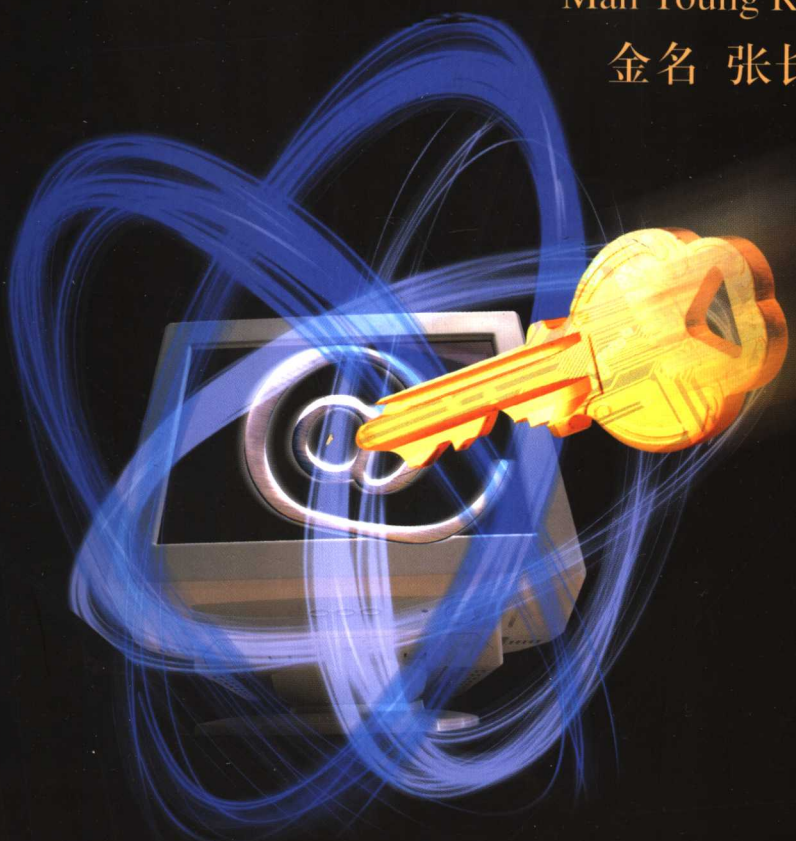
WILEY Publishers Since 1807
世界著名计算机教材精选

网络安全

加密原理、算法与协议

Man Young Rhee 著
金名 张长富 等译



INTERNET SECURITY

CRYPTOGRAPHIC PRINCIPLES, ALGORITHMS AND PROTOCOLS

清华大学出版社

世界著名计算机教材精选

网络安全

加密原理、算法与协议

Man Young Rhee 著
金 名 张长富 等译

清华大学出版社
北 京

内 容 简 介

Man Young Rhee

Internet Security: Cryptographic Principles, algorithms, and protocols

EISBN: 0-470-85285-2

北京市版权局著作权合同登记号 图字 01-2007-1847 号

图书在版编目(CIP)数据

网络安全: 加密原理、算法与协议/(韩)李迈勇(Rhee. M. Y)著; 金名等译. —北京: 清华大学出版社,2007.7

书名原文: Internet Security

ISBN 978-7-302-15259-0

Ⅰ. 网… Ⅱ. ①李… ②金… Ⅲ. 因特网—安全技术 Ⅳ. TP393.48

中国版本图书馆 CIP 数据核字(2007)第 074186 号

责任编辑: 张 剑

责任印制: 孟凡玉

出版发行: 清华大学出版社 **地 址**: 北京清华大学学研大厦 A 座

http://www.tup.com.cn **邮 编**: 100084

c-service@tup.tsinghua.edu.cn

社 总 机: 010-62770175 **邮购热线**: 010-62786544

投稿咨询: 010-62772015 **客户服务**: 010-62776969

印 装 者: 北京国马印刷厂

经 销: 全国新华书店

开 本: 185×260 **印 张**: 20.75 **字 数**: 485 千字

版 次: 2007 年 7 月第 1 版 **印 次**: 2007 年 7 月第1 次印刷

印 数: 1~3000

定 价: 39.00 元

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　计算机与信息分社营销室　收

邮编：100084　　电子信箱：jsjjc@tup.tsinghua.edu.cn

电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：网络安全：加密原理、算法与协议

ISBN：978-7-302-15259-0

个人资料

姓名：_____　年龄：_____所在院校/专业：_____

文化程度：_____　通信地址：_____

联系电话：_____　电子信箱：_____

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书的总体满意度：

从语言质量角度看　□很满意 □满意 □一般 □不满意

从科技含量角度看　□很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？(可附页)

