

<<信息隐藏>>

#### 图书基本信息

书名：<<信息隐藏>>

13位ISBN编号：9787302119258

10位ISBN编号：7302119252

出版时间：2006-3

出版时间：清华大学出版社

作者：王育民

页数：245

字数：337000

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：<http://www.tushu007.com>

## <<信息隐藏>>

### 内容概要

本书介绍信息隐藏理论与技术的基本知识，包括密码学基础、隐写术、隐信道、阙下信道、隐匿签字、匿名通信、加密和数字水印等有关技术。

随着信息化社会的发展，信息隐藏技术将在很多领域（如在电子政务、电子商务系统的信息安全方面）得到广泛应用。

本书可作为通信工程、计算机应用、信号与信息处理、信息安全和密码学等专业的大学生和研究生的教材，以及信息安全部门的专业技术人员和计算机网络安全产品研发人员的参考书。

#### 作者简介

王育民，西安电子科技大学教授，博士生导师，中国电子学会和中国通信学会会士、中国密码学会理事、中国电子学会信息论学会委员、中国自然科学基金研究会会员、IEEE高级会员。主要研究方向为通信理论、信息论、编码和密码学。已在国内外学术刊物和会议上发表论文200余篇。

## 书籍目录

第1章 密码学——信息保密、认证和完整性技术 1.1 信息化社会中的信息安全的重要性 1.1.1 信息化社会的发展 1.1.2 信息化社会的特点 1.1.3 信息化社会中网络安全的严峻形势 1.1.4 信息战 1.1.5 信息化社会中信息安全的特点 1.1.6 信息产业的出现 1.1.7 结论 1.2 密码学基本概念 1.2.1 保密与保密系统 1.2.2 认证与认证系统 1.2.3 完整性 1.2.4 密码体制的种类 1.3 单钥密码体制 1.3.1 流密码 1.3.2 分组密码 1.4 双钥密码体制 1.4.1 双钥密码概述 1.4.2 RSA密码体制 1.4.3 ElGamal密码体制 1.4.4 椭圆曲线密码体制 1.5 数据的完整性 1.5.1 杂凑函数 1.5.2 MD-4和MD-5杂凑算法 1.5.3 安全杂凑算法 1.6 认证与身份证明 1.6.1 身份证明系统的组成和要求 1.6.2 身份证明的基本分类 1.6.3 实现身份证明的基本途径 1.6.4 个人特征的身份证明技术 1.6.5 零知识证明的基本概念 1.7 安全协议 1.7.1 协议的基本概念 1.7.2 基本密码协议分类 1.7.3 密钥建立协议 1.7.4 认证协议 1.7.5 消息认证 1.7.6 实体认证协议 1.7.7 Kerberos协议 1.8 时戳业务 1.8.1 仲裁方案 1.8.2 链接协议 1.8.3 分布式协议 1.9 信息安全基础设施建设 1.9.1 信息安全基础设施建设的内容 1.9.2 信息安全基础设施建设的目标 参考文献第2章 隐写术——信息隐藏技术原理 2.1 引言 2.2 信息隐藏技术的分类及基本要求 2.2.1 信息隐藏技术分类 2.2.2 信息隐藏技术的基本要求 2.3 信息隐藏的基本原理和模型 2.4 信息隐藏的基本方法 .....第3章 阙下信道——阙下传信技术（一）：对检查者隐匿消息的技术第4章 隐信道——阙下传信技术（二）：对检查者隐匿路由的技术第5章 隐匿签字——盲签字技术：对签字者隐匿身份信息的技术第6章 隐匿通信——不可追踪技术第7章 加密技术——数字版权保护技术（一）第8章 数字水印——数字版权保护技术（二）

<<信息隐藏>>

#### 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:<http://www.tushu007.com>