

<<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：9787030365064

10位ISBN编号：7030365062

出版时间：2013-2

出版时间：聂旭云，廖永建 科学出版社 (2013-02出版)

作者：聂旭云，廖永建

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

《信息安全数学基础(普通高等教育信息安全类国家级特色专业系列规划教材)》编著者聂旭云等。

《信息安全数学基础(普通高等教育信息安全类国家级特色专业系列规划教材)》介绍了信息安全研究所涉及的数论、代数、信息论、复杂度理论及组合数学的基础理论，具体包括：整数；同余；群；环和域；多项式；有限域；椭圆曲线；保密系统的信息理论；计算复杂度理论；组合数学等。在介绍这些数学理论的同时，举例介绍了部分运算计算机实现的算法设计。通过阅读本书可系统地学习信息安全研究所涉及的数学理论。

本书可以作为高等院校信息安全专业本科生或研究生教材，也可作为计算机、通信及电子商务等专业的参考书，同时也可作为信息安全相关工程技术人员的参考读物。

## &lt;&lt;信息安全数学基础&gt;&gt;

## 书籍目录

从书序前言	第1章 整数	1.1 整除概念和基本性质	1.2 整数中的算法	1.3 素数与算术基本定理	1.4 整数的表示	1.5 多精度数的运算	习题	第2章 同余	2.1 同余的概念和基本性质	2.2 同余类与剩余系	2.3 同余方程与中国剩余定理	2.4 二次同余方程与二次剩余	2.5 模m的算法	习题	第3章 群	3.1 二元运算	3.2 群的定义和简单性质	3.3 子群、陪集	3.4 正规子群、商群和同态	3.5 循环群	3.6 置换群	3.7 群中的一些常用算法	习题	第4章 环和域	4.1 环的定义	4.2 整环、除环和域	4.3 子环、理想和商环	4.4 素理想、极大理想和商域	习题	第5章 多项式	5.1 多项式相关概念	5.2 因式	5.3 多项式同余	5.4 多元多项式	5.5 多项式环中的一些算法	习题	第6章 有限域	6.1 域和扩域	6.2 有限域的结构	6.3 不可约多项式的根, 迹和范数	6.4 有限域上元素的表示	6.5 有限域中的算法	习题	第7章 椭圆曲线	7.1 椭圆曲线的基本概念	7.2 椭圆曲线的运算	7.3 除子和双线性对	7.4 椭圆曲线上的离散对数	习题	第8章 保密系统的信息理论	8.1 保密系统的数学模型	8.2 熵	8.3 熵的特性	8.4 假密钥和唯一性距离	8.5 互信息	习题	第9章 计算复杂度理论	9.1 基本概念	9.2 图灵机	9.3 基本原理	9.4 归约方法	9.5 NP完全问题(NP Complete)	习题	第10章 组合数学	10.1 排列与组合	10.2 抽屉原理与容斥原理	10.3 递推关系	10.4 生成函数	习题	索引	参考文献
-------	--------	---------------	------------	---------------	-----------	-------------	----	--------	----------------	-------------	-----------------	-----------------	-----------	----	-------	----------	---------------	-----------	----------------	---------	---------	---------------	----	---------	----------	-------------	--------------	-----------------	----	---------	-------------	--------	-----------	-----------	----------------	----	---------	----------	------------	--------------------	---------------	-------------	----	----------	---------------	-------------	-------------	----------------	----	---------------	---------------	-------	----------	---------------	---------	----	-------------	----------	---------	----------	----------	-------------------------	----	-----------	------------	----------------	-----------	-----------	----	----	------

## <<信息安全数学基础>>

### 编辑推荐

《信息安全数学基础(普通高等教育信息安全类国家级特色专业系列规划教材)》编著者聂旭云等。

本书内容具体包括：整数的运算、同余；群、环、域及有限域的概念及性质，椭圆曲线；信息论基础；复杂度理论基础；组合数学等，在介绍这些数学理论的同时，举例介绍了部分运算的计算机实现算法设计。

通过阅读本书可系统的学习信息安全研究所涉及的数学理论。

<<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>