

<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787030106070

10位ISBN编号：7030106075

出版时间：2002-7-1

出版时间：科学出版社

作者：沈世镒,陈鲁生

页数：156

字数：197000

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>

<<现代密码学>>

内容概要

本书系统地介绍现代密码学的基本内容，取材具有典型性，全书共分9章，第1章介绍密码学中的一些基本概念，第2章介绍古典密码的加密方法和一些典型的古典密码体制，第3章介绍Shannon的密码学理论，第4章和第5章分别讨论分组密码和公钥密码，第6章介绍序列密码和线性移位寄存器序列。第7章和第8章分别讨论数字签名和Hash函数，第9章介绍一些重要的密码协议，本书每章末均附有习题，其中有些习题是对正文内容的补充，以供学生复习巩固书中所学内容。

本书可作为高等院校信息科学专业或其他相关专业本科生的教材。
也可作为相关领域中的教学、科研人员以及工程技术人员的参考书。

<<现代密码学>>

书籍目录

第1章 引言 1.1 密码学的发展概况 1.2 密码学的基本概念第2章 古典密码 2.1 古典密码中的基本加密运算 2.1.1 单表古典密码中的基本加密运算 2.1.2 多表古典密码中的基本加密运算 2.2 几种典型的古典密码体制 2.2.1 几种典型的单表古典密码体制 2.2.2 几种典型的多表古典密码体制 2.3 古典密码的统计分析 2.3.1 单表古典密码的统计分析 2.3.2 多表古典密码的统计分析 习题第3章 Shannon理论 3.1 密码体制的数学模型 3.2 熵及其性质 3.3 伪密钥和惟一解距离 3.4 密码体制的完善保密性 3.5 乘积密码体制 习题第4章 分组密码 4.1 分组密码的基本原理 4.2 数据加密标准DES 4.2.1 DES加密算法 4.2.2 DES的解密过程 4.2.3 DES的安全性 4.3 多重DES 4.3.1 双重DES 4.3.2 三重DES 4.4 DES的工作模式 4.5 高级加密标准AES 4.5.1 AES的数学基础 4.5.2 AES的输入输出和中间状态 4.5.3 AES的加密过程 4.5.4 密钥扩展 4.5.5 AES的解密过程 习题第5章 公钥密码 5.1 公钥密码的理论基础 5.2 RSA公钥密码 5.2.1 基本的数论知识 5.2.2 RSA公钥密码体制 5.2.3 RSA的安全性讨论 5.2.4 模 n^2 求逆的算法 5.2.5 模 n^2 的大数幂乘的快速算法 5.2.6 因子分解 5.3 大素数的生成 5.3.1 素数的分布 5.3.2 Legendre符号和Jacobi符号 5.3.3 Solovay Strassen素性测试法 5.3.4 Miller Rabin素性测试法 5.4 ElGamal公钥密码 5.4.1 ElGamal公钥密码体制 5.4.2 ElGamal公钥密码体制的安全性 5.4.3 有限域上离散对数的计算方法 5.5 椭圆曲线上的Menezes—Vanstone公钥密码 5.5.1 有限域上的椭圆曲线 5.5.2 Menezes-Vanstone公钥密码体制. 习题第6章 序列密码与移位寄存器 6.1 序列密码的基本原理 6.2 移位寄存器与移位寄存器序列 6.3 线性移位寄存器的表示 6.4 线性移位寄存器序列的周期性 6.5 线性移位寄存器的序列空间 6.6 线性移位寄存器序列的极小多项式第7章 数字签名 第8章 Hash函数第9章 密码协议主要参考文献

<<现代密码学>>

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>