_____

_____

您希望本书在哪些方面进行改进？(可附页)

_____

_____

译者序

今天，因特网是所有信息的基础设施，是信息传播的一种机制，是个人、政府机关、金融机构、学术团体和各种商业贸易之间进行协作和交互的媒介，而且没有地理位置的限制。

不论由于是个人还是专业使用的需要，人们已经变得越来越依赖于因特网了，如E-mail、文件传送、远程登录、Web页面访问或商业事务处理。因特网使计算和通信世界发生了革命性的变化，以开发和支持客户和服务器服务。因特网的可用性及其能提供的强大的计算和通信能力，使得形成了一种新的商业模式。由于浏览器和万维网技术的应用，允许用户很容易地访问链接到全球的信息，这更是得到了极大地促进这种商业模式。

因特网是全球范围的，但这种全球的互连网络是开放的、不安全的媒体。随着人们对因特网的不断认识和因特网的普及，因特网安全问题显现出来了。要保护用户免受基于因特网的攻击，当出现安全问题时提供恰当的解决办法，必须应用密码技术。本书介绍的就是在因特网安全中有关密码操作、原理、算法和协议的核心内容。要消除由犯罪活动产生的各种威胁，必须依靠密码技术。在培育、改进和提供因特网安全中，认证、消息完整性和加密是非常重要的。没有这种认证过程，攻击者可以模仿任何人，然后获得对网络的访问权。要求消息完整性是因为数据在因特网中传输时可能被修改。没有经过加密，信息就可能变成真正的公开了。

本书通过严谨、彻底和定性的讲述，深入地介绍了因特网安全及其实现的理论与实践知识。本书由11章组成，重点介绍了一些与因特网有关的关键的安全性问题。本书首先简要介绍了因特网的历史和TCP/IP协议族，使读者对因特网和TCP/IP协议有一个初步的了解，为后面介绍因特网安全打下基础。接着介绍了一些重要的分组加密算法和数字签名技术，并介绍了几种公钥加密系统以及因特网的公钥基础设施，然后介绍了网络层安全的IPsec协议和安全套接字层协议，这些是实现因特网安全所需的技术和手段。最后介绍了E-mail的安全性和防火墙的设计与实现，以及用于保护因特网信用卡事务处理的SET协议。

本书由金名、张长富主译，黄中敏、马静静、冯华君、宋明钧、刘守燕、杨咏梅、魏敬安、朱建波、徐志平、赵杰辉、傅祎、郭碧莲、郭洵、洪晓煜、黄宣达、江松波、柯渝、赖曲芳、廖阳、刘文红、贺军、王雷、戴军等人也参与了本书的一些工作。

本书适用于高年级本科生和研究生、专业工程师和研究人员作为因特网原理的入门教材。作为一本参考书，对计算机工程师、通信工程师和系统工程师都是很有用的。它还适用于自学。本书可以被学术和专业人士使用，还可以作为企业和研究机构的培训使用。

前言

因特网是全球范围的，但这种全球的互连网络是开放的、不安全的媒体。因特网使计算和通信世界发生了革命性的变化，以开发和支持客户和服务器服务。因特网的可用性及其能提供的强大的计算和通信能力，使得形成了一种新的商业模式。由于浏览器和万维网技术的应用，允许用户很容易地访问链接到全球的信息，这更是得到了极大地促进这种商业模式。因特网已被证实为当今信息贸易的基础工具。

今天，因特网是所有信息的基础设施，是信息传播的一种机制，是个人、政府机关、金融机构、学术团体和各种商业贸易之间进行协作和交互的媒介，而且没有地理位置的限制。

不论由于是个人还是专业使用的需要，人们已经变得越来越依赖于因特网了，如 E-mail、文件传送、远程登录、Web 页面访问或商业事务处理。随着人们对因特网的不断认识和因特网的普及，因特网安全问题显现出来了。在不安全的媒介上进行在线事务处理，很容易诱发因特网犯罪活动。

