普通高等学校计算机科学与技术专业新编系列教材

Introduction to Information Security

信息安全概论

钟 诚 赵跃华 主编

```
#include <stdio.h>
#include <stdio.h>
void main()
void main()
{
   void swap(int *ptr1,int *ptr2);
   void swap(int *ptr1,int *ptr2);
  int x,y,*ptr1,*ptr2;
  int x,y,*ptr1,*ptr2;
  printf("input x,y:");scanf("%d,%d",&x
  printf("input x,y:");scanf("%d,%d",&x
  printf("%d\t%d\n",x,y);ptr1=&x;ptr2=
  printf("%d\t%d\n",x,y);ptr1=&x;ptr2=
  if(x<y)
  if(x<y)
  swap(ptr1,ptr2);
  swap(ptr1,ptr2);
  printf("%d\t%d\n",x,y);
  printf("%d\t%d\n",x,y);
}
void swap(int *ptr1,int *ptr2)
void swap(int *ptr1,int *ptr2)
```

武汉理工大学出版社
Wuhan University of Technology Press

普通高等学校计算机科学与技术专业新编系列教材

Introduction to Information Security

信息安全概论

钟　诚　赵跃华　主编

钟　诚　赵跃华　杨铭熙
叶　震　陆向艳　宋建华　编著

武汉理工大学出版社
Wuhan University of Technology Press

内 容 提 要

本书介绍信息安全的基本概念、方法和技术。主要内容包括信息安全的基本知识、信息安全模型、当代主流的密码技术、数据库加密和安全访问机制、数字签名和信息认证技术、计算机网络操作系统安全、安全电子商务系统、网络入侵检测方法与技术等。

本书取材新颖、全面，内容先进、科学、实用，编排合理，少而精，理论与实践相结合、可读性强，例题和习题配置适当。

本书可作为计算机科学技术、电子信息工程、通信工程、自动化和管理信息系统等信息类专业的教材，也可供从事信息安全工作的管理干部和工程技术人员参考。

图书在版编目(CIP)数据

信息安全概论/钟诚，赵跃华主编. —武汉：武汉理工大学出版社，2003.8
普通高等学校计算机科学与技术专业(本科)新编系列教材
ISBN 7-5629-1952-6

Ⅰ.信… Ⅱ.①钟… ②赵… Ⅲ.信息系统-安全技术-高等学校-教材
Ⅳ.TP309.08

中国版本图书馆 CIP 数据核字(2002)第 106862 号

出版发行：武汉理工大学出版社(武汉市武昌珞狮路 122 号 邮编：430070)
http://cbs.whut.edu.cn
E-mail:wutp02@163.com wutp@public.wh.hb.cn
经 销 者：各地新华书店
印 刷 者：湖北省荆州市翔羚印刷实业公司
开 本：787×960 1/16
印 张：16.375
字 数：320 千字
版 次：2003 年 8 月第 1 版
印 次：2003 年 8 月第 1 次印刷
印 数：1～5000 册
定 价：22.00 元

普 通 高 等 学 校
计算机科学与技术专业新编系列教材
编 审 委 员 会

出版说明

当今世界已经跨入了信息时代，计算机科学与技术正在迅猛发展。尤其是以计算机为核心的信息技术正在改变整个社会的生产方式、生活方式和学习方式，推动整个人类社会进入信息化社会。为了顺应时代潮流，适应计算机专业调整及深化教学改革的要求，充分考虑到不同层次高校的教学现状，满足广大高校的教学需求，武汉理工大学出版社经过广泛调研，与国内近30所高等院校的计算机专家进行探讨，决定组织编写“普通高等学校计算机科学与技术专业新编系列教材”。

