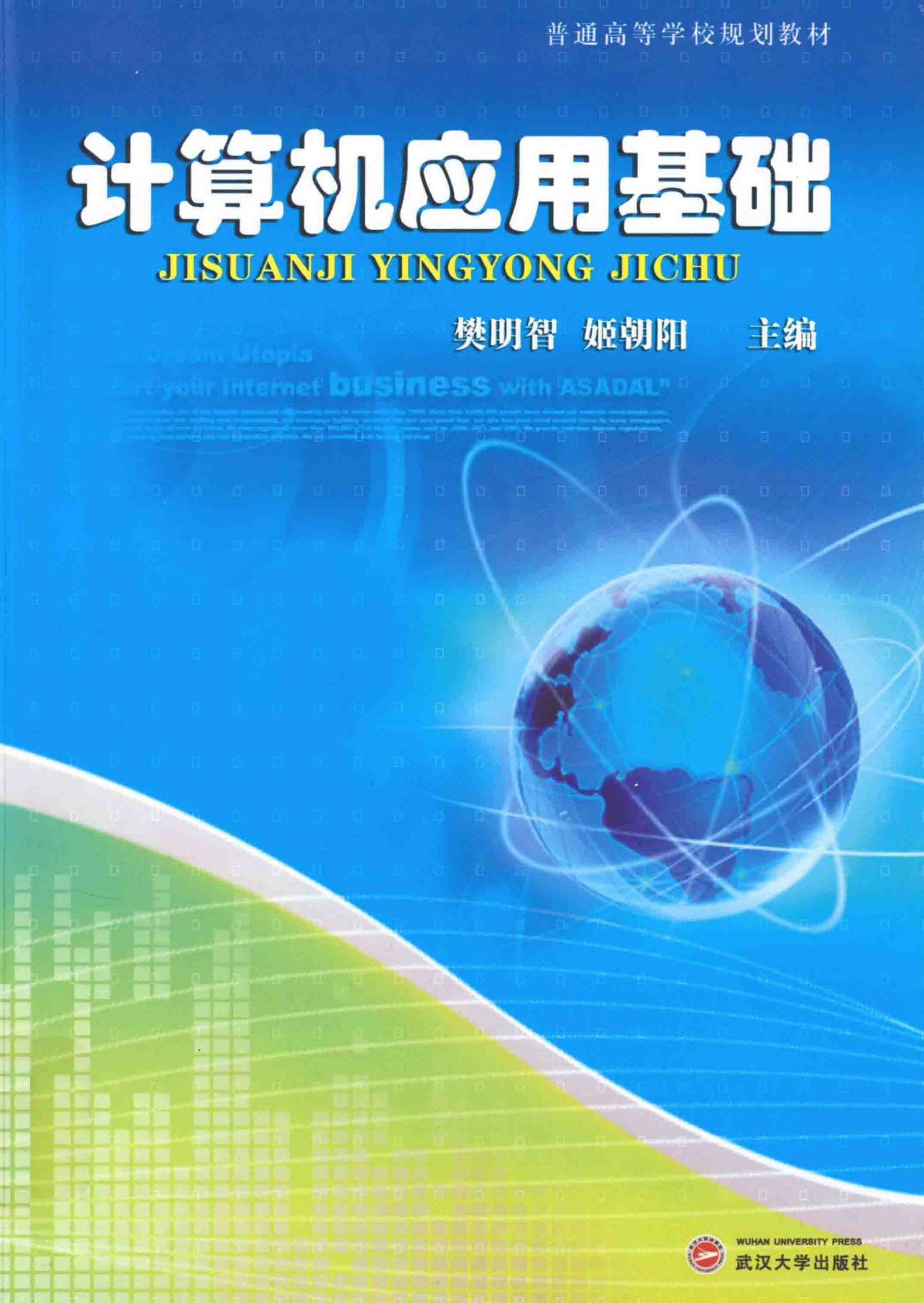
普通高等学校规划教材

计算机应用基础

JISUANJI YINGYONG JICHU

樊明智 姬朝阳 主编



WUHAN UNIVERSITY PRESS
武汉大学出版社

高等教育“十一五”国家级规划教材

应用密码学

胡向东　魏琴芳　编著

王晓京　主审

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书兼具专著和教材的双重属性，是作者从事多年的应用密码学相关教学和科研工作实践的结晶。本书全面介绍了应用密码学的基本概念、基本理论和典型实用技术。全书共 15 章，内容涉及密码学基础、古典密码、密码学数学引论、对称密码体制、非对称密码体制、HASH 函数和消息认证、数字签名、密钥管理、序列密码、量子密码；书中还介绍了应用密码学在电子商务支付安全、数字通信安全、工业网络控制安全和无线传感器网络感知安全这四个典型领域的应用方法和技术。语言简练，内容重点突出，逻辑性强，算法经典实用；突出的特色是将复杂的密码算法原理分析得透彻深入，便于读者花少量的时间尽快掌握应用密码学的精髓。

本书可作为高等院校密码学、应用数学、信息安全、通信工程、计算机、信息管理、电子商务、检测技术、控制理论与控制工程、系统工程等专业高年级本科生和研究生教材，也可供从事网络和通信信息安全相关领域应用和设计开发的研究人员、工程技术人员参考。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

应用密码学 / 胡向东等编著. —北京：电子工业出版社，2006.11
ISBN 978-7-121-03226-4

I. 应… II. 胡… III. 密码－理论 IV. TN918.1

中国版本图书馆 CIP 数据核字（2006）第 119168 号

责任编辑：刘志红　康　霞
印　　刷：
装　　订：北京京科印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×1092　1/16　印张：22.25　字数：541 千字
印　　次：2011 年 1 月第 4 次印刷
