

<<简明信息安全数学基础>>

图书基本信息

书名：<<简明信息安全数学基础>>

13位ISBN编号：9787040311815

10位ISBN编号：704031181X

出版时间：2011-1

出版时间：高等教育出版社 高等教育出版社 (2011-01出版)

作者：陈恭亮

页数：244

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>

<<简明信息安全数学基础>>

内容概要

《简明信息安全数学基础》简明而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基本数学理论和方法，以及它们在信息安全实践中的应用。

《简明信息安全数学基础》可作为信息安全、通信、计算机和应用数学等专业的本科生、专科生的教科书，也可作为信息专业技术人才知识更新培训课程的教科书，还可作为信息安全从业人员的参考书。

<<简明信息安全数学基础>>

书籍目录

第1章 整数的可除性1.1 整除的概念1.2 Euclid除法1.3 广义Euclid除法1.4 素数的生成1.5 最大公因数1.6 习题第2章 同余2.1 同余的基本性质2.2 Euler定理Fermat小定理2.3 模重复平方算法2.4 大素数的生成2.5 习题第3章 同余式3.1 一次同余式3.2 中国剩余定理3.3 RSA公钥密码系统3.4 习题第4章 二次同余式与平方剩余4.1 二次同余式4.2 二次互反律4.3 Rabin公钥密码系统4.4 习题第5章 原根5.1 指数5.2 原根5.3 Diffie-Hellman密钥协商5.4 习题第6章 基本代数6.1 群6.2 环6.3 域6.4 习题第7章 有限域7.1 有限域的构造7.2 有限域的基底7.3 习题第8章 椭圆曲线8.1 椭圆曲线的概念8.2 重复倍加算法8.3 椭圆曲线密码系统8.4 习题附录A 三大难解数学问题附录B附录C附录D附录E 部分习题参考答案参考文献索引

<<简明信息安全数学基础>>

章节摘录

版权页：插图：

<<简明信息安全数学基础>>

编辑推荐

《简明信息安全数学基础》特色：《简明信息安全数学基础》作者主讲的“信息安全数学基础”课程为上海市精品课程。

教材结合信息安全最新研究成果和工程实践，深刻把握所涉及的数学理论和方法的本质，并运用数学语言和方法以及具体的案例和应用，简明阐述信息安全的数学理论和方法。

- 基础性 对关于信息安全的重要数学理论和方法以及算法。

给出详细的推理过程和说明。

- 实用性 对信息化建设可能遇到的关于信息安全的数学基础知识，以具体的案例作出简明阐述。
- 系统性 运用统一的数学语言与符号，形成大整数因数分解问题、离散对数问题、椭圆曲线离散对数问题三大难解数学问题的知识体系。

<<简明信息安全数学基础>>

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>