我们在组织编写新编本套系列教材时，**以培养现代化高级人才为重任，以提高学生综合素质、培养学生应用能力和创新能力为目的，以面向现代化、面向世界、面向未来为准绳，注重系列教材的特色和实用性，反映最新的教学与科研成果，体现本专业的时代特征。**同时，面对教育改革的需要、人才的需要和社会的需要，在编写本教材时，借鉴、学习国外一流大学的先进教学体系，结合国内的实际需要，吸取具有先进性、实用性和权威性的国外教材的精华，以更好地促进国内教材改革顺利进行。从时代和国际竞争要求的高度来思考，为打造一套高起点、高水平、高质量的系列教材而努力。

本套教材具有以下特色：

与时俱进，内容科学先进——充分体现计算机学科知识更新快的特点，及时更新知识，确保教材处于学科前沿，以拓宽学生知识面，培养学生的创新能力。

紧跟教学改革步伐，体现教学改革的阶段性成果——符合全国高校计算机专业教学指导委员会、中国计算机学会教育委员会制订的“计算机学科教学计划2000”的内容要求。

实现立体化出版，适应教育方式的变革——本套教材努力使用和推广现代化的教学手段，凡有条件的课程都准备组织编写、制作和出版配合教材使用的实验、习题、课件、电子教案及相应的程序设计素材库。

本套教材首批25种预定在2003年秋季全部出齐。我们的编审者、出版者决不敢稍有懈怠，一定高度重视，兢兢业业，按最高的质量标准工作。教材建设是我们共同的事业和追求，也是我们共同的责任和义务，我们诚恳地希望大家积极选用本套教材，并在使用过程中给我们多提意见和建议，以便我们不断修订、完善全套教材。

武汉理工大学出版社

2002年10月

前　言

21世纪是信息的社会，是知识经济的时代。在这个时代里，信息与我们息息相关。信息技术在国民经济建设、社会发展、国防、科学研究、教育等领域的作用日益重要。随着计算机互联网络的迅速发展和广泛应用，它打破了传统的时间和空间的局限性，使得人们获取信息更快捷、更方便、更容易和更有效，大大地改变了人们的工作方式和生活方式，促进了经济和社会的发展，提高了人们的工作水平和生活质量。由于计算机互联网络的国际化、社会化、开放化、个性化的特点，使得它在向人们提供信息共享、资源共享和技术共享的同时，也带来了不安全的隐患。信息安全问题如果不解决的话，它不但威胁到国家的安全，阻碍电子政务、电子商务、网络银行、网络远程教育、网络远程诊断等的正常开展，而且也使得个人的隐私信息得不到保障。信息安全是构建整个社会信息化的根本保证。信息安全不但可以确保信息革命带来的高效率、高效益，而且它是对抗信息霸权主义、抵御信息侵略的重要屏障。信息安全保障能力是21世纪综合国力、国际竞争力的重要组成部分，它已成为影响国家全面发展和长远利益的重大关键问题。

信息安全是近20年来特别是近几年来迅速发展起来的新兴学科，由于其战略地位十分重要，各国都给予极大的关注和投入。我国政府已经充分意识到信息安全的极端重要性，党和国家领导人对此多次作出重要的指示。国家“973”计划、国家“863”计划和国家自然科学基金将信息安全理论与技术列为“十五”期间我国高新技术的重大研究课题。在信息安全教育方面，“信息安全概论”课程已列入国家教育部制订的计算机、电子信息、通信、管理信息系统等信息类专业的教学计划中，而且我国已有部分高校开设了本科信息安全专业。

信息安全所涉及的内容相当广泛，本教材将有侧重地对有关问题予以介绍。全书共8章。第1章首先阐述信息安全的重要意义，指出学习和研究信息安全的必要性和紧迫性，然后从信息的存储到信息的传输和接收过程中所涉及的安全问题进行了概括性的介绍。第2章介绍信息安全的基本概念和技术，包括实体安全、运行安全、信息保护安全、安全管理和信息安全标准等内容。第3章比较详细地讨论了信息安全的模型，重点介绍自主型访问控制模型和强制型访问控制模型。第4章介绍信息安全的基础——密码技术，选择有代表性的对称密码系统DES、公开密钥密码系统RSA、椭圆曲线密码系统ECC和背包密码系统进行介绍，并简介了密钥管理和密钥恢复技术。第5章专门阐述数据库加密与