定　　价：39.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn。盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

序

随着信息化在全球的发展，互联网、电信网、广播电视网正在走向融合，计算机、通信、数码电子产品也朝着 3C 融合的方向发展，人们的社会生活对网络的依赖越来越大，信息及信息系统的安全与公众利益的关系日益密切。当人类面对外界时，人身安全是第一需求，人们需要相互传授安全防范的经验和技能。当人类步入信息社会之时，我们不难发现信息安全还是我们的第一需求，而且现在比过去任何时候都更需要普及信息安全的意识和知识。只有当这种意识和知识为工程技术人员真正掌握，并为公众所接受，整个社会的信息安全才有可靠的保障。

自 50 多年前香龙的“保密通信的信息理论”一文问世以来，密码学逐步从经验艺术走上了严谨科学的道路，成为了当今社会信息安全技术的坚实基石。不了解密码学，也很难真正驾驭信息安全。另一方面，互联网等当代信息技术领域提出的一系列信息安全新课题（其中许多还是有趣的科学问题和严肃的社会问题），反过来又推动着密码学不断深入发展和广泛应用，使密码学洋溢着生机和魅力。

密码学及其应用是跨学科的交叉研究领域，其成果和思想方法的意义已经不限于数学，甚至也不仅仅限于信息安全。国外从 20 世纪 70 年代起，密码和编码理论及技术逐渐成为许多工程学科的基础课程。事实上，它们不仅对理工科学生的训练有益，法律、管理等文科的学生也能从中吸收到思想和心智的知识养分。

现代密码学的确是建立在数学理论的基础之上的，但使用它的人绝不限于数学家，当代工程技术人员对它的需求也许更为迫切，它的应用和发展更需要普及和深入到越来越多的交叉领域中去。为了能够达到精确、简洁、优美的目的，密码学常常需要从形式化的数学层面来刻画；同时密码学也需要人们从工程应用的角度来理解它，甚至需要从逻辑常识和宽广的知识背景来介绍它和思考它，才能领会它的精髓，丰富它的内涵，灵活它的使用。

然而由于历史原因，适合工程技术人员的密码学中文教程相对较少，现代密码学的抽象形式使许多其他专业背景的人对它望而生畏，这就妨碍了它精妙思想和方法的普及。今天，网络安全等领域提出了越来越多的密码技术应用问题，客观上对应用密码学这种体裁的专著有了更广泛、更迫切的需要。

