制措施。

2. 计算机病毒及其防治

《中华人民共和国计算机信息系统安全保护条例》中明确指出："计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码"。通常情况下我们可以这样来理解：计算机病毒是一段人为编制的、寄生于计算机合法程序或系统文件中的、可自我执行、具有传染性、以自我表现或破坏计算机系统正常工作为目的的程序，其工作过程由引导、传染和表现（攻击）三个阶段组成。计算机病毒的主要来源有这么几个方面：计算机专业人员或业余爱好者为了显示个人的编程技巧或出于恶作剧心理制造出来的病毒；软件开发者为了惩罚盗版者，在自己的软件中隐藏着病毒程序；出于研究目的而编写的程序却产生了意外的结果；以攻击和破坏为目的而专门编制的病毒。最早被记录在案的病毒之一是 1983 年由美国南加州大学学生 Fred Cohen 编写的，当该程序安装在硬盘上后，就可以对自身进行无限制地复制扩展，使计算机遭到"自我破坏"。随后，其他病毒也相继出现，如 1987 年非常流行的 Pakistani Brain 和 Lehigh 病毒，之后，病毒开始在全世界计算机业内大肆流行，直至今日。在 2000 年 12 月召开的亚洲计算机反病毒大会上公布的数据，病毒种类已达 55000 种。

当计算机传染上病毒后，人们一般不容易马上发现它，计算机仍能"正常"工作，这时我们会观察到计算机的一些反常现象，根据计算机表现出来的症状进一步来判断系统是否可能染上病毒。下面给出一些具体的症状：

- 屏幕上出现异常，如小球飞来飞去、彩块变幻、区域闪烁等；
- 执行文件无理由加长（尤其是随时间不断变长）；文件夹/目录中多了一些奇怪或重复的文件；原来可以执行的文件无故不能执行了或者突然消失了；
- 计算机执行速度越来越慢；系统空间越来越少；
- 系统出现经常性的"死机"或启动异常；
- 网络速度变慢或者出现一些莫名奇妙的网络连接；
- 电子信箱中出现来路不明的邮件等。

计算机出现了异常症状后，不用担心更不要惊慌，我们可根据经验和计算机专业知识来进行判断分析该现象是否是由病毒造成的，如果是病毒造成的，要进一步判断是什么类型的病毒？该病毒的工作机制是什么？这些都需要有一定的了解，也为后续的病毒清除工作做好了准备。下面我们就对病毒的分类，计算机病毒的清除以及如何预防病毒一一介绍。

（1）计算机病毒的分类

究竟世界上有多少种计算机病毒，答案肯定是未知的，然而我们可以对计算机病毒的种类加以区分。目前针对计算机病毒的分类方法有很多，有基于技术的，基于传染对象的，基于破坏程度的，基于入侵方式的。下面我们就根据病毒对传染对象的不同加入区分。

引导型病毒：引导型病毒将自身或自身的一部分隐藏在系统的引导扇区中，系统一旦启动病毒就驻留在内存中，修改引导程序后，再去引导系统，比如 Pakistani Brain 病毒就是将原始引导信息移动到磁盘的其他部分，然后将自己复制到引导扇区中。引导型病毒的一个重要特点就是对软盘和硬盘的引导扇区进行攻击。我们都知道引导扇区一般是磁盘上 0 柱 0 面的第一个扇区，对于装载操作系统具有关键性的作用，该病毒感染的主要方式就是计算机通过已被感染的引导盘引导时发生的。在 MS-DOS 时代典型的引导型病毒有 Pakistani Brain、大麻病毒、小球病毒等。

文件型病毒：文件型病毒是以感染可执行文件（.exe，.com，.bat 等）而著称的病毒。这种病毒把可执行文件作为病毒传播媒体，当用户执行带病毒的文件时，病毒就获得了对计算机的控制权，开始实施破坏活动。曾喧嚣一时的 CIH 病毒就是一种文件型病毒。

宏病毒：宏病毒是一种寄存于文档或模板宏中的计算机病毒。它是制作者针对软件（例如 Word、Excel 等）本身所提供的宏能力而设计编写的。用户一旦打开这样的文档，宏病毒就会被激活，并驻留在 Normal 模板中，在用户使用期间，所有自动保存的文档都会被“感染”，网络上的其他计算机用户如果打开了这样的文件，宏病毒还会自动转移到其他计算机上。下面我们以 Word 中的宏病毒感染文件为例，对宏病毒的工作机制作一介绍。

