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：9787512100565

10位ISBN编号：7512100566

出版时间：2010-3

出版时间：贾春福、钟安鸣、 赵源超 清华大学出版社，北京交通大学出版社 (2010-03出版)

作者：贾春福，等 编

页数：212

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

第一图书网, tushu007.com

前言

计算机与网络技术的飞速发展和广泛应用，极大地促进了社会的发展，也极大地改变了人们的生活和工作方式。
与此同时，信息安全问题也更多地受到关注：信息安全理论与技术已经成为信息科学与技术中极为重要的研究领域；信息安全专门人才的培养受到了社会空前的重视。
“信息安全数学基础”是新兴的信息安全专业本科的专业基础课，对信息安全理论和技术的深入学习具有重要的意义。
本书是在南开大学信息安全专业“信息安全数学基础”课程授课讲义的基础上整理而成的。
全书共分为6章：第1章是预备知识，介绍了书中所涉及的基础知识；第2章和第3章是数论基础，包括整数的因子分解、同余式、原根、二次剩余和数论的应用等内容；第4章是代数系统，包括群、环、域的概念，一元多项式环和有限域理论初步等内容；第5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6章是线性反馈移位寄存器，包括反馈移位寄存器、分圆多项式和本原多项式、m序列等内容。
书中每章末都配有适量的习题，供学生在学习和复习巩固书中所学内容时使用。
本书内容的选取，我们参照了“信息安全类专业指导性专业规范”中对“信息安全数学基础”相关教学内容和要求的阐述；并将多年来积累的实际教学经验融入其中，力求知识系统化、较好地覆盖信息安全领域所涉及的数学基础知识。
对书中内容所涉及的基础预备知识作了简明扼要的介绍；书中所涉及的数学结论都给出了详细的证明；习题的配置着力于帮助学生巩固所学的内容和能力拓展。
本书适合高等学校信息安全、计算机科学技术和通信工程等专业本科生和研究生使用，也可供相关领域的科研人员和技术人员参考。
本书由贾春福、钟安鸣、赵源超等编写，最后由贾春福统稿。
王冬、刘昕海等对书中的内容进行了校对，在此表示感谢。
另外，本书是南开大学教材资助项目，在此也表示衷心的感谢。
由于时间仓促，书中难免有疏漏和不当之处，敬请读者批评指正。

第一图书网, tushu007.com

<<信息安全数学基础>>

内容概要

《信息安全数学基础》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6章：第1章是预备知识，介绍了书中后面几章所涉及的基础知识；第2章和第3章是数论基础，包括整数的因子分解、同余式、原根、二次剩余、数论的应用等内容；第4章是代数系统，包括群、环、域的概念，一元多项式环和有限域理论初步等内容；第5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6章是线性反馈移位寄存器，包括反馈移位寄存器、分圆多项式和本原多项式、m序列等内容。

书中每章末都配有适量习题，以供学生学习和复习巩固书中所学内容。

《信息安全数学基础》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，同时，也可以供从事信息安全和其他信息技术工作的人员参考。

第一图书网, tushu007.com

<<信息安全数学基础>>

书籍目录

第1章 预备知识1.1 集合、关系和函数1.1.1 集合1.1.2 关系1.1.3 函数1.2 组合数学初步知识1.2.1 排列与组合1.2.2 生成函数习题第2章 数论基础（一）2.1 整除2.1.1 整除与带余除法2.1.2 最大公因子与辗转相除法2.1.3 连分数2.1.4 算术基本定理2.1.5 梅森素数和费马素数2.2 同余2.2.1 同余的概念和性质2.2.2 剩余类和欧拉定理2.2.3 线性同余方程2.2.4 孙子定理与同余方程组2.2.5 高次同余方程习题第3章 数论基础（二）3.1 原根3.1.1 整数的次数3.1.2 原根3.1.3 指数与n次剩余3.2 二次剩余3.2.1 二次剩余的概念和性质3.2.2 勒让德符号与二次互反律3.2.3 雅可比符号3.3 数论的典型应用3.3.1 素性检验算法3.3.2 因子分解算法习题第4章 代数系统基础4.1 群4.1.1 群及其基本性质4.1.2 子群4.1.3 循环群和群的生成4.1.4 陪集和拉格朗日定理4.1.5 同态与同构4.1.6 正规子群与商群4.1.7 循环群的分类4.1.8 置换群4.2 交换环和域4.2.1 交换环及其基本性质4.2.2 域及其基本性质4.2.3 同态与同构4.2.4 一元多项式环4.2.5 理想和商环4.3 域上的一元多项式环4.3.1 一元多项式的整除4.3.2 一元多项式环的理想4.3.3 域上一元多项式唯一分解定理4.3.4 多项式不可约性检验4.3.5 一元多项式的同余与商环4.4 有限域理论初步习题第5章 椭圆曲线5.1 椭圆曲线的预备知识5.1.1 仿射平面和射影平面5.1.2 判别式、结式和代数不变量5.1.3 一元三次方程的公式解——Caftan公式5.2 椭圆曲线5.2.1 Weierstrass方程5.2.2 椭圆曲线5.2.3 椭圆曲线上点的加法群（Mordell-Weil群）5.2.4 有限域上的椭圆曲线5.3 离散对数初步5.3.1 有限域上的离散对数5.3.2 椭圆曲线上的离散对数习题第6章 线性反馈移位寄存器（LFSR）6.1 反馈移位寄存器6.1.1 反馈移位寄存器6.1.2 线性反馈移位寄存器（LFSR）6.1.3 非线性组合移位寄存器简介6.2 分圆多项式和本原多项式6.2.1 分圆多项式6.2.2 本原多项式6.3 m序列6.3.1 LFSR的特征多项式6.3.2 m序列的产生条件6.3.3 m序列的特点6.3.4 m序列的破译习题参考文献

第一图书网, tushu007.com

章节摘录

插图：第1章 预备知识在当前的信息安全专业的课程体系中，由于“信息安全数学基础”课程涉及的一些数学基础知识在前期的“高等数学”等课程中介绍得较少，本书将对相关的这部分内容进行一些补充，以便读者能够顺利地阅读书中后续的各个章节。
本章是与书中后面几章内容相关的预备知识的介绍，包括集合、关系和函数的基本概念、排列与组合及生成函数等内容。
1.1 集合、关系和函数集合论是德国著名数学家康托尔（cantor）于19世纪末创立的，康托尔当时建立的集合论称为朴素集合论。
20世纪初，策梅罗（zermelo）给出了第一个集合论的公理系统，并在此基础上逐步形成了公理化集合论和抽象集合论，使该学科成为在数学中发展最快的一个分支。
集合论是现代数学的基础，通俗地讲，数学所研究的一切概念都可以用集合来定义，甚至包括很多已经非常熟悉的概念，如整数、实数和函数等，都可以用集合加以表示。
此外，集合概念的引入，也使得我们能够摆脱具体数系的束缚，建立和研究很多抽象的数学概念和对象，从而得到很多抽象层次上的具有更多普遍含义的结论，这一点将在本书的第4章得到较多的体现。
现在，集合论观点已经渗透到了古典分析、泛函、概率和信息论等各个领域。
本节将介绍集合论的基础知识，包括集合与关系、集合运算、函数和等势的概念和规则。

第一图书网, tushu007.com

编辑推荐

《信息安全数学基础》：高等学校信息安全类专业系列教材

第一图书网, tushu007.com

<<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