《应用密码学》使工科背景的读者多了一个选择，在一定程度上弥补了上述遗憾。这本

书的许多内容来源于作者在工程学科的密码学教学实践，注重从工程技术人员和学生易于接受的方式来介绍密码学的要领，不拘泥于细腻的理论证明和形式上的严谨。书中的一些重点章节还设置了许多有价值的具体实例，全书配有计算机 CAI 教学课件，这些对读者当不无裨益。针对当前网络安全的热点问题，作者在书中也适时地介绍了一些新的典型应用，抛砖引玉，使图书内容增色不少。

本书似也在追求一种信念：更多人的实践和思考有助于推动密码学的发展，多种风格、面向多种应用领域的应用密码学知识能够为密码学大厦添砖加瓦。读后有感，是为序。

中国科学院成都计算机应用研究所研究员、博导

试读结束：需要全本请在线购买： www.ertongbook.com

前　言

随着通信和计算机技术的快速发展及经济全球化应用的推动，互联网表现出广泛的覆盖性（包括地域覆盖性、应用领域的覆盖性、使用人群的覆盖性）、使用的方便性、信息传递的快捷性和运作的低成本特性，人们对信息网络的依赖程度越来越大，各种新兴的网络应用层出不穷，并相互推动。移动通信、电子商务、电子政务、企业信息化、“三金工程”等与社会发展、人们生产和生活息息相关领域的信息安全问题，越来越成为全社会关注的焦点，并成为制约网络应用发展的主要瓶颈之一。没有安全就没有应用，没有应用就没有发展，提高全社会的网络信息安全意识和基本专业知识是保障我国信息化建设健康、稳步、快速发展的前提和基础。

应用密码学作为实现网络信息安全的核心技术，在保障网络信息安全的应用中具有重要的意义，而对典型密码学算法的掌握又是快速实现信息安全的捷径。在各种网络应用迫切呼唤信息安全的背景下，作者在学习、总结众多国内外有关网络信息安全和应用密码学文献基础上，凝聚自己多年的教学和科研工作实践成果，特别针对教学工作需要和学习规律完成了本书的编著工作。在本书编撰过程中，特别注重体现以下特色。

先进性。本书根据应用密码学的发展趋势，在讲清应用密码学基本概念的同时，力求对当前及未来具有很强应用前景的对称密码体制（包括序列密码）、非对称密码体制的典型密码算法的基本工作原理及其应用方法进行了系统、深入的介绍。

典型性。本书不求面面俱到，力争帮助读者快速入门并掌握密码学的核心内容，因此在密码算法的选取、例题设置和不同领域的应用方法等方面都体现出广泛的代表性和典型性。

易学性。本书的编排从教学适用性出发，特别重视读者对应用密码学知识的系统理解和有针对性地重点掌握，在内容安排上力求层次清晰、结构合理、由浅入深、循序渐进、逻辑严密、前后呼应、主次分明、重点突出；在语言表达上力求文笔流畅、言简意赅、深入浅出、通俗易懂。

有趣性。科学是严谨的，但科学与生活并不是完全分离的，书中提供的部分背景知识增加了学习密码学的趣味性，有助于调节学习节奏，倡导和发现科学中孕育的和谐。

本书全面介绍了应用密码学的基本概念、基本理论和典型实用技术。在结构上分为网络信息安全概述、密码学基础、古典密码、密码学数学引论、对称密码体制、非对称密码体制、

HASH 函数和消息认证、数字签名、密钥管理、序列密码、密码学与电子商务支付安全、密码学与数字通信安全、密码学与工业网络控制安全、密码学与无线传感器网络感知安全、密码学的新进展——量子密码学。每章末都给出了适量的思考题和习题作为巩固知识之用，并附有参考答案。为了方便使用，对于较高要求的部分用符号“*”标识。

本书兼具专著和教材的双重属性，突出的特色是将复杂的密码算法原理分析得透彻深入，便于读者花少量的时间尽快掌握应用密码学的精髓。教师可在 32～56 学时内讲解全部或选讲部分内容，还可以配以适当的上机教学进行动手实践，在有限的时间内快速掌握应用密码学的核心内容，提高学习效率。

本书可作为高等院校密码学、应用数学、信息安全、通信工程、计算机、信息管理、电子商务、检测技术、控制理论与控制工程、系统工程等专业高年级本科生和研究生教材，也可供从事网络和信息安全相关领域应用和设计开发的研究人员、工程技术人员参考。