Word 的工作模式是当载入文档时，就先执行起始的宏，接着载入相应文档的内容，这个创意本来很好，因为随着文档内容的不同 Word 需要用不同的宏工作。可是事实上，很少有人会对宏产生兴趣，因为宏的编写相当于学习一套程序语言，尽管它的语法被编写得很简单，可是大多数的人，一方面不知情不了解，另一方面虽知如此，却宁愿多花几秒重复几个动作。因此，Word 便为大众事先定义一个共用的范本文档（Normal.dot），里面包含了基本的宏。只要启动 Word，就会自动运行 Normal.dot 文件。类似地电子表格软件 Excel 支持宏，但它的范本文件是 Personal.xls。然而这样做，也等于是为宏病毒大开方便之门，只要编写了有问题的宏，再去感染这个共用范本（Normal.dot 或 Personal.xls），那么只要执行 Word 或 Excel，这个受感染的共用范本即被载入，计算机病毒便随之传播到之后所编辑的文档中去。我们都知道编写宏病毒所使用的 Word Basic 语言提供了许多系统低层调用，如直接使用 DOS 系统命令，调用 Windows API，调用.dde、dll 等。这些操作均可能对系统造成直接威胁，而 Word 在指令安全性、完整性上检测能力很弱，破坏系统的指令很容易被执行。在今天的网络社会中 Word 文档是交流最广泛的文件类型之一，由此而产生的危害性相当严重。

变体病毒：这是一类高级的文件型病毒，其特点是每次进行传染时都会改变病毒程序代码的特征，以防止杀毒软件的追杀。此类病毒的算法比一般病毒复杂，杀毒软件有时也检测不到。

除上述这些病毒外，在网路上还有其他一些毁坏性严重的代码，如逻辑炸弹、特洛伊木马和蠕虫等，它们会窃取计算机系统资源或损坏数据，从技术角度看它们不能归类为病毒，属于恶意软件，因为它们并不复制自己，但它们对用户来讲仍然是高危险的东西。

（2）计算机病毒的检测与分析

计算机病毒的检测主要有比较法、扫描法、计算机病毒特征字的识别法和分析法。在这里我们只介绍分析法，计算机病毒的分析包括行为分析和代码分析。行为分析主要是指对计算机病毒

在系统中的行为的分析和记录。代码分析主要是指通过反汇编病毒文件得到源代码以确定病毒行为的原因和感染文件的细节等。相对来讲，行为分析比较容易，入门门槛低，结果也相对直观准确。代码分析比较困难，需要有扎实的计算机系统低层知识和编程知识，但可以全面深入地了解病毒特性。在对病毒行为分析时，常常会涉及以下几个方面：

- 查看文件的基本信息及预处理：就像医生看病需要事先知道病人的年龄、性别等基本信息一样，对于病毒文件的分析处理也要首先知道文件的基本信息，如文件名、扩展名和文件的大小等。这些信息在 Windows 环境中可以通过查看文件“属性”来获取。但要进行病毒分析时，还需要至少确定文件是否被加壳、什么类型壳和是否为捆绑文件等，这时常常需要借助于专用工具了，比如侦壳工具 PEiD v0.93，文件编辑工具 UltraEdit-32、WinHex，跟踪工具 OllyDbg。

- 记录生成文件和修改注册表行为：行为分析的主要目的就是在于记录文件在系统中的动作，比如生成文件，改动注册表项目等。一些注册表监视以及安装记录类软件可以忠实地记录下某个软件或者文件在系统中运行的结果。注册表快照类软件的工作原理就是利用分别记录软件安装、运行前后的文件、注册表等的变化，然后通过运行目标病毒文件，记录其所有行为，对比系统变化部分，来达到分析目的。注册表快照类软件是我们行为分析的主要工具，常用的有 InstallWatch Pro、RegSnap、RegShot 等。

- 综合分析其他信息形成报告：快照运行的过程就是病毒程序运行的过程，在这个过程中系统的各种异常现象就是病毒发作的现象。这个时候要分析、保存各种截图和其他症状信息，其实无论是行为分析还是代码分析，更多地是需要分析员的经验，因为现在的病毒代码中已经运用了大量的迷惑性手段。