因特网访问经常会产生一个安全缺陷。要保护用户免受基于因特网的攻击，当出现安全问题时提供恰当的解决办法，必须应用密码技术。本书介绍的就是在因特网安全中有关密码操作、原理、算法和协议的核心内容。要消除由犯罪活动产生的各种威胁，必须依靠密码技术。在培育、改进和提供因特网安全中，认证、消息完整性和加密是非常重要的。没有这种认证过程，攻击者可以模仿任何人，然后获得对网络的访问权。要求消息完整性是因为数据在因特网中传输时可能被修改。没有经过加密，信息就可能变成真正的公开了。

本书通过严谨、彻底和定性的讲述，深入地介绍了因特网安全及其实现的理论与实践知识。本书适用于高年级本科生和研究生、专业工程师和研究人员作为因特网原理的入门教材。本书由 11 章组成，重点介绍了一些与因特网有关的关键的安全性问题。下面是每章内容的概述。

第 1 章开始介绍了因特网的简要历史，内容包括：(1) 网络技术基础，如 LAN (Ethernet、令牌环、FDDI)，WAN(帧中继、X. 25、PPP)和 ATM；(2) 连接设备，如电路交换和包交换、转发器、网桥、路由器和网关；(3) OSI 模型，它说明了其七层的功能；最后(4)五层的 TCP/IP 协议族，它提供了由物理标准、网络接口和互连网络组成的分层协议。

第 2 章介绍了 TCP/IP 协议族，内容包括：(1) TCP/IP 网络层协议，如 ICMP、与 IP 包格式有关的 IPv4 和 IPv6，寻址(包括 ARP、RARP 和 CIDR)和路由；(2) 传输层协议，如 TCP 和 UDP；(3) 用于万维网的 HTTP；(4) 用于文件传递的 FTP、TFTP 和 NFS 协议；(5) 用于E-mail 的 SMTP、POP3、IMAP 和 MIME；(6) 用于网络管理的 SNMP 协议。

第 3 章介绍了现代一些重要的分组加密算法，这些算法是近年来开发的，重点介绍了使用最广泛的加密技术，如数据加密标准(Data Encryption Standard, DES)国际数据加密算

法(International Data Encryption Algorithm，IDEA)，RC5 和 RC6 加密算法，以及高级加密标准(Advanced Encryption Standard，AES)。AES 指的是经 FIPS 认可的 Rijndael 算法(2001)，它可以处理 128 位的数据分组，使用的密钥长度为 128、192 和 256 位。DES 不是新东西，但它已经经受了 20 多年的强度密码分析。本章还全面分析了 CBC 模式的三重 DES-EDE、用于 E-mail 的 Pretty Good Privacy (PGP)，用于常规分组加密的文件存储实用工具 IDEA，以及用于公钥加密的 RSA 和用于哈希编码的 MD5。RC5 和 RC6 都是大小可变、轮数可变、密钥长度可变的参数化分组算法。它们在性能和安全级别上都有很大的灵活性。

第 4 章介绍了基于数字签名的不同认证技术。通常，通信双方需要验证对方的身份。这样做的一个实用方法是使用密码认证协议，该协议应用了一个单向的哈希函数。本章介绍了几种现代的哈希函数(例如 DMDC、MD5 和 SHA-1)，用于计算消息摘要或哈希代码，为认证提供对称方法。本章还扩展讨论了因特网标准 HMAC，它是受保护数据的一种安全摘要。HMAC 使用了不同的哈希算法，包括 MD5 和 SHA-1。传输层安全(Transport Layer Security，TLS)也使用了 HMAC 算法。

第 5 章在介绍了常规加密后，还介绍了几种公钥加密系统。本章重点介绍了用于公钥加密、数字签名和认证的技术。本章还详细介绍了广泛使用的 Diffie-Hellman 密钥交换技术(1976)、RSA (Rivest-Schamir-Adleman)算法(1978)、ElGamal 算法(1985)、Schnorr 算法(1990)、数字签名算法(DSA，1991)和椭圆曲线加密系统(ECC，1985)与椭圆曲线数字签名算法 (ECDSA，1999)。

