<<初等数论及其在信息科学中的应用>>

图书基本信息

书名：<<初等数论及其在信息科学中的应用>>

13位ISBN编号：9787302238003

10位ISBN编号：7302238006

出版时间：2010-9

出版时间：清华大学出版社

作者：朱萍

页数：169

内容概要

《初等数论及其在信息科学中的应用》是一本关于初等数论及其在密码学中应用的基础教材。全书共分5章。
第1章和第2章分别介绍整除性和同余理论。
第3章讨论前两章知识在古典密码学和RSA公钥密码体制中的应用。
第4章介绍二次剩余及其在硬币抛掷和零知识证明中的应用。
第5章介绍阶、原根和离散对数的概念及其在伪随机数生成、ElGamal公钥密码体制和椭圆曲线密码中的应用。
每章后面都配有习题，书末附有习题答案及提示。
另外，在附录中，我们按照章节顺序列出了两种常用数学软件Maple和Mathematica用于数论计算的有关命令。

《初等数论及其在信息科学中的应用》可以作为综合性和工科院校数学专业和信息科学相关专业的初等数论本科生课程教材，也可作为相关领域中的教学科研人员以及工程技术人员的参考书。

<<初等数论及其在信息科学中的应用>>

书籍目录

第1章 整除性1.1 整除1.2 最大公因数与欧几里得算法1.3 最小公倍数1.4 一次不定方程1.5 算术基本定理1.6 厄拉多塞筛法1.7 素数分布习题一第2章 同余2.1 同余定义及基本性质2.2 剩余系2.3 欧拉函数与默比乌斯函数2.4 一次同余方程2.5 中国剩余定理2.6 模为素数的高次同余方程2.7 模为合数的高次同余方程2.8 伪素数和素性测试习题二第3章 RSA密码体制3.1 密码学基本概念3.2 几种简单密码体制及其破译3.3 RSA公钥密码体制3.4 RSA的实现3.5 RSA的安全性讨论习题三第4章 二次剩余4.1 概念及判别4.2 勒让德符号4.3 二次同余方程4.4 雅可比符号4.5 二次剩余的应用习题四第5章 原根及其应用5.1 整数的阶5.2 原根5.3 一般既约剩余系的构造5.4 离散对数5.5 伪随机数5.6 ElGamal密码体制5.7 椭圆曲线密码习题五附录A 抽象代数基本概念附录B 数学软件Maple和Mathematica中的一些与数论相关的命令B.1 Maple中的一些与数论相关的命令B.2 Mathematica中的一些与数论相关的命令习题答案及提示索引参考文献

编辑推荐

《初等数论及其在信息科学中的应用》以经典理论与现代应用相结合的方式，比较系统地介绍了初等数论的基本概念和方法。
具体内容包括模为素数的高次同余方程、密码学基本概念、RSA的安全性讨论、ElGamal密码体制、椭圆曲线密码等。
该书可供各大专院校作为教材使用，也可供从事相关工作的人员作为参考用书使用。

版权说明