安全的有关问题，主要介绍数据库加密的特点、方式和方法，数据库的安全访问模型和授权系统。第 6 章讨论确保信息安全传输所涉及的数字签名技术、身份认证和信息认证技术。第 7 章介绍计算机网络系统安全的有关问题，包括计算机病毒及其防治技术、防火墙技术、操作系统安全技术、电子邮件安全系统以及电子商务系统的安全协议。第 8 章介绍目前信息安全研究热点之一的入侵检测技术，较详细地介绍入侵检测系统的定义、模型和分类，并重点讨论若干典型的入侵检测方法与技术。

信息安全涉及近世代数、数论、概率与统计、运筹学、数理逻辑、形式语义学、心理学、管理学、法律、信息论、编码理论、计算复杂性、程序设计、计算机密码学、计算机体系结构、算法设计与分析、计算机网络、数据库系统、操作系统、人工智能等，是一门综合性的交叉学科。因此，建议将本课程安排在大学三年级的下学期或者四年级的上学期讲授。

本书是在作者授课讲义的基础上，参考国内外有关文献编写而成。本书由钟诚、赵跃华主编。钟诚编写第 1 和 8 章，赵跃华编写第 2 和 3 章，陆向艳编写第 4 章，宋建华编写第 5 章，叶震编写第 6 章，杨铭熙编写第 7 章。全书由钟诚统稿、润色和校订。

本书的面世，除了编著者的努力之外，许多人在本书的构思、讨论、写作、编排、校对、印刷和出版过程中做出了积极的贡献；此外，本书直接或者间接引用了专家、学者的有关文献，我们深表感谢。同时，我们感谢我们的家人对本书写作的充分理解和大力支持；感谢鲁晓明、吕皖丽和冯志新在本书部分资料收集和部分文档整理方面的辛勤劳动；感谢武汉理工大学出版社为本书提供了出版机会，感谢责任编辑徐秋林先生和孙成林、田道全、段超先生及其他编排人员为本书规划、编辑、出版、发行所做出的卓有成效的工作。

我们希望本书的出版能为我国计算机和信息安全教育事业的发展起到添砖加瓦的作用。由于编者学术水平有限，加之编写时间较紧，书中定有错误和不妥之处，敬请专家、学者和读者批评、指正。

编 者

2003 年 1 月

目　录

1 引　论

本章提要

我们已经迈入21世纪的知识经济时代。在这个新时代里，信息与我们息息相关。信息对于巩固国防、确保国家安全，促进经济发展、推动社会进步、提高人们的工作水平和生活质量等具有重大的作用。确保信息安全至关重要，没有信息的安全就谈不上信息的应用。学习、研究和应用信息安全的知识、理论、方法和技术是21世纪高等教育的一个重要方面。本章首先阐述学习、研究信息安全的必要性和紧迫性，指出信息安全是国家安全的重要基础；然后，从教育、管理和技术等方面介绍信息安全的有关内容；最后从学科的角度列出了与信息安全有关的基础课程。

1.1 信息安全是国家安全的重要基础

21世纪是信息的社会。信息在国民经济建设、社会发展、国防和科学研究等领域的作用日益重要。随着由计算机技术与通信技术相结合而诞生的计算机互联网络的迅速发展和广泛应用，它打破了传统的时间和空间的局限性，极大地改变了人们的工作方式和生活方式，促进了经济和社会的发展，提高了人们的工作水平和生活质量。

科学技术是第一生产力。世界范围内的信息革命则激发了人类历史上最活跃的生产力。计算机网络和通信是促进信息化社会发展的最活跃的因素。然而，任何事物的发展都具有二重性。由于计算机互联网络的国际化、社会化、开放化、个性化的特点，使得它在向人们提供信息共享、资源共享和技术共享的同时，也带来了不安全的隐患。信息安全问题已威胁到国家的政治、经济和国防等

