<<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：9787307052345

10位ISBN编号：7307052342

出版时间：2006-9

出版时间：武汉大学出版社

作者：李继国、余纯武、张福泰、马春光

页数：210

<<信息安全数学基础>>

内容概要

本书全面系统地介绍了数论、代数、组合数学等相关基础理论和密码学研究中用到的一些实用算法。包括整除、同余、二次同余式与平方剩余、原根、群、环、有限域、格及其应用、椭圆曲线、组合数学等数学知识以及素性测试、因数分解和离散对数计算等一些实用算法，共13章。
书末列出了主要参考文献。
本书可作为信息安全、计算机科学与技术、通信工程、数学与应用数学等专业本科生和研究生的教材，也可供从事信息安全、密码学和其他信息技术工作的科研和工程技术人员参考。

<<信息安全数学基础>>

书籍目录

<<信息安全数学基础>>

版权说明