《信息安全的数学基础》

图书基本信息

书名：《信息安全的数学基础》

13位ISBN编号：9787118072327

10位ISBN编号：711807232X

出版时间：2011-4

出版社：罗守山、陈萍、罗群、 等 国防工业出版社 (2011-04出版)

页数：153

《信息安全的数学基础》

内容概要

《信息安全的数学基础》围绕信息安全相关课程所需的数学基础，介绍数论、近世代数、组合数学的基本原理和方法。《信息安全的数学基础》的内容包括：整数和多项式的表示与运算、同余方程与不定方程、群、环、域、组合数学基础。为了增强学生对信息安全中数学方法的理解，在每一章的最后还介绍了相关数学知识在信息安全与密码学中的应用。同时，各章还配有一定数量的习题，便于教学与自学。
《信息安全的数学基础》可以作为信息安全相关专业的本科生教材，也可供从事相关专业的教师、科研人员和工程技术人员参考。

《信息安全的数学基础》

书籍目录

《信息安全的数学基础》

章节摘录

版权页：插图：群理论在密码学中有着重要的应用。利用群中元素之间的运算，可以完成公钥密码体制中的密钥生成、加密运算、解密运算等工作。本节首先介绍公钥密码的基本概念。之后，介绍两个公钥加密体制：RSA公钥密码体制和背包公钥密码体制。在这些密码体制中，相关的密码变换都是基于群中元素的运算的。3.7.1公钥密码的概念公开密钥密码体制是现代密码学的最重要的发明和进展之一。一般地理解，密码学就是用于保护信息传递的机密性。但这仅仅是当今密码学主题的一个方面；对信息发送与接收者的真实身份的验证、对所发出／接收信息在事后的不可抵赖以及保障数据的完整性是现代密码学主题的另一个方面。公开密钥密码体制对这两方面的问题都给出了出色的解答，并正在继续产生许多新的思想和方案。在公钥体制中，加密密钥不同于解密密钥。人们将加密密钥公之于众，而解密密钥只有解密人自己知道。迄今为止的所有公钥密码体系中，RSA系统是最著名、使用最广泛的一种。公钥密码由Diffie和Hellman于1976年首次提出的一种密码技术。与对称密码体制相比，公钥密码体制有两个不同的密钥分别实施加密与解密。这两个密钥中的一个密钥称为私钥，需要秘密地保存；另一个密钥称为公钥，不需要保密。公钥密码学的概念是为了解决传统密码中最困难的两个问题而提出的，这两个问题是密钥分配问题和数字签名问题。密钥分配问题：很多密钥分配协议引入了密钥分配中心，一些密码学家认为，用户在保密通信的过程中，应该具有保持完全的保密性的能力。但引入密钥分配中心，违背了密码学的精髓。数字签名问题：能否设计出一种方案，就像手写签名一样，能确保数字签名是出自某特定的人，并且各方对此没有异议。

《信息安全的数学基础》

编辑推荐

《信息安全的数学基础》为中国密码学会教育工作委员会推荐教材。

《信息安全的数学基础》

精彩短评

1、纸张质量不错 内容也可以

《信息安全的数学基础》

版权说明