

<<密码学与编码理论>>

图书基本信息

书名：<<密码学与编码理论>>

13位ISBN编号：9787115174352

10位ISBN编号：7115174350

出版时间：2008-4

出版时间：人民邮电

作者：王鹏

页数：300

译者：王全龙,王鹏,林昌露

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>

<<密码学与编码理论>>

内容概要

本书是密码学方面的经典著作，是作者对其多年教学经验的总结。

书中主要内容包括数论、数据加密标准（DES）、高级加密标准Rijndael、RSA算法、离散对数、散列函数、信息论、格方法、纠错码以及量子密码等，其中许多内容都反映了业内的新进展。

本书配有大量实例、习题以及用Mathematica（r）、Maple（r）、MATLAB（r）编写的上机练习。

本书可作为高等院校相关专业密码学、通信安全和网络安全等课程的教材或参考书，也可供计算机工程技术人员参考。

<<密码学与编码理论>>

书籍目录

第1章 密码学及其应用概述1.1 安全通信1.1.1 可能的攻击1.1.2 对称和公钥算法1.1.3 密钥长度1.2 密码学应用第2章 传统密码系统2.1 移位密码2.2 仿射密码2.3 维吉内尔密码2.3.1 算出密钥长度2.3.2 算出密钥的第一种方法2.3.3 算出密钥的第二种方法2.4 替换密码2.5 夏洛克·福尔摩斯2.6 Playfair和ADFGX密码2.7 分组密码2.8 二进制数和ASCII码2.9 一次一密2.10 伪随机序列的生成2.11 线性反馈移位寄存序列2.12 Enigma密码机习题上机练习第3章 基本数论3.1 基本概念3.1.1 整除性3.1.2 素数3.1.3 最大公因子3.2 求解 $ax + by = d$ 3.3 同余式3.3.1 除法3.3.2 使用分式3.4 中国剩余定理3.5 模指数3.6 费马小定理和欧拉定理3.7 本原根3.8 矩阵模 n 取逆3.9 模 n 平方根3.10 勒让德和雅可比符号3.11 有限域3.11.1 除法3.11.2 $GF(28)$ 3.11.3 线性移位寄存器序列3.12 连分数习题上机练习第4章 数据加密标准4.1 引言4.2 DES算法的简化版4.3 差分密码分析4.3.1 3轮的差分密码分析4.3.2 4轮的差分密码分析4.4 DES4.5 工作模式4.5.1 电子密码本4.5.2 密码分组链接4.5.3 密码反馈4.5.4 输出反馈4.5.5 计数器4.6 破解DES4.7 中间相遇攻击4.8 口令安全习题上机练习第5章 高级加密标准: Rijndael5.1 基本算法5.2 层的描述5.2.1 ByteSub变换5.2.2 ShiftRow变换5.2.3 MixColumn变换5.2.4 AddRoundKey变换5.2.5 密钥扩展方案5.2.6 S盒的构成5.3 解密算法5.4 设计中的考虑习题第6章 RSA算法第7章 离散对数第8章 散列函数第9章 数字签名 1459.1 RSA签名方案第10章 安全协议第11章 数字现金第12章 秘密分享方案第13章 游戏第14章 零知识技术第15章 信息论第16章 椭圆曲线第17章 格方法第18章 纠错码第19章 密码学中的量子技术附录A附录B附录C推荐阅读参考文献索引

<<密码学与编码理论>>

编辑推荐

《密码学与编码理论(第2版)》可作为高等院校相关专业密码学、通信安全和网络安全等课程的教材或参考书，也可供计算机工程技术人员参考。

<<密码学与编码理论>>

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>