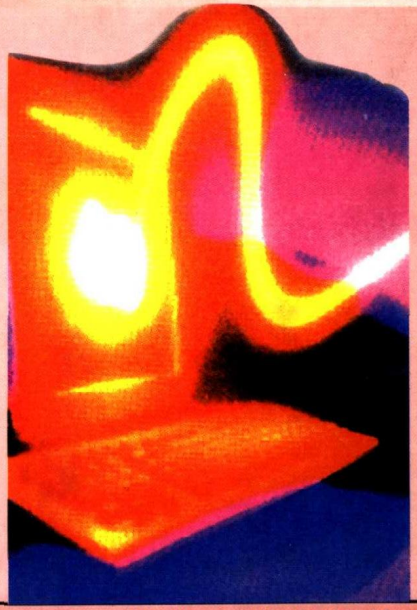
上海市计算机学会组织编写

《新编计算机与信息科学十万个为什么》
丛书编委会　编著

新编计算机与信息科学十万个为什么

12 计算机安全与保密



清华大学出版社
http://www.tup.tsinghua.edu.cn

新编计算机与信息科学十万个为什么

丛书编委会 编著

计算机与信息科学（新编）十万个为什么

上海市计算机学会组织编写

⑫ 计算机安全与保密

清华大学出版社
http://www.tup.tsinghua.edu.cn

(京)新登字 158 号

内 容 简 介

计算机安全是由计算机管理延伸出来的一门技术学科，它涉及对自然灾害的防护、环境安全、技术安全、政策法规、人事管理、道德教育等诸多方面。本书包括以下三部分：第一部分简要介绍有关计算机信息安全的法律法规和计算机安全技术；第二部分介绍密码学在计算机安全技术中的应用；第三部分介绍计算机病毒的概念和机理，以提高对计算机病毒的认识，并积极加以防范。

本书可供具有初中以上文化程度的计算机爱好者或非计算机专业的广大读者阅读。

书　名：新编计算机与信息科学十万个为什么 · 12 · 计算机安全与保密

作　者：《新编计算机与信息科学十万个为什么》丛书编委会

出版者：清华大学出版社（北京清华大学学研大厦，邮编 100084）

http:// www.tup.tsinghua.edu.cn

印刷者：世界知识印刷厂

发行者：新华书店总店北京发行所

开　本：787×1092 1/24　印张：10.75　字数：251 千字

版　次：2000 年 9 月 第 1 版　2000 年 9 月 第 1 次印刷

书　号：ISBN 7-302-03931-3/TP · 2299

印　数：0001～5000

定　价：200.00 元（全套）

《新编计算机与信息科学十万个为什么》

丛书编委会

《新编计算机与信息科学十万个为什么》

各篇、各专题编委

篇、专题名	主　编	副主编	主　审
引路篇	郁宝忠	王心园	吴洪来
综合应用技术篇	陈一民	高黎新	王心园
专业技术基础篇			
系统结构	孙德文	徐伟民	张吉锋
软件基础	吴洪来	徐国定	夏宽理
数据库与信息检索	陆　皓	周　宁	周广声
办公自动化与管理信息系统	何礼义	黄天敏	张吉锋
计算机网络与数据通信	方起兴	谢承德	张根度
		荆金华	俞嘉惠

篇、专题名	主　编	副主编	主　审
因特网、内联网和家庭网络	方起兴	谢承德	张根度
		荆金华	俞嘉惠
多媒体技术	施鹏飞	程耀华	郑衍衡
计算机辅助设计	宣国荣	李启炎	仲　毅
		彭澄廉	
人工智能	童　频	缪淮扣	朱关铭
计算机安全与保密	鲍振东	赵一鸣	覃　光

序

人类进入了信息时代。

随着以计算机和现代通信技术为核心的信息技术迅速发展和广泛应用，信息资源得到进一步开发和利用，大大推动了人类社会各个方面的发展，并对人们的工作、学习和生活产生了深刻的影响。

在当今世界，发达国家和新型工业化国家都在大力发展信息技术，竞相规划和建设本国的信息基础设施，加速信息化进程，力争在这场世纪之交的大竞争、大发展中立于不败之地。当前，我国也在大力发展信息技术，加强信息产业和信息基础设施的建设，以迎接信息时代对我们的挑战。

实现信息化，关键是人才。我们不但需要有一批熟悉信息系统与信息资源开发，致力于信息化建设的技术专家，更需要有一大批能掌握计算机与信息技术，会用并用好信息系统与信息资源的应用人才，还要在全社会普及计算机及信息知识，增强信息化意识，使人们学会并适应在信息社会环境中工作、学习和生活。

