

<<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：9787302084471

10位ISBN编号：7302084475

出版时间：2004-6

出版时间：清华大学出版社

作者：陈恭亮

页数：211

字数：340000

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所涉及的数论、代数和椭圆曲线论等数学理论，特别是对在信息安全工程实践中所涉及的数学知识做了较详细的讲述；此外，本书还介绍了在信息安全研究和应用中所产生的一些新的数学成果。

本书可作为信息安全专业、通信专业、信息专业、计算机专业的本科生和研究生的教科书，也可以供从事信息安全工作的科研人员参考。

## 书籍目录

第一章 整数的可除性 1.1 整除的概念 欧几里得除法 1.2 整数的表示 1.3 最大公因数与广义欧几里得除法 1.4 整除的进一步性质及最小公倍数 1.5 素数 算术基本定理 1.6 素数定理 1.7 习题第二章 同余 2.1 同余的概念及基本性质 2.2 剩余类及完全剩余系 2.3 简化剩余系与欧拉函数 2.4 欧拉定理 费马小定理 2.5 模重复平方算法 2.6 习题第三章 同余式 3.1 基本概念及一次同余式 3.2 中国剩余定理 3.3 高次同余式的解数及解法 3.4 素数模的同余式 3.5 习题第四章 二次同余式与平方剩余 4.1 一般二次同余式 4.2 模为奇素数的平方剩余与平方非剩余 4.3 勒让德符号 4.4 二次互反律的证明 4.5 雅可比符号 4.6 模 $p$ 平方根 4.7 合数的情形 4.8 素数的平方表示 4.9 习题第五章 原根与指标 5.1 指数及其基本性质 5.2 原根存在的条件 5.3 指标及 $n$ 次剩余 5.4 习题第六章 素性检验 6.1 拟素数 6.2 Euler拟素数 6.3 强拟素数 6.4 习题第七章 连分数 7.1 连分数 7.2 简单连分数 7.3 循环周期连分数 7.4 习题第八章 群 8.1 群 8.2 同态和同构 8.3 商群 8.4 习题第九章 群的结构 9.1 循环群 9.2 有限生成交换群 9.3 置换群 9.4 习题第十章 环 10.1 环和同态 10.2 分式域 10.3 理想 10.4 多项式环第十一章 域和Galois理论 11.1 域的扩张 11.2 基本定理 11.3 可分域 代数闭包 11.4 习题第十二章 域的结构 12.1 超越基 12.2 有限域的构造 12.3 习题第十三章 椭圆曲线 13.1 椭圆曲线基本概念 13.2 加法原理 13.3 有限域上的椭圆曲线 13.4 习题第十四章 AKS素性检验附录一 三个数学难题附录二 索引主要参考文献

## <<信息安全数学基础>>

### 媒体关注与评论

书评本色特色：详细介绍了信息安全，特别是公钥密码系统所涉及的数论、代数和椭圆曲线论等数学理论。

对欧几里得除法、模同余、欧拉定理、中国剩余定理、二次同余、原根、有限群、有限域、椭圆曲线做了较详细的讲述。

不仅能使读者从数学方面了解密码系统的安全性，而且可帮助读者运用所学知识去构建安全有效的密码系统。

## <<信息安全数学基础>>

### 编辑推荐

本色特色： 详细介绍了信息安全，特别是公钥密码系统所涉及的数论、代数和椭圆曲线论等数学理论。

对欧几里得除法、模同余、欧拉定理、中国剩余定理、二次同余、原根、有限群、有限域、椭圆曲线做了较详细的讲述。

不仅能使读者从数学方面了解密码系统的安全性，而且可帮助读者运用所学知识去构建安全有效的密码系统。

<<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>