（3）计算机病毒的清除

计算机系统在检测出感染了病毒或确定了病毒种类之后，就要设法去消除病毒。消除病毒的方法较多，总体上可分为人工消除和自动消除两种方法。

- 人工消除病毒法：人工消毒法是借助工具软件对病毒进行手工清除。操作时使用工具软件打开被感染的文件，从中找到并清除病毒代码，使之复原。手工消毒操作复杂、速度慢、风险大，要求操作者具有熟练的操作技能和丰富的计算机知识。这种方法是专业防病毒研究人员用于消除新病毒时采用的，普通用户不宜采取这种方法。下面我们以处理引导型病毒为例来介绍一下手动消除引导型病毒的过程。引导型病毒的一般清理方法是格式化磁盘，但这种方法的缺点是，当用户格式化磁盘后，不但病毒被杀掉了，而且磁盘上有用的其他数据也被清除掉了。为了能保留有用的数据，我们采取不用格式化磁盘的方法来清除病毒，不过还需要一些有关硬磁盘的相关知识。

与引导型病毒有关的磁盘扇区大概有下面 3 个部分。

① 第一部分是硬盘的物理第一扇区，即 0 柱面、0 磁头和 1 扇区。这个扇区称为“硬盘主引导扇区”，上面包括两个独立的内容，第一部分是开机后硬盘上所有可执行代码中最先执行的部分，即在该扇区的前半部分内容，称其为“主引导记录”（Master Boot Record，MBR）。

② 第二部分不是程序，而是非执行的数据，记录硬盘分区的信息，即人们常说的“硬盘分区表”（Partition Table）。

③ 第三部分是硬磁盘活动分区中的第一个扇区。一般位于 0 柱面、1 磁头和 1 扇区，这个扇区称为“活动分区的引导记录”，它是开机后继 MBR 运行后的第二段代码的所在之处。其他分区也具有一个引导记录（BOOT），但是其中的代码不会被执行。

清除病毒时先用无病毒的 DOS 引导软盘启动计算机，然后可按下面的步骤，执行不同的工作

任务达到完成清除病毒的工作。

① “Fdisk/MBR”用于重写一个无毒的 NBR。

② “Fdisk”用于读取或重写一个无毒的 MBR。

③ “Format C/S”或“SYSC;”会重写一个无毒的“活动分区的引导记录”。

针对不同类型的病毒，需要采用不同的清除手段，还需要大量计算机专业知识，这里不再赘述。

- 自动消除病毒法：自动消除病毒法是使用杀毒软件来清除计算机病毒。用杀毒软件进行杀毒，操作简单，用户只要按照菜单提示和联机帮助就可实施操作。自动消除病毒具有效率高、风险小的特点，是一般用户常使用的方法。常见杀毒软件见第 8 章中第 6 节。

（4）计算机病毒的预防

计算机病毒的防治工作应从日常管理和技术两个方面入手，应做好以下几个方面的工作。

- 在思想上要树立预防为主的思想，以“预防为主，防治结合”的思想为指导，制定出切实可行的管理措施和技术措施方案，并在日常工作中坚持执行。
- 在日常工作中，尊重他人，使用正版软件，不随意复制、传播各种非法软件。
- 对服务器及其他重要设备的使用要实行严格的安全操作规程，明确各级权限各负其责。
- 定期和不定期地对系统中的重要数据进行备份。随时注意观察计算机及网络系统的运行情况，发现异常及时进行处理。在工作中逐步养成良好的操作习惯。
- 不要将自己的邮件地址放在网络上，以防止类似 SirCam 病毒的窃取，带来潜在的隐患。不要轻易打开陌生人传来的页面链接，防止“W32 Leave.Worm”等病毒陷阱的攻击。
- 在技术层次上要安装、设置防火墙，对网络内部实施安全保护；安装实时监测的杀毒软件，定期升级软件版本，打开杀毒软件提供的各种保护服务；禁用 Windows Scripting Host，以防求职信（Klez）及其变种病毒的攻击；使用即时聊天软件、浏览各种非官方网站时，不要轻易打开页面及网页中的各种元素，以防感染各种木马病毒。

3. 信息安全技术

将人类的生态环境与计算机网络环境进行类比，我们就可知道计算机网络上的信息同样会受到各种各样的威胁，包括网络病毒的感染、恶意软件的入侵、黑客的攻击等，给网络信息系统的安全性带来了极大的安全隐患。俗话讲“兵来将挡、水来土掩”，有矛就有盾。随着信息科学和信息技术的发展和进步，针对信息安全问题人们已经进行了多年的研究并取得了许多令人鼓舞的成果，确立了独立的学科体系，在有的大学本科教育阶段还设置了信息安全专业。保障网络信息系统安全的方法很多，涉及许多信息安全技术，然而其理论基础就是密码学。下面我们就以密码学理论为依据，对信息安全中的核心技术数据加密和数字签名作一介绍。