领域。因此，很早就有人提出了“信息战”的概念并将信息武器列为继原子武器、生物武器和化学武器之后的第四大武器。信息的泄漏、篡改、假冒和重传，黑客入侵，非法访问，计算机犯罪，计算机病毒传播等等对信息网络已构成重大威胁。如果这些问题不解决，国家安全会受到威胁，电子政务、电子商务、网络银行、网络科研、远程教育、远程医疗等等都将无法正常开展起来，个人的隐私信息也得不到保障。

信息不仅是一种十分重要的公用资源和商业资源，信息更是一种重要的战略资源。国际上围绕着信息的获取、使用和控制的斗争已经展开并正在逐步引向深入。美国正在利用其经济和军事优势下的信息技术优势，极力推行信息霸权主义。一方面，美国不断地向其他国家大肆倾销其信息产品，掠取别国财富；另一方面，在其出口的信息系统中植入“陷阱”和“后门”，以控制、破坏和截取别国的秘密信息。美国著名的未来学家阿尔温·托夫勒声称：“计算机网络的建立与普及将彻底改变人类生存及生活的模式，而控制与掌握网络的人就是人类未来命运的主宰。谁掌握了信息、控制了网络，谁就将拥有整个世界。”美国前总统克林顿坦言：“今后的时代，控制世界的国家将不再是依靠军事实力，而是信息能力走在前面的国家。”同时，美国正在积极准备信息战。早在 1995 年 10 月，美国就组建了世界上第一支信息战分队。目前，美国已建立了 20 多个高层次的信息战机构。信息战的核心是获取“信息控制权”。在 20 世纪 90 年代的海湾战争中，美国将带有计算机病毒的微机芯片装入伊拉克从法国购买的用于防空系统的新型打印机中，从而达到了使伊拉克军事指挥中心计算机失灵的目的，充分显示了现代高技术条件下“信息控制权”的关键作用。20 世纪 90 年代中后期的科索沃战争也是美国实施信息战的一次试验，再次证明信息网络已成为高技术战争的十分重要的对抗领域。在 2001 年的“9 · 11”事件后，美国这个超级大国更是大打信息战。信息战突破了传统的地缘概念，无法用领土、领空、领海来划分，信息战的另一特点是隐蔽，被称为“没有硝烟”的战争。

特别要指出的是，美国为了能达到称霸世界的目的，凭借其信息技术优势，通过提供出口信息安全产品来达到控制、获取别国秘密信息的目的。他们开始时先限制 40 位密钥长度以上的密码产品出口，然后同意具有密钥托管或密钥恢复功能的强密码出口，但是这些都是美国政府可以控制和解读的。更为严重的是在计算机芯片和操作系统中可能还会隐藏着尚未被人们发现的、危害性更大的“陷门”和“特洛伊木马”等安全陷阱。一旦发生重大国际冲突，那些隐藏的“特洛伊木马”可能在秘密指令下激活起来，破坏或篡改信息系统中的重要信息，或把这些重要信息秘密发送出去，从而达到制胜的目的。

信息资源的争夺和信息领域的斗争，使我们充分认识到在信息社会中只讲信息应用是不行的，必须同时考虑信息安全问题。信息安全是整个国家安全的

重要组成部分，它已成为影响国家全面发展和长远利益的重大关键问题。信息安全不但可以确保信息革命带来的高效率、高效益，而且它是对抗信息霸权主义、抵御信息侵略的重要屏障。信息安全保障能力是21世纪综合国力、国际竞争力的重要组成部分。

