

《计算机信息安全》

图书基本信息

书名：《计算机信息安全》

13位ISBN编号：9787113070816

10位ISBN编号：7113070817

出版时间：2006-8

出版社：中国铁道

作者：印润远

页数：213

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《计算机信息安全》

内容概要

本书主要内容包括：计算机信息系统安全概述、信息论与数学基础、信息加密技术与应用、数字签名技术与应用、黑客行径概述、鉴别与防御“黑客”入侵、防火墙技术与预防病毒。本书具有很强的实用性和指导性，内容新颖，通俗易懂。在阐述基本理论和、基本方法的同时，力求实用和可操作。

书籍目录

第1章 计算机信息系统安全概述	1.1 计算机信息系统及其安全的基本概念	1.1.1 计算机信息系统	1.1.2 计算机信息系统安全	1.2 计算机信息系统面临的威胁及其脆弱性	1.2.1 计算机信息系统面临的威胁	1.2.2 计算机信息系统受到的威胁和攻击	1.2.3 计算机信息系统的脆弱性	1.3 计算机信息系统安全保护概述	1.3.1 计算机信息系统安全保护的基本概念	1.3.2 计算机信息系统保护的基本目标和任务	1.4 我国计算机信息系统安全保护的基本政策	1.4.1 我国信息化建设的总指导方针	1.4.2 计算机信息系统保护的基本原则	1.4.3 我国信息系统安全保护的总政策	1.5 计算机安全监察	1.5.1 计算机信息系统的安全监督检查的总体目标	1.5.2 计算机安全监察工作指导方针	1.5.3 实施安全监督检查	1.5.4 计算机安全监察的业务范围																				
思考题	第2章 信息论与数学基础	2.1 信息论	2.1.1 熵和不确定性	2.1.2 语言信息率	2.1.3 密码体制的安全性	2.1.4 唯一解距离	2.1.5 信息论的运用	2.1.6 混乱和散布	2.2 复杂性理论	2.2.1 算法的复杂性	2.2.2 问题的复杂性	2.2.3 NP-完全问题	2.3 数论	2.3.1 模运算	2.3.2 素数	2.3.3 最大公因子	2.3.4 取模数求逆元	2.3.5 费马小定理	2.3.6 欧拉函数	2.3.7 中国剩余定理	2.3.8 二次剩余	2.3.9 勒让德符号	2.3.10 雅可比符号	2.3.11 Blum整数	2.3.12 生成元	2.3.13 有限域	2.3.14 GF (pm)上的计算	2.4 因子分解	2.4.1 因子分解算法	2.4.2 模n的平方根	2.5 素数生成元	2.5.1 Solovag-Strassen方法	2.5.2 Rabin-Mi11ei方法	2.5.3 lehmann方法	2.5.4 强素数	2.6 有限域上的离散对数	2.6.1 离散对数基本定义	2.6.2 计算有限群中的离散对数	思考题
第3章 信息加密技术与应用	3.1 网络通信中的加密方式	3.1.1 链路-链路加密	3.1.2 节点加密	3.1.3 端一端加密	3.1.4 ATM网络加密	3.1.5 卫星通信加密	3.1.6 加密方式的选择	3.2 分组加密与高级加密标准	3.2.1 分组密码与DES	3.2.2 21世纪高级加密标准	第4章 数字签名技术与应用	第5章 黑客行径概述	第6章 鉴别与防御“黑客”入侵	第7章 入侵检测	第8章 防火墙技术	第9章 预防病毒	第10章 身份认证与访问控制	第11章 信息隐藏技术	第12章 计算机信息系统安全法律与规范																			

《计算机信息安全》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com