（1）数据加密

数据加密技术是一种用于信息保密的技术，是信息安全领域中的核心技术之一，数据加密技术通常直接用于对数据的存储及传输过程当中，信息通过数据加密技术的处理能有效地防止被非法用户使用。一个加密系统是由明文、密文、加密算法和密钥组成的。加密是发送方将原文信息即明文进行伪装处理，经加密后的信息我们称为密文，加密时使用的信息变换规则称为密码算法，密码算法又分为加密算法和解密算法，密码算法通常是一些数学公式、函数或程序，而密钥是由数字、字母或特殊字符组成的一个字符串，用它来控制数据加密、解密过程。通过加密密钥将数据加密后发送出去，接收方在收到密文后，再用解密算法和解密密钥将密文还原回明文。在传输的过程中，即使密文被非法分子偷窃获得，也是一堆杂乱无章的数据，无法识别其真正含义，从

而起到数据保密作用，工作过程如图 1-1 所示。

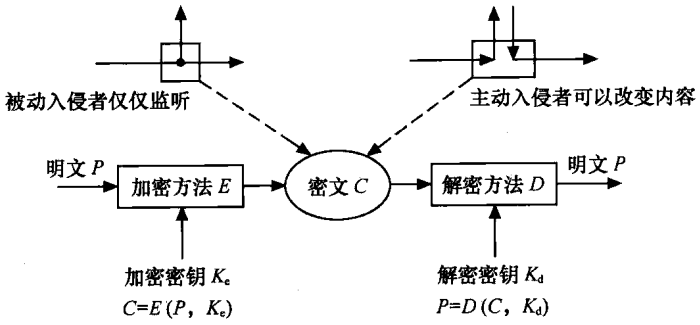


图 1-1　数据加密的基本过程

图 1-1 中，明文 P 由一个加密算法 $E(P, K_e)$变换成密文 C，这个函数（加密算法）以密钥 K_e 和明文 P 为参数。解密时用解密算法 $D(C, K_d)$对密文 C 进行变换，还原成明文 P，即 $P=D(C, K_d)$，也就是 $P=D(E(P, K_e), K_d)$。如果 $K_e=K_d$，称为对称加密体制，如 1977 年美国政府颁布的数据加密标准（Data Encryption Standard，DES）。否则为非对称加密体制，如公钥密码体制的代表加密算法（Rivest-Shamir-Adleman，RSA）。在加密过程中所有加密算法的安全性都依赖密钥的安全性，而不是看算法细节上的安全性，这就意味着算法是可以公开的，也可以被分析，现实中大量使用相同算法的产品比比皆是。

基于密钥的算法通常有两类：对称算法和公用密钥算法。对称算法有时又叫传统密码算法，就是加密密匙能够从解密密钥中推导出来，反过来也成立。在大多数对称算法中，加/解密密钥是相同的。这些算法也叫秘密密钥算法或单密钥算法。它要求发送者和接收者在安全通信之前，先商定一个密钥。对称算法的安全性依赖于密钥，泄露密钥就意味着任何人都能对消息进行加解密。也就是说只要通信需要保密，密钥就必须保密。对称算法的加密和解密也可表示为

$$E_K(P)=C$$

$$D_K(C)=P$$

其中，P 是明文，C 是密文，K 是密钥，E 是加密算法，D 是解密算法。

公用密钥算法（Public-Key Aalgorithm）也叫非对称算法，它是这样设计的：用于加密的密钥不同于用作解密的密钥，而且解密密钥不能根据加密密钥计算出来。之所以叫公用密钥算法，是因为加密密钥能够公开，即陌生者能用加密密钥加密信息，但只有用相应的解密密钥才能解密信息。在一些系统中，加密密钥叫做公用密钥，解密密钥叫私人密钥。私人密钥有时也叫秘密密钥。使用公用密钥算法加密，与使用对称算法即通过单密钥加密不同，它使用相互关联的一对密钥，一个是公用密钥，任何人都可以知道，另一个是私人密钥，只有拥有该对密钥的人才知道。如果有人将信息发送给某个人，发送方就用接收方的公用密钥对信息进行过加密，当接收方收到信息后，他就可以用其私人密钥对信息进行解密，而且只有接收方持有的私人密钥才可以解密。这种加密方式的好处显而易见。私人密钥只有一个人持有，也就更加容易进行保密，因为不需要再在网络上传送私人密钥，也就不用担心别人在认证会话初期截获密钥。公用/私人密钥技术具有以下几个特点：

- 公用密钥和私人密钥是两个相互关联的密钥；
- 公用密钥加密的文件只有私人密钥才能解开；
- 私人密钥加密的文件只有公用密钥才能解开。