目前，我国信息与网络防御能力比较脆弱，形势逼人。许多重要的信息系统，基本上处于不设防状态，缺乏安全保障。一些重要的计算机信息系统，使用从国外引进的安全设备，无法保证其安全利用和有效监管。国内信息安全研究力量比较分散，已有的研究仅注重于封堵已发现的安全漏洞，无法从根本上解决国家信息安全问题。

信息安全是近20年来特别是近几年来迅速发展起来的新兴学科，由于其战略地位十分重要，各国都给予极大的关注和投入。我国信息安全研究这些年来取得了长足的进步，但是由于起步较晚、投入不足、研究力量分散，总体来说与发达国家相比存在着较大差距。信息安全体系结构和安全协议的研究更是薄弱环节。面对激烈的网络信息战的对抗和冲突，面对日益增强的计算能力和人类智慧，信息安全理论与技术面临着空前的挑战和机遇。我国政府已经充分意识到信息安全的极端重要性，党和国家领导人为此多次作出重要的指示。国家"973"计划、国家"863"计划和国家自然科学基金已将信息安全理论与技术列为"十五"期间我国高新技术的重大研究课题。我们必须在吸取国外信息安全的先进管理、理论和技术的基础上，奋发努力、勇于开拓、不断创新，独立自主地发展我国的信息安全技术。我们必须从国家和民族的最高利益出发，在国家主管部门统一组织下，发挥社会主义能够办大事的优势，发扬"两弹一星"精神，集中力量开展信息安全研究，特别地加强对信息安全理论、信息安全发展战略、安全操作系统和安全芯片、密码理论和技术、网络信息安全平台、信息安全检测和监控技术、入侵检测与反击技术、电磁泄漏技术以及病毒防治等方面的研究，确立自主的、创新的、整体的信息安全理论体系，构筑我国自主的网络信息安全系统。

1.2 信息安全的主要内容

随着全球信息化的飞速发展，我国大量建设的各种信息化系统也已成为国家关键基础设施，它们支持着电子政务、电子商务、电子金融、电子投票、网络通信、网络合作研究、网络教育、网络医疗和社会保障等方方面面。网络化、数字化的特点使得这些系统均与保密或敏感信息有关，运作方式有别于传统模式，所以这些设施的安全维护显得格外重要。要保证电子信息的安全性和有效性，除了需要根据知识经济的发展，制订出相适应的政策、法规和管理规范外，还需要通过信息安全技术来提供安全保障。信息安全是构建整个社会信息化的根本保

证。

考虑信息安全保障应当总体规划，不仅要在技术上统筹计划，并强调信息保障研究跨学科的性质；更重要的是加强信息安全教育与管理，强调系统规划和责任，重视对信息系统使用的法律与道德规范问题，将法律、法规和各种规章制度融合到信息安全解决方案之中。总之，信息安全保障和信息安全的本质在于思想观念上的主动防御而不是被动保护；信息安全保障涉及管理、制度、人员、法律和技术等方面。解决信息安全的基本策略是综合治理。

信息安全研究所涉及的内容相当广泛，包括信息人员的安全性，信息管理的安全性，信息设施的安全性，信息自身的保密性（保证信息不泄漏给未经授权的人），信息传输的完整性（防止信息被未经授权的篡改、插入、删除或重传），信息的不可否认性（保证发送和接受信息的双方不能事后否认他们自己所作的操作行为），信息的可控性（对信息和信息系统实施安全监控管理，防止非法用户利用信息和信息系统）和信息的可用性（保证信息和信息系统确实能为授权者所用，防止由于计算机病毒或其他人侵行为造成系统的拒绝服务）等等。本教材有侧重地对下列问题予以介绍：

(1)安全管理

信息最终是由人类控制与利用的。因此，确保信息安全的首要条件是对信息人员进行审查，加强对有关人员的信息安全教育，建立和完善各种信息安全的法律、法规和规章制度，严格按照法律、法规和规章制度来管理和使用信息。

