第一图书网, tushu007.com

<<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：9787310025305

10位ISBN编号：731002530X

出版时间：2006-5

出版时间：南开大学出版社

作者：贾春福

页数：197

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

本书系统地介绍了信息安全理论与技术所涉及的数论、代数、椭圆曲线等数学理论基础。
全书共分为5章：第1章是预备知识，介绍了书中内容所涉及的基础知识；第2章是数论基础，包括整数的因子分解，同余式，原根，二次剩余，连分数和素性检验等内容；第3章是代数系统基础，包括代数系统的基本概念，群、环、域的概念，一元多项式环和有限域理论初步等内容；第4章是椭圆曲线，包括椭圆曲线的预备知识，椭圆曲线，椭圆曲线上的离散对数等内容；第5章是反馈移位寄存器，包括反馈移位寄存器，分圆和本原多项式，m序列等内容。
书中每章末都配有习题，以供学生学习和复习巩固所学内容。
　　本书是高等学校信息安全专业本科生的教材，也可作为信息科学技术类专业(如计算机科学技术、通信工程和电子科学技术等)本科生和研究生的教材，还可以供从事信息安全和其他信息技术工作的人员参考。

<<信息安全数学基础>>

书籍目录

第1章 预备知识　1.1 集合论基础　1.1.1 集合　1.1.2 关系　1.1.3 函数　1.1.4 基数　1.2 排列与组合　1.2.1 基本计数原理　1.2.2 排列　1.2.3 组合　1.3 生成函数　1.3.1 生成函数的定义　1.3.2 生成函数的性质　1.3.3 生成函数的一个应用——整数拆分　习题第2章 数论基础　2.1 整数的因子分解　2.1.1 整除与素数　2.1.2 辗转相除法　2.1.3 唯一分解定理　2.1.4 完全数、梅森素数和费马素数　2.2 同余式　2.2.1 同余的定义和基本性质　2.2.2 剩余类和完全剩余系　2.2.3 欧拉函数与缩系　2.2.4 同余方程　2.2.5 孙子定理　2.2.6 高次同余方程　2.3 原根　2.3.1 整数的次数　2.3.2 原根　2.3.3 指数　2.3.4 n次剩余　2.4 二次剩余　2.4.1 二次剩余　2.4.2 勒让德符号　2.4.3 雅可比符号　2.5 连分数　2.5.1 连分数的基本性质　2.5.2 简单连分数　2.6 素性检验　2.6.1 素性检验和伪素数　2.6.2 强伪素数　习题第3章 代数系统基础　3.1 代数系统的基本概念　3.1.1 代数系统　3.1.2 同构与同态　3.2 群　3.2.1 半群　3.2.2 群和子群　3.2.3 陪集和商群　3.2.4 循环群　3.3 环和域的概念　3.3.1 环　3.3.2 域　3.3.3 理想和商环　3.3.4 整环的分式域　3.4 一元多项式环　3.4.1 一元多项式环的概念　3.4.2 一元多项式的整除　3.4.3 一元多项式环的理想　3.4.4 一元多项式的同余与商环　3.4.5 域上一元多项式唯一分解定理　3.4.6 多项式不可约性检验　3.5 有限域理论初步　习题第4章 椭圆曲线　4.1 椭圆曲线的预备知识　4.1.1 仿射平面和射影平面　4.1.2 判别式、结式和代数不变量　4.1.3 一元三次方程的公式解——Cartan公式　4.2 椭圆曲线　4.2.1 Weierstrass方程　4.2.2 椭圆曲线　4.2.3 椭圆曲线上点的加法群　4.2.4 有限域上的椭圆曲线　4.3 椭圆曲线与离散对数　4.3.1 有限域上的离散对数　4.3.2 椭圆曲线上的离散对数　习题第5章 反馈移位寄存器　5.1 反馈移位寄存器　5.1.1 反馈移位寄存器　5.1.2 线性反馈移位寄存器(LFSR)　5.1.3 非线性组合移位寄存器简介　5.2 分圆多项式和本原多项式　5.2.1 分圆多项式　5.2.2 本原多项式　5.3 m序列　5.3.1 LFSR的特征多项式　5.3.2 m序列的产生条件　5.3.3 m序列的特点　5.3.4 m序列的破译　习题主要参考文献

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