<<密码学与信息安全技术>>

图书基本信息

书名：<<密码学与信息安全技术>>

13位ISBN编号：9787563519040

10位ISBN编号：7563519041

出版时间：2009-4

出版时间：北京邮电大学出版社

作者：罗守山 等编著

页数：384

前言

随着计算机网络的发展，特别是Internet的发展，我们的学习、工作、生活方式都发生了变化。
由于计算机系统的大量增加，人们越来越依赖这些系统，用它们来实现信息的存储与传输，同时也带来了新的需求，包括保证数据与资源不被泄露、保证数据与消息的真实性、保护系统不受攻击。
密码学与信息安全技术能够满足这些需求。
近年来，密码学与信息安全学科正在迅速发展与成熟，它们能够提供很多安全应用的解决方案。
本书介绍了密码学与信息安全技术的基本理论和基本方法。
本书的结构安排如下。
第1章“密码学与网络安全基础”介绍了密码学的数学基础、信息论基础和计算复杂性基础，同时还介绍了密码学与信息安全技术的基础知识。
第2章“现代密码学加密算法与协议”介绍了重要的对称密码体制与非对称密码体制，同时还介绍了密码协议的知识，并将针对密码协议研究中的一个热点问题一安全多方计算协议——作比较详细的论述。
第3章“信息认证与身份识别”介绍了杂凑函数、数字签名和身份识别协议等内容。

<<密码学与信息安全技术>>

内容概要

本书是在作者多年的教学与科研实践的基础上编写的。
本书系统地介绍了密码学与信息安全技术的基本原理和方法。
本书的内容包括密码学与网络安全基础、现代密码学加密算法与协议、信息认证与身份识别、密钥管理、访问控制、网络攻击、防火墙和虚拟专用网等内容。
　本书可作为计算机、通信、信息安全等专业的本科生教材，也可供从事相关专业的教学、科研人员和工程技术人员参考。

<<密码学与信息安全技术>>

书籍目录

章节摘录

插图：第1章 密码学与网络安全基础The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message Selected at another point. Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem.——O.E.SHANNON，1948通信的基本问题是：通信的一方选择一条信息，另一方能够将其精确地(或近似地)恢复出来。
通常，这些信息是有含义的，它们与某些物理或概念的实体有关。
通信的语义方面与工程问题不相关。
——香农，1948信息安全已经成为一个全社会关注的问题。
密码学与网络安全和国家的政治安全、经济安全、社会稳定以及人们的日常生活密切相关。
从技术角度看，密码学与网络安全是一个涉及计算机科学、网络技术、通信技术、密码技术、应用数学、信息论等多知识、边缘性的综合学科，其重要性有目共睹。
特别是随着全球信息基础设施的建立与形成，网络化、信息化已经成为现代社会的一个重要特征。
应用密码技术，提供这些信息基础设施的安全保障机制是社会发展的需要。
本章介绍密码学的数学基础、信息论基础、计算复杂性基础，同时还将介绍密码学与网络安全的一些基础知识。
1.1 密码学的数学基础在现代密码学中需要使用许多的数学理论。
例如，近世代数、数论、组合论、概率论及线性代数等，这些数学理论均为设计密码系统及协议不可或缺的工具。
本节将对现代密码学中必要的数学基础作一重点整理。
同时。
也简单地介绍一些应用实例，一方面能够使读者了解所学的数学知识在密码学与网络安全中的应用，另一方面也可以将这些应用实例作为背景，帮助读者更好地理解这些抽象的数学知识。

编辑推荐

《密码学与信息安全技术》为普通高等教育“十一五”国家级规划教材之一。

<<密码学与信息安全技术>>

版权说明