

<<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：9787302128458

10位ISBN编号：7302128456

出版时间：2006-8

出版时间：清华大学出版社

作者：覃中平

页数：275

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

本书介绍了群、环、域、数论、组合论、移位寄存器序列、计算复杂性、信息论与数理逻辑等诸多与信息安全相关联的数学基础内容。

本书以大量的例题说明数学的抽象概念对信息安全中的诸多对象的本质刻画。

本书内容全面系统，包括信息安全领域最主要的数学知识，并与信息安全的应用结合十分紧密，这是目前其他书籍所不具备的显著特点。

本书可作为信息安全领域的研究生与大学生的相关课程的教材，也可作为信息安全领域的工程技术人员参考书。

## 书籍目录

第1章 群 1.1 群的定义 1.2 群的性质 1.3 群的陪集分解 1.4 正规子群、商群、群同态、群同构 1.5 置换群 习题第2章 环 2.1 环的定义 2.2 理想、商环 2.3 多项式环 2.4 商域 习题第3章 域 3.1 域的概念 3.1.1 域的定义 3.1.2 域的基本性质 3.1.3 域上的多项式 3.2 有限域加法特性 3.3 有限域的乘法特性 3.4 最小多项式与本原多项式 3.4.1 最小多项式与本原多项式的概念 3.4.2 有限域上的多项式 $x^n-1$ 的分解 3.4.3 多项式的周期 3.5 有限域的表示和运算 3.5.1 有限域 $GF(2^n)$ 的表示和运算 3.5.2 素域 $GF(p)$ 的表示和运算 3.6 有限域的结构 3.6.1 数论函数 3.6.2 有限域的结构 习题 参考文献第4章 数论一：整数的整除和同余 4.1 辗转相除法及其应用 4.1.1 辗转相除法 4.1.2 最大公因数与最小公倍数 4.1.3 一次不定方程 4.1.4 一次同余方程 4.1.5 整数的唯一分解定理 4.2 整数的同余 4.2.1 剩余系 4.2.2 欧拉函数和欧拉定理 4.2.3 孙子定理和剩余表示 4.3 一般同余方程 4.4 二次同余方程 4.4.1 二次同余方程的化简 4.4.2 二次剩余 4.4.3 勒让德符号和雅可比符号 4.4.4 二次同余方程的解法 习题 参考文献第五章 数论二：原根和素性检测 5.1 原根 .....第6章 组合论第7章 移位寄存器序列第8章 计算复杂性第9章 信息论第10章 数理逻辑基础

<<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>