(2)实体安全

实体安全就是保护计算机设备、网络以及其他设施免遭地震、水灾、火灾、有害气体和其他环境事故破坏的措施和过程。它包括三个方面：环境安全，指对计算机信息系统所在环境的安全保护；设备安全，指对计算机信息系统设备的安全保护，如设备的防盗和防毁，防止电磁信息泄漏，防止线路截获，抗电磁干扰以及电源保护等；介质安全，指对介质的安全保管（包括介质的防盗、防毁、防霉和防砸等），目的是保护存储在介质上的信息。

(3)运行安全

运行安全是信息安全的重要环节，是为保障系统功能的安全实现，提供风险分析、审计跟踪、备份与恢复和应急等一套安全措施来保护信息处理过程的安全。

所谓风险分析是指对计算机信息系统进行人工或自动的风险分析。在系统设计前和系统运行前首先进行风险分析，以便发现系统潜在的安全隐患；然后对系统进行动态分析，即在系统运行过程中测试、跟踪并记录相关的活动，目的在于发现系统运行期间的安全漏洞；最后是系统运行后的分析，并提供相应的系统脆弱性分析报告。

审计跟踪是指对计算机信息系统进行人工或自动的审计跟踪、保存审计记录和维护详尽的审计日记。其安全功能可归纳为三个方面：记录和跟踪各种系统状态的变化，实现对各种安全事故的定位，如监控和捕捉各种安全事件，保存、维护和管理审计日记等。

备份与恢复则是指对系统设备和系统数据的备份与恢复。可以使用多种介质（比如磁介质、纸介质、光盘、缩微胶卷等）备份和恢复系统的数据。它的安全功能包括提供场点内高速度、大容量自动的数据存储、备份和恢复，提供场点外的数据存储、备份和恢复，以及提供对系统设备的备份等。

所谓应急是指在紧急事件或安全事故发生时，保障计算机信息系统继续运行或紧急恢复的措施。应急的安全功能包括紧急事件或安全事故发生时的影响分析、应急计划的总体和详细设计、应急计划的测试与完善三个方面。

(4)安全计算机

数字化信息存储在计算机中并通过计算机网络传输。为了确保这些数字化信息的安全，首先要求存储和处理信息的计算机系统是安全的，包括安全芯片、容错计算机、安全存储介质等方面。容错计算机的基本特点是：电源稳定可靠、预知故障、保证数据的完整性、数据备份与恢复等。即使在某个可操作的子系统遭到破坏后，容错计算机能够继续正常地运行。也就是说，当出现操作错误和电源掉电等等之类的故障时，容错系统能够及时发现、及时补救，保护文件数据，恢复和维持其运行。容错系统由故障检测、故障隔离、运行恢复和动态冗余切换等特殊模块组成。

(5)安全操作系统

操作系统是计算机系统的核心，它管理和控制计算机系统的资源。虽然通常的操作系统（Unix 及其变种、Solaris、Linux、VAX/VMS、IBM MVS、IBM VM/370、Windows 等）都在一定程度上具有访问控制、安全内核和系统设计等安全功能。但是为了适应更高安全环境要求，有必要设计一些专用的安全操作系统。比较常用的安全操作系统有 Honeywell 公司的 SCOMP 系统、UCLA 安全 UNIX 操作系统、内核化的 VM/370 等。特别需要说明的是，从国家安全、军事和经济安全的角度考虑，完全有必要开发我国独立的、自主的安全操作系统。我们国家具有快速地集中全国人力、物力和财力办大事的无可比拟的优势，因此，我们确信通过继续发扬“两弹一星”精神，团结一致、奋发努力、勇于实践，完全有能力设计和开发出具有自主知识产权的先进的安全操作系统。

(6)密码技术

利用数学变换保护秘密信息是密码最原始、最基本的功能。密码作为运用于军事和政治斗争的一种技术，历史悠久，无论是在古希腊时代还是在现代都发挥了非常重要的作用。随着信息技术的发展，现代密码学不仅用于解决信息的