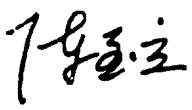
在科学技术普及的事业中，书籍有着极其重要的作用。书籍是人类进步的阶梯。一部好的科普丛书能启迪人们的心智，激发人们进一步学习科学技术的兴趣和奋发向上的精神。早在20世纪60年代，上海的科学家们就编写了一套《数、理、化、生十万个为什么》，对推动科学文化普及做出了有益的贡献。今天，上海市计算机学会继承和发扬这一优良传统，组织了100多位专家学者，通过调查研究，编撰成这套《新编计算机与信息科学十万个为什么》丛书。丛书内容丰富，形式新颖，图文并茂，深入浅出，面向青少年和广大群众，是计算机与信息科学普及教育难得的好教材。丛书不仅能让人们获

得从事计算机与信息技术所需的知识和技能，更重要的是，还能使人们从中受到科学思想、科学精神、科学态度和科学方法的教育。因此，这也是一部宣传社会主义精神文明的普及读物。

一部好书可以影响一代人。《新编计算机与信息科学十万个为什么》的编写出版，得到清华大学出版社以及中国计算机报社的大力支持，这是一件有意义的事情。采用“十万个为什么”的方式普及计算机知识，是一种十分有益的尝试。希望编写丛书的专家学者不断跟踪科技发展趋势，不断修改、扩充和更新丛书内容和媒体形式，使丛书越出越好，以满足广大读者的需要。

我们希望有更多的专家学者和学术团体参加科技普及工作，编写出版普及读物，传播科学知识，为推动两个文明建设，为把我国的经济建设转移到依靠科技进步和提高劳动者素质的轨道上来作出自己的贡献。

祝贺《新编计算机与信息科学十万个为什么》丛书出版成功。



丛书前言

计算机与信息科学的普及应用是一个国家现代化程度的重要标志，计算机与信息科学的发展水平和开发能力更是现代国家国力的重要表现。党中央和国务院在制订发展我国高新技术产业政策时，把计算机与信息科学列为优先发展的领域之一。举国上下，越来越多的人认识到学习和掌握这一领域的知识和技能的重要性，为了能在激烈竞争的现代社会生活中不落人后，为了能为实现社会主义四个现代化建设做出更大贡献，利用一切可以争取到的机会，甚至动用家庭有限的收入作投资，创造条件，学习计算机科学知识和技能，在全国各地正在形成越来越高的热潮。在这种形势下，作为在计算机和信息科学领域里耕耘多年的识途老马们，自然有义不容辞的责任，为青少年和广大迫切需要学习计算机与信息科学的已入门和未入门的群众做出自己应有的贡献，帮助大家克服困难，少走弯路，尽快占领这一领域的各个高地。

帮助青少年和广大群众掌握计算机与信息科学的基础知识和基本技能是实现科技兴国战略任务的重要组成部分。当今，计算机与信息科学早已从为少数科学家所专有演变为解决科学、技术、工程和日常生活各方面问题的强有力的技术和工具。掌握计算机科学的原理和应用技能既可以为儿童、青少年进一步学习科学技术打下良好基础，也是广大群众掌握现代工具、提高生活技能的有效途径。为了有效地实现这一目标，最重要的是激发大家学习和掌握计算机知识与技能的兴趣和睿智，而不是简单地让大家学会几条指令的操作或某几个软件的使用，因为这些东西会随着科技的进步、版本的更新很快“过时”，唯有掌握学习的能力和探讨计算机科学技术的兴趣是长久不衰的。

基于上述原因，上海市计算机学会在清华大学出版社、电子工业部计算机与微电子发展研究中心、中国计算机报社的大力支持下，聘请了100多位长期从事计算机与信息科学各个领域的教学和科学研究、有丰富经验、学有所成的专家、教授，从计算机与信息科学的宝库中，选取了人们在学习、工作以及生活中经常会碰到的问题，力图用生动有趣的例子、浅显明白的道理、通俗准确的语言来回答这些问题，来描述计算机与信息科学的过去、现在和未来，真可以说是历经寒暑，十易其稿，最终编写成这套《新编计算机与信息科学十万个为什么》丛书。

丛书包括“引路篇”、“综合应用技术篇”和“专业技术基础篇”三篇，分为12个分册出版。作为丛书的第一本，“引路篇”提供的是学习计算机和信息科学的综合基础知识与技能，同时，也说明本篇的编写宗旨是“引路”，即起到“引进门”的作用。“综合应用技术篇”单独成册，主要是通过典型例子说明计算机技术是如何应用于日常生活的各个方面的。“专业技术基础篇”分为10个分册，包括以下12个专题：