第 6 章因特网的公钥基础设施(public-key infrastructure，PKI)。PKI 通过公钥证书自动地管理公钥。策略认可机构(Policy Approval Authority，PAA)是证书管理基础设施的根。该机构对 PKI 整个级别上的所有项都是已知的，为所有用户生成指导说明，CA 和下级的策略制定机构必须遵守。策略认证机构(Policy Certificate Authorities，PCA)由该基础设施中第二级的所有项组成。PCA 必须发布安全策略、过程、合法性问题、费用以及其他认为有必要的内容。认证机构(Certification Authorities，CA)形成了 PCA 的下一级。PKI 由很多的 CA 组成，CA 不负责策略的制定。CA 由用户和它认证的 RA 组成。CA 的基本功能是生成和管理公钥证书，它把用户的身份与用户的公钥捆绑在一起。注册机构(Registration Authority，RA)是用户与 CA 之间的接口。RA 的基本功能是从 CA 的角度进行用户的身份确认和认证。它还给终端用户发放 CA 证书。X.500 描述的是目录服务。X.509 使用 X.500 目录描述了认证服务。X.509 证书经历了三个版本：1998 年的版本 1，1993 年的版本 2 和 1996 年的版本 3。现在的 X.509 v3 是基于大量产品和因特网标准而形成的。这三个版本将依次介绍。最后，证书注销列表(Certificate Revocation Lists，CRL)用于列举那些已注销的未到期的证书。CRL 可能是从例程管理注销到私钥生成条件等多种原因被重新激活。本章还介绍了因特网 PKI 的证书路径合法认证过程和 PKI 证书管理基础设施的体系结构。

第 7 章介绍了网络层安全的 IPsec 协议。IPsec 提供了在因特网或公用 WAN 上的 LAN 和虚拟专用网(virtual private network，VPN)进行安全通信的能力。IPsec 的使用使得商业活动可以极大地依赖因特网。IPsec 协议是由 IETF 开发的一组安全扩展，使用密码算法和协议在 IP 层提供保密和认证服务。要保护 IP 数据包(datagram)的内容，有两种主要的转换类型：认证头(Authentication Header，AH)和封装安全负载(Encapsulating

Security Payload，ESP)。这些是提供无连接完整性、数据原始认证、保密性和反重放服务的协议。安全关联(Security Association，SA)是 IPsec 的基础。AH 和 ESP 都使用了 SA。SA 是发送方与接收方之间的一个简单连接，为其中进行的数据流量提供安全服务。本章还介绍了 OAKLEY 密钥确认协议和 ISAKMP。

第 8 章讨论了安全套接字层协议版本 3(Secure Socket Layer version 3，SSLv3)和传输层安全协议版本 1(Transport Layer Security version 1，TLSv1)。TLSv1 协议本身是基于 SSLv3 协议的。很多与算法有关的数据结构和规则都非常类似，因此 TLSv1 和 SSLv3 之间的差别不大。TLSv1 协议为因特网上的通信双方提供通信保密与数据完整。这两种协议都允许客户/服务器应用程序以这样一种方式进行通信：防止偷听、篡改或消息伪造。SSL 或 TLS 协议由两层组成：记录协议与握手协议。记录协议携带要传递的高层应用消息，把数据分割成易管理的分组，还可以压缩数据，应用 MAC，进行加密，添加头部，并把结果传递给 TCP。被接收的数据经解密后给更高级的客户。握手协议是在记录层之上进行操作的，是 SSL 或 TLS 最重要的部分。握手协议由客户与服务器交换的消息系列组成。该协议在服务器与客户之间提供了三种服务。握手协议允许客户/服务器达成一个协议版本，通过组成一个 MAC 来进行相互认证，在传递应用程序协议或接收数据的第一个字节之前，协商一个加密算法和密钥，用于保护以 SSL 记录形式发送的数据。受密钥保护的哈希消息认证码(hashing message authentication code，HMAC)是一些受保护数据的安全摘要。没有 MAC 秘密的知识，无法伪造 HMAC。HMAC 可以与多种不同的哈希算法一起使用：MD5 和 SHA-1，这可以表示为 HMAC-MD5 (secret，data)和 SHA-1 (secret，data)。SSLv3 方案与 TLS MAC 方案有两个不同：TSL 使用的是定义在 RFC 2104 中的 HMAC 算法，TLS 的主秘密计算也与 SSLv3 的不同。

