<<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

<<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

<<信息安全数学基础>>

版权说明