

<<应用编码与计算机密码学>>

图书基本信息

书名：<<应用编码与计算机密码学>>

13位ISBN编号：9787302112181

10位ISBN编号：7302112185

出版时间：2005-11

出版时间：清华大学

作者：龙冬阳

页数：284

字数：427000

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>

## <<应用编码与计算机密码学>>

### 内容概要

本书从编码理论与信息论的角度系统地阐述了计算机密码学研究的核心内容，首先介绍了变长编码理论的若干基本概念，讨论信息熵、信源编码和数据压缩方法等问题，然后详细描述了传统的古典密码体制、迭代码全制、数据加密标准DES、高级加密标准AES、公钥密码体制、Hash函数、数字签字、密钥管理及安全协议等内容，最后简单介绍了量子密码学的基本概念。

为了便于选用本书作为教材或教学参考书的读者进行自学，随同本书提供了相关的素材文件，读者可以通过访问<http://www.tupwk.com.cn/downpage>或<http://infosec.sysu.edu.cn>下载。

其中包括了我们教学过程中许多本科生或研究生所做的课程设计内容，如用Visual C++或Java等语言工具实现的DES, AES, RSA, MD5, SHA1等典型密码算法等。

本书可用作计算机科学与工程、信息系统管理、数字与通信等相关专业本科生或低年级研究生计算机密码学课程的教材或教学参考书，同时也可供从事信息处理、计算机网络与信息安全等专业的工程技术人员参考使用。

## &lt;&lt;应用编码与计算机密码学&gt;&gt;

## 书籍目录

第1章 变长码概述 1.1 字与语言 1.2 惟一可分码与McMillan定理 1.3 前缀码与Kraft定理 1.4 应用编码的三个基本目标 1.5 练习

第2章 熵与数据压缩 2.1 熵 2.1.1 离散信源的熵 2.1.2 条件熵 2.1.3 熵的链规则 2.2 最优信源编码 2.2.1 最优信源编码 2.2.2 比较熵与交互信息量 2.2.3 编码与数据加密 2.3 霍夫曼编码 2.4 字典方法与LZ编码 2.4.1 字典方法 2.4.2 LZ77初步 2.5 算术编码 2.5.1 渐进均匀分布 2.5.2 算术编码 2.6 练习

第3章 Shannon理论与密码学 3.1 古典密码体制 3.1.1 基本概念 3.1.2 移位密码 3.1.3 维吉尼亚密码 3.1.4 置换密码 3.1.5 替代(代换)密码 3.1.6 分组密码与流密码 3.2 密码体制分析 3.3 “好”密码体制的若干特性 3.3.1 Shannon标准 3.3.2 混淆与扩散 3.3.3 完善保密性 3.3.4 冗余度与惟一解距离 3.3.5 乘积密码 3.3.6 编码与密码体制 3.4 练习

第4章 分组密码 4.1 替代-置换网格 4.2 Feistel密码结构 4.3 数据加密标准 4.3.1 DES算法描述 4.3.2 DES安全分析 4.3.3 DES的工作模式 4.4 高级加密标准 4.4.1 AES中一些数学基础 4.4.2 AES加密算法 4.4.3 AES安全分析 4.5 练习

第5章 公钥密码体制 5.1 公钥密码的基本思想 RSA公钥密码体制 5.2.1 与RSA相关的若干数学基础 5.2.2 RSA密码体制描述 5.2.3 RSA的实现 5.2.4 RSA的安全性分析 5.3 基于离散对数的公钥密码体制 5.3.1 离散对数 5.3.2 Diffie-Hellman算法 5.3.3 ElGamal密码体制 5.4 椭圆曲线密码体制 5.4.1 椭圆曲线的若干基本概念 5.4.2 椭圆密码体制的实现 5.5 McEliece系统 5.6 一个基于L系统的公钥密码系统 5.6.1 同态 5.6.2 L系统简介 5.6.3 同态的迭代与DOL, DTOL 5.6.4 基于同态的迭代(L系统)的公钥密码 5.6.5 密码体制的实现 5.6.6 密码体制的评价与探讨 5.7 练习

第6章 散列函数 6.1 散列函数概述 6.1.1 定义 6.1.2 构造散列函数 6.1.3 散列函数的安全性 MD5算法 6.3 SHA-1算法 6.3.1 SHA-1算法描述 6.3.2 SHA-1算法分析 6.4 消息认证码 6.4.1 HMAC描述 6.4.2 HMAC安全性 6.5 练习

第7章 数字签名 7.1 基本概念 7.2 签名方案攻击 7.3 签名方案与函数 7.4 ElGamal签名 7.4.1 签名描述 7.4.2 ElGamal签名和安全性 7.5 ElGamal签名方案的变体 7.5.1 Schnorr签名 7.5.2 DSA算法 7.5.3 椭圆曲线数字签名 7.6 几种特殊的数字签名 7.6.1 一次签名 7.6.2 不可否认的签名 7.6.3 盲签名(Blind Signature) 7.6.4 具有恢复消息功能的数字签名 7.6.5 基于RSA的带门限的代理签名 7.7 练习

第8章 密钥分配与管理 8.1 密钥的基本概念 8.2 密钥分配 8.2.1 应用对称密码体制的密钥分配 8.2.2 应用公钥密码体制的密钥分配 8.2.3 公钥密码体制中的密钥分配 8.3 公钥基础设施 8.3.1 PKI的组成 8.3.2 证书 8.3.3 证书认证系统 8.4 密钥托管技术 8.4.1 密钥托管的概念 8.4.2 常用的密钥托管技术 8.5 练习

第9章 密码协议 9.1 基本协议 9.1.1 密钥交换 9.1.2 鉴别 9.1.3 鉴别和密钥交换 9.1.4 多密钥公开密钥密码 9.1.5 秘密分割 9.1.6 秘密共享 9.1.7 数据库的密码保护 9.2 应用 9.2.1 加密的数字签名 9.2.2 通用电子支付系统 9.2.3 ISO鉴别框架中的鉴别协议 9.3 典型协议 9.3.1 Shamir协议 9.3.2 智力扑克 9.3.3 抛硬币游戏 9.3.4 不经意传输 9.3.5 电子投票协议 9.4 零知识证明 9.4.1 基本概念 9.4.2 零知识证明的例子 9.4.3 身份的零知识证明 9.5 练习

第10章 量子密码学入门 10.1 研究背景 10.2 量子密码保密的物理基础 10.2.1 量子态和Hilbert空间 10.2.2 与保密通信相关的量子力学基本原理 10.3 量子密钥分配基本协议 10.3.1 无噪声的BB84协议 10.3.2 有噪声的BB84协议 10.3.3 B92协议 10.3.4 协议的安全性分析 10.4 量子密码学现状与未来 10.4.1 面临的挑战 10.4.2 前景及未来 10.5 练习参考文献

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>