第 9 章介绍了 E-mail 的安全性。由 Philip Zimmermann 发明的 Pretty Good Privacy (PGP)，在全球计算机社区的多种平台上，被广泛地用在了个人和商业版本中。PGP 组合使用了对称密钥和非对称公钥加密，为 E-mail 和数据文件提供安全服务。PGP 使用数字签名、加密、压缩(ZIP)和 radix-64 转换(ASCII Armor)为消息和数据文件提供数据完整性服务。随着人们对 E-mail 和文件存储依赖的不断加深，认证和保密服务变得越来越重要了。多用途因特网邮件扩展(Multipurpose Internet Mail Extension，MIME)是 RFC 822 框架的扩展，它定义了使用 E-mail 发送文本消息的格式。MIME 真正的目的是解决使用 SMTP 的某些问题和限制。S/MIME 提高了 MIME 因特网 E-mail 格式标准的安全，它基于来自 RSA 数据安全的技术。尽管 PGP 和 S/MIME 走的都是 IETF 标准之路，但看起来 PGP 为很多用户保持了对个人 E-mail 安全性的选择，而 S/MIME 是作为商业和企业使用的工业标准出现的。PGP 和 S/MIME 方案都在本章进行了介绍。

第 10 章讨论了防火墙主题。防火墙是一种用于防止内部系统免受因特网安全威胁的有效方法。防火墙是一个安全的网关，它控制了在公用因特网与专用内部网(或企业网)之间的访问。防火墙是一种代理，它以某种方式监视网络流量，阻止它认为是不恰当或危险的流量。在现实中，因特网访问为单个用户、政府机关和大多数组织带来了好处。但这种访问也产生了安全威胁。在双向处理 SMTP 和 HTTP 连接中，防火墙起到了一个中间服务器的作用。防火墙还要求使用访问协商和诸如 SOCKS 之类的封装协议，以获得对因特网和内部网的访问。很多防火墙支持三重宿主，允许使用 DMZ 网络。要设计和配置防火墙，需

要熟悉堡垒主机(bastion host)代理服务器、SOCKS、节流点(choke point)、DMZ、日志与警告、VPN 等。防火墙可以划分为三大类：包过滤器、电路层网关和应用程序网关。本章将依次介绍每种防火墙。最后，本章将介绍遮挡式主机(screened host)防火墙以及如何实现防火墙策略。要实现一定级别的安全，可以考虑三种基本的防火墙设计：单宿主堡垒主机(single-homed bastion host)、双宿主堡垒主机(dual-homed bastion host)和遮挡式子网防火墙。

第 11 章介绍了用于保护因特网信用卡事务处理的 SET 协议。近年来电子商务的快速发展，为消费者、零售商和金融机构提供了巨大的机会。SET 协议依靠密码和 X.509 v3 数字证书来确保消息保密、支付完整性和身份认证。使用 SET 协议，通过保证支付信息是安全的，只能被既定的接收者访问，保护了消费者和经销商。SET 协议通过确保信息在任何时候都是经安全加密的，使用数字签名验证那些访问支付信息的人的身份，防止传输信息在传送时被修改。SET 是唯一的因特网事务处理协议，通过认证来提供安全性。消息数据使用随机对称密钥进行加密，而该随机对称密钥又使用接收者的公钥进行了加密。已加密消息与数字信封一起发送到接收者。接收者用私钥把数字信封解密，然后使用对称密钥还原原始消息。SET 协议通过使用数字签名和数字证书验证信用卡持卡人与经销商之间的金融关系，解决了因特网购物的匿名问题。本章还全面地探讨了如何确保因特网的安全信用卡事务处理。

本书适用于高年级本科生或研究生一或两学期课程的教材。作为一本参考书，对计算机工程师、通信工程师和系统工程师都是很有用的。它还适用于自学。本书可以被学术和专业人士使用，还可以作为企业和研究机构的培训使用。在本书的最后，有一个常用的缩写语列表和参考书目。

