

<<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：9787115156624

10位ISBN编号：711515662X

出版时间：2007-4

出版单位：人民邮电

作者：裴定一,徐详

页数：171

字数：275000

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

数学是信息的保密技术和认证技术的理论基础。

本书介绍与数学在这个领域中的应用密切相关的一些基础知识，主要包括整数的算术，连分数，群、环、域的概念，多项式，有限域，波尔函数，图论，计算复杂度等内容。

在介绍这些数学知识的同时，举例介绍了它们在信息安全领域的一些应用。

通过这些应用实例，也有利于帮助读者理解这些抽象的数学理论。

本书可作为信息安全专业及相关的数学和信息科学专业的本科教材。

<<信息安全数学基础>>

书籍目录

第1章 整数的因子分解 1.1 带余除法和整除法 1.2 整数的表示 1.3 最大公因子与辗转相除法 1.4 整数的唯一分解定理 1.5 素数 1.6 多项式的整除法 习题第2章 同余式 2.1 中国剩余定理 2.2 剩余类环 2.3 同余方程 2.4 原根 2.5 RSA公钥密码体制 习题第3章 二次剩余 3.1 Legendre符号及Euler判别法则 3.2 二次互反律 3.3 Jacobi符号和二次剩余问题 习题第4章 不定方程 4.1 一次不定方程 4.2 二次不定方程 习题第5章 连分数 5.1 简单连分数 5.2 用连分数表实数 5.3 连分数因子分解算法 5.4 连分式 5.5 连分式和线性递归序列 习题第6章 群 6.1 群的定义 6.2 群的乘法表 6.3 变换群、置换群 6.4 等价关系、子群的陪集分解 6.5 正规子群、商群、同态 6.6 循环群 习题第7章 环 7.1 环的定义 7.2 子环、理想和商环 7.3 多项式环 习题第8章 域 8.1 分式域 8.2 素域 8.3 单扩张 8.4 代数扩张 8.5 二次域 8.6 多项式的分裂域 习题第9章 有限域 9.1 有限域的刻画 9.2 分圆多项式 9.3 有限域中元素的表示方法 9.4 有限域中的开平方算法 9.5 有限域中离散对数 9.6 有限域在编码和密码中的应用举例 习题第10章 组合电路与布尔代数 10.1 组合电路 10.2 布尔代数 习题第11章 布尔函数 11.1 布尔函数的表示方法 11.2 非线性度 11.3 相关免疫性 11.4 严格雪崩准则和扩散准则 习题第12章 图论 12.1 基本概念 12.2 连通性 12.3 图的矩阵表示 12.4 树 12.5 欧拉图与哈密顿图 12.6 M序列与德布鲁恩-古德图 习题第13章 计算复杂度 13.1 算法复杂度 13.2 图灵机与确定多项式时间 13.3 非确定多项式时间 13.4 概率多项式时间 习题 中文名词索引 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>