本书由重庆邮电大学胡向东教授组织编著，第 3，4，10，12 章由魏琴芳高工编著，胡向东负责其余章节的编著和全书的统稿。作者要特别感谢参考文献中所列各位作者，包括众多未能在参考文献中一一列出资料的作者，正是因为他们在各自领域的独到见解和特别的贡献为作者提供了宝贵的资料和丰富的写作源泉，使作者能够在总结教学和科研工作成果的基础上，汲取各家之长，形成一本体现自身价值、极具特色的应用密码学教材。

参加本书编写、CAI 课件和习题答案制作等工作的还包括重庆邮电大学自动化学院张毅、蔡军、张开碧、谢颖等老师；高旸、徐笑尘、易明华、余刚等研究生参与了部分资料的收集和整理工作；中科院成都计算机应用研究所的王晓京研究员对本书进行了认真细致的审阅并提供了宝贵的修改意见和建议；电子工业出版社的刘志红、康霞编辑为本书的高质量出版倾注了大量心血；在此对他们付出的辛勤劳动表示由衷的感谢。本书的编著出版受到高等教育“十一五”国家级教材规划建设项目、重庆市教委科技研究项目、重庆市科委自然科学基金计划项目和重庆邮电大学出版基金资助，并得到上海交通大学访问学者项目和江志斌教授的支持。

本书另配有相应的 CAI 课件，如有需要，请与出版社或作者联系免费索取，或从电子工业出版社华信教育资源网免费下载。

应用密码学是一门内容广泛、发展迅速的学科，对本书的编著是作者在此领域的一次努力尝试，限于作者的水平和学识，书中难免存在疏漏和错误之处，诚望读者不吝赐教，以利修正，让更多的读者获益。我们的联系方式是：huxd@cqupt.edu.cn。

作　者

2006 年 9 月

目　录

试读结束：需要全本请在线购买： www.ertongbook.com

第1章 绪 论

1.1 网络信息安全概述

1.1.1 网络信息安全问题的由来

随着通信与计算机网络技术的快速发展和公众信息系统（包括计算机互联网、移动通信网、磁卡系统等）商业性应用步伐的加快，当数据通信和资源共享等网络信息服务功能广泛覆盖于各行各业及各个领域，网络用户来自各个阶层与部门，人们对网络环境和网络信息资源的依赖程度日渐加深时，网络信息的安全隐患就从各个方面越来越明显地突现出来，大量在网络中存储和传输的数据需要保护，因为这些数据本身对于所有者来说可能是敏感数据（如个人的医疗记录、信用卡账号、登录网络的口令，或者企业的战略报告、销售预测、技术产品的细节、研究成果、人员的档案等）。这些数据在存储和传输过程中都有可能被盗用、暴露、篡改和伪造。除此之外，基于网络的信息交换还面临着身份认证和防否认等安全需求。这些问题被公认为是21世纪公众信息系统发展的关键。

目前，作为数据通信和资源共享的重要平台——互联网是一个开放系统，其具有资源丰富、高度分布、广泛开放、动态演化、边界模糊等特点，安全防御能力非常脆弱，而攻击却易于实施，且难留痕迹。随着网络技术及其应用的飞速发展，黑客袭击事件不断发生并在逐年递增，网络安全引起了世界各国的普遍关注。就我国而言，目前，我国信息化建设已进入高速发展阶段，电子政务、电子商务、网络金融、网络媒体等正在兴起，这些与国民经济、社会稳定息息相关的领域急需信息安全保障。

1.1.2 网络信息安全问题的根源

产生网络信息安全问题的根源可以从三个方面分析：自身缺陷、开放性和人的因素。

1．网络自身的安全缺陷

网络自身的安全缺陷主要是指协议不安全和业务不安全。

导致协议不安全的主要原因：一方面是Internet从建立开始就缺乏安全的总体构想和设计，因为Internet起源的初衷是方便学术交流和信息沟通，并非商业目的。Internet所使用的TCP/IP协议是在假定的可信环境下，为网络互联专门设计的，本身缺乏安全措施的考虑。TCP/IP协议的IP层没有安全认证和保密机制（只基于IP地址进行数据包的寻址，无认证和保密）。在传输层，TCP连接能被欺骗、截取、操纵，UDP易受IP源路由和拒绝服务的攻击。另一方面，协议本身可能会泄露口令、连接可能成为被盗用的目标、服务器本身需要读写特权、密码保密措施不强等。