1. 软件基础
2. 接口技术
3. 数据库
4. 信息检索
5. 数据通信
6. 计算机网络
7. 管理信息系统
8. 办公自动化
9. 多媒体
10. 计算机辅助设计
11. 人工智能
12. 计算机安全与保密

上述各篇各专题中问题的选取原则是，既针对青少年和广大群众当前学习的实际需

要，又照顾到计算机科学日新月异的发展。编写力求做到科学性、通俗性、趣味性并重，既有原理的说明，也有应用技术的指导。考虑到本丛书的基本读者群体是青少年和具有中等及中等以上文化程度的有志学习计算机知识的广大群众，每个题目都完整地说明一个知识点，绝大多数条目在知识结构上是相对独立的，在学习时不需要以其他题目的知识作为基础，这样的安排也是为了适应业余学习间隙性的需要。

每一分册条目的编号按以下原则编排： 条目编号的形式为 $x.y$，x 表示本书在丛书中的分册序号，y 表示该条目在本书中的序号。

本丛书的每一部分都包含了少量的计算机与信息科学的前沿知识，这种局部超前的安排，不仅是为了适应广大青少年进一步学习计算机和信息科学的需要，也有助于具有一定基础的各类专业人员扩展自己的知识面。而且，由于计算机科学及相关技术发展迅速，今天的所谓前沿知识，随着时代的进步和技术的发展，将成为日后大众的普及知识。

本丛书在编写时致力于提高读者的知识水平与学习能力，尽可能用简洁、准确的文字讲清原理，使读者在理解的基础上激发进一步学习的主观能动性，进行创造性的学习。我们认为，经常研究“为什么”，可以养成自己提出问题、解决问题的习惯，学会举一反三、融会贯通、启迪思路，一旦读者自己弄清了“为什么”的道理，一些具体操作通过相应的操作手册是容易掌握的。

希望本丛书能够成为青少年和广大群众前往计算机与信息科学殿堂时的登堂台阶，这就是我们的用心所在。

《新编计算机与信息科学十万个为什么》
丛书编委会

2000 年 4 月

编者的话

计算机安全是一门政策性、技术性、实用性很强的综合学科。随着计算机技术的迅速发展，计算机应用日益深入社会各个方面。计算机信息的大量积聚和传播，使计算机和计算机信息的管理出现了一个崭新的局面。计算机作为现代科学、军事、经济、工农业生产、交通、通信、教育卫生等领域的高科技手段，它既为社会经济的飞跃发展、社会教育的普及提高创造了十分有益的条件；同时又为个别人利用计算机进行违法犯罪或某些不道德行为，提供了极具危害性的工具和危害性的工具和空间。因此，如何从法规条例、道德教育、风险分析、技术防护、科研探索等方面来改善计算机管理的质量，使计算机在现代信息管理中做到有序、有利、有效，这就是对计算机安全进行技术研究、技术开发、技术实施和技术评估的目标。一般地说，一个高质量的计算机系统应伴有一个相对完善的安全体系。

计算机的不安全因素来自诸多方面，例如自然的、环境的、管理的、计算机软件的、硬件的以及各种人为的因素。所以，计算机安全作为一门新兴学科，它除了与计算机本身的各个学科，如计算机科学、计算机硬件、计算机程序设计、操作系统、数据库、计算机网络……有关外，还与数学、物理、通信、信息管理、密码学、工程技术学，甚至生物、化学、社会科学、人文科学等等学科有着密切的关联，所以，要准确全面地反映计算机安全的全貌是十分困难的。

为了能让广大读者对计算机安全有一个初步了解，本书仅以计算机安全技术，密码学和计算机病毒等三部分为基础，将与计算机安全有关的最基本的概念、方法、政策、技术等知识简要地介绍给大家。由于写作时间紧迫，资料收集也不够充分，所以只涉及到当今国内外有关计算机安全问题中部分内容，仅供大家参考。有兴趣的读者可以在此

基础上查阅更多的资料，得以补益。

本书在上海市计算机学会、上海市公安局计算机管理监察处、复旦大学计算机科学系和部分从事计算机安全产品开发生产的企业支持下，组织部分人员编写的。参加编写的作者有：鲍振东，赵一鸣，马先玉，覃光，徐寿怀，须勇敏，黄寿根，王岩增，黄步根，吴洪来，卢先捷，严明，吴一鸣，廖继，邓寅，梁兆明，燕来。

感谢本丛书主编张吉锋教授和吴洪来常务编委对本分册全部文稿进行了仔细审阅并提出了宝贵意见。我们也感谢关心并组织出版本书的单位、领导和有关人员。欢迎广大读者对书内的不当之处提出意见。

编　者

2000 年 9 月

目　　录

计算机安全技术

密码学在计算机安全技术中的应用