

<<信息安全数学基础>>

图书基本信息

书名：<<信息安全数学基础>>

13位ISBN编号：9787307052345

10位ISBN编号：7307052342

出版时间：2006-9

出版时间：武汉大学出版社

作者：李继国、余纯武、张福泰、马春光

页数：210

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>

<<信息安全数学基础>>

内容概要

本书全面系统地介绍了数论、代数、组合数学等相关基础理论和密码学研究中用到的一些实用算法。包括整除、同余、二次同余式与平方剩余、原根、群、环、有限域、格及其应用、椭圆曲线、组合数学等数学知识以及素性测试、因数分解和离散对数计算等一些实用算法，共13章。

书末列出了主要参考文献。

本书可作为信息安全、计算机科学与技术、通信工程、数学与应用数学等专业本科生和研究生的教材，也可供从事信息安全、密码学和其他信息技术工作的科研和工程技术人员参考。

书籍目录

第1章 整除 1.1 整除的基本性质和余数定理 1.2 最大公因数和最小公倍数 1.3 算术基本定理
1.4 实验 1.5 习题第2章 同余 2.1 同余的定义和基本性质 2.2 剩余类与剩余系 2.3 几个著名定理 2.4 RSA公开密钥密码系统 2.4.1 密钥的产生 2.4.2 RSA系统 2.4.3 RSA的安全性
2.4.4 RSA参数的选择 2.5 同余式 2.6 一次同余式 2.7 中国剩余定理 2.8 高次同余式的解法和解数 2.9 模为素数的高次同余式的求解 2.10 实验 2.11 习题第3章 二次同余式与平方剩余 3.1 二次同余式与平方乘余的概念 3.2 模为奇素数的平方剩余与平方非剩余 3.3 勒让德符号 3.4 雅可比符号 3.5 模 P 平方根 3.6 模为合数的情形 3.7 实验 3.8 习题第4章 原根 4.1 指数及其基本性质 4.2 原根及其计算 4.3 指标及 n 次剩余 4.4 实验 4.5 习题第5章 群 5.1 准备知识 5.1.1 二元运算的概念 5.1.2 二元运算的性质 5.1.3 代数系统的定义 5.2 群的定义与性质 5.2.1 群的定义 5.2.2 群中元素的阶 5.2.3 子群及子群的判定 5.3 同态和同构 5.3.1 同态、同构的定义 5.3.2 同态的性质 5.4 循环群和置换群 5.5 群的应用 5.6 习题第6章 环 6.1 环的定义和性质 6.2 整环和域 6.3 环的应用 6.3.1 非负整数环中的幂等元素及其性质 6.3.2 基于幂等元素加密算法的实现 6.3.3 加密算法举例 6.4 习题第7章 有限域理论 7.1 域的扩张 7.2 有限域的基本概念与性质 7.3 最小多项式与本原多项式 7.4 多项式的周期.....第8章 格及其应用第9章 椭圆曲线第10章 组合数学第11章 素性测试第12章 因数分解第13章 离散对数计算附录参考文献

<<信息安全数学基础>>

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>