世界著名计算机教材精选

书　名：**计算机网络(第 4 版)** Computer Networks, 4E 著译者：Andrew S. Tanenbaum 著　潘爱民 等译 ISBN：7-302-08977-9 开　本：16 开 定　价：60.00 元	书　名：**TCP/IP 协议族(第 3 版)** TCP/IP Suite, 3E 著译者：Behrouz A. Forouzan 著　谢希仁 等译 ISBN：7-302-12753-0 开　本：16 开 定　价：98.00 元
书　名：**软件体系结构** Software architecture: perspective on an emerging discipline 著译者：Mary Shaw,David Garlan 著　牛振东 编译 ISBN：978-7-302-14550-9 开　本：16 开 定　价：29.80 元	书　名：**算法设计** Algorithm Design 著译者：Jon Kleinberg 著　张立昂 屈婉玲 译 ISBN：978-7-302-14335-2-9 开　本：16 开 定　价：75.00 元
书　名：**标准 C 程序设计(第 3 版)** Programming in ANSI C, 3E 著译者：E Balagurusamy 著　金名 等译 ISBN：7-302-12756-5 开　本：16 开 定　价：59.00 元	书　名：**Visual Basic 2005 程序设计(第 6 版)** An Introduction to Programming Using Visual Basic 2005, 6E 著译者：David Schneider 著　孙燕 等译 ISBN：978-7-302-14551-6 开　本：16 开 定　价：69.00 元
书　名：**计算机组织与体系结构：性能设计(第 7 版)** Computer Organization and Architecture, 7E 著译者：William Stallings 著　张昆藏 等译 ISBN：7-302-12444-2 开　本：16 开 定　价：66.00 元	书　名：**逻辑设计基础(第 2 版)** Introduction to Logic Design 著译者：Alan B. Marcovitz 著　殷洪玺 等译 ISBN：7-302-12491-4 开　本：16 开 定　价：58.00 元
书　名：**数据结构与算法分析** **——C++ 语言描述(第 2 版)** ADTs, Data Structures, and Problem Solving with C++, 2E 著译者：Larry Nyhoff 著　黄达明 等译 ISBN：7-302-13839-7 开　本：16 开 定　价：98.00 元	书　名：**面向对象软件工程：使用 UML、模式与 Java (第 2 版)** Object-Oriented Software Engineering, 2E 著译者：Bernd Bruegge, Allen H. Dutoit 著 叶俊民 等译 ISBN：7-302-13554-1 开　本：16 开 定　价：69.00 元
书　名：**Java 面向对象程序设计(第 2 版)** Introduction to Programming using Java, 2E 著译者：Arnow, Dexter, Weiss 著　郑莉 等译 ISBN：7-302-13510-X 开　本：16 开 定　价：69.00 元	书　名：**计算理论基础(第 2 版)** Elements of The Theory of Computation, 2E 著译者：Harry Lewis Christos Papadimitriou 著 张立昂 等译 ISBN：7-302-13288-7 开　本：16 开 定　价：29.80 元
书　名：**程序设计语言概念** Programming Language Concepts 著译者：John Mitchell 著　冯建华 等译 ISBN：7-302-11107-3 开　本：16 开 定　价：56.00 元	书　名：**3D 计算机图形学(OpenGL 版)** 3D Computer Graphics 著译者：Samuel R. Buss 著　唐龙 等译 ISBN：7-302-13604-1 开　本：16 开 定　价：45.00 元

