<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787302177159

10位ISBN编号：7302177155

出版时间：2008-9

出版时间：清华大学出版社

作者：刘嘉勇　主编；任德斌，胡勇，方勇　编著

页数：247

前言

现代密码技术已被广泛地应用到了信息技术的许多领域，是实现信息系统安全的关键技术之一，在保障网络信息安全的应用中具有重要地位。
现代密码技术的研究内容除传统的信息机密性保护技术外，还包括数字签名、报文与身份鉴别、密钥管理、安全协议等与信息安全密切相关的重要内容。
应用密码学已成为许多高等院校信息安全、通信工程、计算机科学、信息管理、电子商务等本科专业一门重要的专业基础课程及重要的教学内容。

针对高等院校信息技术类相关专业本科生所开设的课程特点，编者结合近几年在应用密码学方面的教学实践情况，广泛汲取了各类成功教材的有益经验，博采众家之长而精心编著了本教材。
在教材的体系构架和内容编排上以培养学生的密码技术应用能力为目标，突出教材的体系性和密码技术的实用性，尽量避免传统密码教材或专著注重密码学的数学原理和理论分析，而应用性偏弱的局限，并对一些需要数学知识可能过于深奥的知识点，如密码学的信息论基础、序列密码以及密码分析等内容进行了简化或忽略，重点选择一些具有典型意义和常用的密码体制和算法进行介绍，并在每章最后均配有思考题和习题以帮助学生对本章重要知识点的掌握和巩固。
使其更加易于课堂教学的实施和学生阅读，激发学生潜在的学习积极性。

本教材的主要特色：可读性强、结构合理、强调基础、注重应用，不求面面俱到，力求使学生能够较快掌握密码技术的核心内容。
在教材内容取舍、结构编排、密码算法选择及习题设计上尽量体现出广泛的代表性和典型性，做到教材内容主次分明、结构清晰、重点突出、逻辑性强，对知识点的阐述强调由浅人深、循序渐进，使教材具有显著的可读性和实用性。
可使读者能够在充分掌握密码学基础知识的同时，掌握应用密码技术，并将其尽快运用到实际工作中，是一本较为系统全面介绍密码学基本原理和典型应用的教材。
全书共分为10章，其具体章节内容安排如下。

第1章主要介绍密码学与信息安全、密码技术发展概况以及密码学的基本概念，包括密码学的任务、密码系统、密码系统攻击以及密码体制的分类等内容。

第2章介绍古典密码体制中的基本加密运算、几种典型的古典密码体制以及关于古典密码体制的基本破译方法。

<<应用密码学>>

内容概要

应用密码学是信息安全学科体系和信息系统安全工程的重要组成部分。
本书旨在从应用的角度系统介绍密码学的体系结构、基本原理和技术。
全书共分为10章，主要内容包括密码学概述、古典密码技术、分组密码体制、公钥密码体制、散列函数与报文鉴别、数字签名技术、密钥管理技术、身份鉴别技术、序列密码技术基础及密码技术应用等，并将与密码学密切相关的一些数学知识作为附录，以供需要的读者学习阅读。
每章最后均配有思考题和习题，以帮助读者掌握本章重要知识点并加以巩固。
　　本书可作为信息安全、计算机科学与技术、信息与计算科学、通信工程、信息管理以及电子商务等信息技术类本/专科专业密码学课程的教材，也可供初学密码学的研究生及从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

<<应用密码学>>

书籍目录

章节摘录

密码学概述　　1．1信息安全与密码技术　　密码技术是一门古老的技术，大概自人类社会出现战争便产生了密码（cipher）。
由于密码技术长期仅用于军事、政治、外交等要害部门的保密通信，使得密码技术的研究工作本身也是秘密进行的，因此密码学知识和相关技术主要掌握在军事、政治、外交等保密机关，难以公开发表。
然而，随着计算机科学技术、通信技术、微电子技术的发展，使得计算机和通信网络的应用进入了人们的日常生活和工作中，出现了电子政务、电子商务、电子金融等必须确保信息安全的网络信息系统，密码技术在信息安全中的应用不断得到发展，密码学也因此而脱去神秘的面纱从军事科学逐步走向商用，成为受到广泛关注的学科。
随着信息技术的发展和信息社会的来临，网络信息交换逐步已成为人们获取和交换信息的主要形式，信息安全变得越来越重要。
密码技术在解决网络信息安全中发挥着重要作用，信息安全服务要依赖各种安全机制来实现，而许多安全机制则需要依赖于密码技术。
使用密码技术不仅可以有效保障信息的机密性，而且可以保护信息的完整性和真实性，防止信息被篡改、伪造和假冒等。
因此，密码技术是信息安全的基础技术，而密码算法又是密码技术的核心，其重要性不言而喻。
可以说密码学贯穿于网络信息安全的整个过程，在解决信息的机密性保护、可鉴别性、完整性保护和信息抗抵赖性等方面发挥着极其重要的作用。
因此，密码学是信息安全学科建设和信息系统安全工程实践的基础理论之一。
密码技术已渗透到信息系统安全工程的多个领域和大部分安全技术或机制中。
可以毫不夸张地说，对密码学或密码技术一无所知的人不可能从技术层面上完全理解信息安全。
1.2密码技术发展简介　　密码技术源远流长，其起源可以追溯到几千年前的埃及、巴比伦、古罗马和古希腊。
早在4000多年以前，古埃及人就在墓志铭中使用过类似于象形文字那样奇妙的符号，这是史载的最早的密码形式。
古代密码虽然不是起源于战争，但其发展成果却首先被用于战争。
可以说，人类社会自从有了战争，有了保密通信的需求，就有了密码技术的研究和应用。
交战双方都为了保护自己的通信安全、窃取对方的情报而研究各种信息加密技术和密码分析技术。

<<应用密码学>>

编辑推荐

《应用密码学》简化或忽略过于深奥的知识点，如密码学的信息论基础，重点介绍具有典型意义和常用的密码体制及算法。

《应用密码学》各章最后均配有思考题和习题，以帮助学生掌握和巩固本章重要知识点，激发学生潜在的学习积极性。

《应用密码学》适于作为高等学校信息安全、通信工程、计算机科学与技术、信息管理、电子商务等专业的本科教材。

版权说明