业务的不安全主要表现为：业务内部可能隐藏着一些错误的信息；有些业务本身尚未完善，难以区分出错原因；有些业务设置复杂，一般非专业人士很难完善地设置。

2．网络的开放性

网络的开放性主要表现为：业务基于公开的协议；连接是基于主机上的社团彼此信任的原则；远程访问使得各种攻击无须到现场就能得手。在电脑网络所创造的特殊的、虚拟的空间中，网络犯罪往往是十分隐蔽的，有时会留下蛛丝马迹，但更多时候是无迹可寻。

3．人的因素

人是信息活动的主体，是引起网络信息安全问题最主要的因素，可以从三个方面来理解。

（1）人为的无意失误

人为的无意失误主要是指用户安全配置不当造成的安全漏洞，包括用户安全意识不强、用户口令选择不当、用户将自己的账号信息与别人共享、用户在使用软件时未按要求进行正确的设置。

（2）黑客攻击

这是人为的恶意攻击，是网络信息安全面临的最大威胁。黑客一词来源于20世纪60年代的美国麻省理工学院（MIT），大意是指电脑系统非法入侵者。这是一类闯入计算机网络系统盗取信息、故意破坏他人财产、使服务中断或仅仅为了显示他们可以做什么的人。黑客们对电脑非常着迷，自认为比他人有更高的才能，因此，只要他们愿意，就闯入某些信息禁区，开玩笑或恶作剧，有时干出违法的事。他们常以此作为一种智力上的挑战，好玩、刺激可能是他们最初追随的动机，但当有利可图时，很多人往往抵制不住诱惑而走上犯罪道路。信息战[①]也是开展黑客攻击的一个非常重要的缘由。

在英文中，黑客有两个概念：Hacker 和 Cracker。Hacker 是这样一类人，他们对钱财和权利蔑视，而对网络本身非常专注，他们在网上进行探测性的行动，帮助人们找到网络的漏

① 信息战的几种具有代表性的样式：1）指挥控制战——其目的是通过对敌信息系统实施物理和电子攻击，来阻隔敌军部队与其指挥者的联系。总的来看，攻击敌军领导与部队的连接部位，可以更有效地破坏敌人的指挥控制系统。2）电子战——现在，只要在保护己方电子系统不受干扰的同时，能干扰或破坏敌方的电子信息系统，就能在战争中取得决定性优势。随着军队对电子系统的依赖性不断增大，这种优势将有增无减。电子战的目的在于使敌方得不到信息，或只能得到少量信息或迟到的信息，或制造假象，使敌军采取错误的行动。3）情报战——人造卫星技术的进步和成像系统的出现，使侦察和监视能力有很大的提高。在信息分发系统研制成功并得到实际运用后，用户便可实时地接收和传输数据。这就使得把传感器、发射设备和信息处理装置纳入一个统一的侦察、监视、目标捕捉和战场损失评估系统成为可能。4）心理战——当针对军队实施心理战时，可利用信息媒体在正在实施或准备实施战斗的部队中制造沮丧和失望情绪，以改变指挥官和士兵的心态。对社会实施心理战在于利用大众媒体左右公众舆论。5）黑客战——计算机黑客行动使用有害软件等高技术手段，摧毁、破坏、利用或危害军用和民用信息系统。黑客战的主要武器是计算机病毒，这种病毒可以通过电话线输入。除了向计算机网络注入病毒外，谍报人员在实施黑客战时，还可向敌方计算机系统注入称为“微生物”的程序或代码，这些“微生物”能吞噬破坏电子系统，以使计算机系统长时间无法有效运行。6）信息、经济战——一个国家可通过有组织地实施黑客行动并利用银行和股票市场，来破坏另一个国家的经济。这种行动将把信息战提高到战略层次，即“信息、经济战”。人们还可以利用这种行动实施信息封锁，可阻止敌方和确保己方利用贸易信息。

试读结束：需要全本请在线购买： www.ertongbook.com