书　名：**数字图像处理：原理与应用** Image Processing: Principles and Applications 著译者：Tinku Acharya 著　田浩 葛秀慧 等译 ISBN：978-7-302-15224-4 开　本：16 开 定　价：元	书　名：**网络安全：加密原理、算法与协议** Internet Security: Cryptographic, Principles, and Protocols 著译者：Man Yong Rhee 著　金名 张长富 等译 ISBN：978-7-302-15259-0 开　本：16 开 定　价：元
书　名：**无线通信与网络(第 2 版)** Wireless Communications and Networks, 2E 著译者：William Stallings 著　何军 等译 ISBN：7-302-11768-1 开　本：16 开 定　价：53.00 元	书　名：**数据通信——原理、技术与应用(第 5 版)** Business Data Communications, 5E 著译者：William Stallings 著　葛秀慧 等译 ISBN：7-302-11632-6 开　本：16 开 定　价：59.00 元
书　名：**操作系统原理** Operating Systems Principles 著译者：Bic, Shaw 著　梁洪亮 等译 ISBN：7-302-11602-4 开　本：16 开 定　价：50.00 元	书　名：**算法基础** Fundamentals of Algorithmics 著译者：Gilles Brassard, Paul Bratley 著　邱仲潘 等译 ISBN：7-302-10609-6 开　本：16 开 定　价：49.00 元
书　名：**密码学与网络安全** Cryptography and Network Security 著译者：Atul Kahate 著　邱仲潘 等译 ISBN：7-302-11490-0 开　本：16 开 定　价：43.00 元	书　名：**经典密码学与现代密码学** Classical and Contemporary Cryptology 著译者：Richard J. Spillman 著　叶阮健 等译 ISBN：7-302-10740-8 开　本：16 开 定　价：35.00 元
书　名：**Java 程序设计** Java Program Design 著译者：James Cohoon 著　黄晓彤 等译 ISBN：7-302-10638-X 开　本：16 开 定　价：88.00 元	书　名：**面向对象设计 UML 实践(第 2 版)** Practical Object-Oriented Design with UML, 2E 著译者：Mark Priestley 著　龚晓庆 等译 ISBN：7-302-10587-1 开　本：16 开 定　价：39.00 元
书　名：**数据挖掘教程** Data Mining: Introductory and Advanced Topics 著译者：Margaret H. Dunham 著　郭崇慧 等译 ISBN：7-302-10533-2 开　本：16 开 定　价：39.00 元	书　名：**数据结构与抽象(Java 语言版)** Data Structures and Abstractions with Java 著译者：Frank Carrano 著　严蔚敏 等译 ISBN：7-302-09375-X 开　本：16 开 定　价：89.00 元
书　名：**分布式系统原理与范例** Distributed Systems: Principles and Paradigms 著译者：Andrew S. Tanenbaum 著　杨剑铎 等译 ISBN：7-302-08961-2 开　本：16 开 定　价：68.00 元	书　名：**安腾体系结构—理解 64 位处理和 EPIC 原理** Itanium Architecture for Programmers: Understanding 64-Bit Processors and EPIC Principles 著译者：James S. Evans, Gregory L. Trimper 著 蒋敬旗 等译 ISBN：7-302-09608-2 开　本：16 开 定　价：49.8 元

书　名：**MPI 与 Open MP 并行程序设计：C 语言版** Parallel Programming: in C with MPI and OpenMP 著译者：Michael J. Qiunn 著　陈文光 等译 ISBN：7-302-09555-8 开　本：16 开 定　价：51.00 元	书　名：**计算机组成和设计硬件/软件接口(第 2 版)** Computer Organization and Design, 2E 著译者：Patterson, Hennessy 著　郑纬民 等译 ISBN：7-302-06901-8 开　本：16 开 定　价：76.00 元
书　名：**数据库管理系统原理与设计(第 3 版)** Database Management Systems, 3E 著译者：Raghu Ramakrishnan 著　周立柱 等译 ISBN：7-302-07939-0 开　本：16 开 定　价：69.00 元	书　名：**数据库系统基础教程** A First Course in Database Systems 著译者：史嘉权 等译 ISBN：7-302-03646-2 开　本：16 开 定　价：36.00 元
书　名：**面向对象系统分析与设计** Object-Oriented Systems Analysis and Design 著译者：周之英 等译 ISBN：7-302-02342-5 开　本：16 开 定　价：35.00 元	书　名：**通信网基本概念与主体结构** Communication Networks: Fundamental Concepts and Key Architectures 著译者：乐正友 等译 ISBN：7-302-06050-9 开　本：16 开 定　价：68.00 元
书　名：**数据结构 C++ 语言描述** Data Structures with C++ 著译者：刘卫东 等译 ISBN：7-302-03160-6 开　本：16 开 定　价：58.00 元	

目录