第一图书网, tushu007.com

<<初等数论及其在密码学中的应用与M>>

图书基本信息

书名：<<初等数论及其在密码学中的应用与Maple实现>>

13位ISBN编号：9787030250049

10位ISBN编号：7030250044

出版时间：2007-9

出版时间：科学出版社

作者：游林

页数：217

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

第一图书网, tushu007.com

前言

在RSA密码出现之前，可以说，大多数人都认为初等数论完全是纯理论性的数学学科。但是，自RSA与ElGamal等公钥密码体制出现以后，人们逐渐认识到初等数学的理论知识在密码学、信息安全及通信等领域具有重要的实际应用价值。

本书以全新的方式介绍了整数的整除性、常用数论函数、同余理论、整数的阶与原根、平方剩余及不定方程理论等初等数论的基本内容。同时，在本书的最后一章介绍了这些初等数论知识在密码学中的一些应用。

本书主要有以下4个方面的特点。

（1）以极丰富的例子诠释了初等数论问题的若干解题技巧与方法，其中，许多例子都来源于奥林匹克数学竞赛题。

（2）除各节配有适量习题外，每章还配有一定数量的研究题及思考题，这些研究题与思考题不仅适合相关专业的本科生作为毕业论文的参考选题，而且也适合对初等数论有浓厚兴趣的读者做研究尝试与探讨。

（3）介绍了初等数论的理论知识在古典密码术及RSA、ElGamal、Rabin等现代公钥密码算法中的应用。

（4）借助数学软件Mapie，给出了若干初等数论问题求解的算法程序。

数论这门古老的科学如今在密码学中发挥着越来越重要的作用，它广泛应用于古典密码术、分组密码、流密码及公钥密码算法或各种密码协议中。本书在第7章以较简洁的形式介绍了初等数论在（Caesar密码、Vigenere密码和Hill密码等比较经典的密码术，以及在RSA、ElGamal、Rabin和MH背包等公钥密码系统中的应用。其实，从古典密码术到现代密码学的各个分支，处处都显现着初等数论这门基础理论学科的踪影。此外，初等数论也是与代数学、组合数学、图论、计算机科学、通信等学科密切相关的一门学科。

本书的编写与出版得到杭州电子科技大学出版基金、国家自然科学基金项目（项目编号：60763009）和教育部科学技术研究重点项目（项目编号：207089）的资助，特此致谢。

由于作者水平有限，书中难免存在不妥之处，敬请读者批评指正。

第一图书网, tushu007.com

内容概要

初等数论是完全以初等的方法研究整数性质的一门很古老的数学分支。
本书介绍了初等数论的基础理论及其在古典密码术与一些公钥密码体制中的应用，同时，还介绍了利用数学软件Maple求解初等数论问题。
全书由整除性理论、常用数论函数、同余理论、整数的阶与原根、平方剩余、不定方程理论、初等数论在密码学中的应用等7章组成，每章的最后一节介绍如何利用数学软件Maple来求解初等数论问题。同时，在每章的最后都单独配有数量丰富的综合例题、思考题与研究题，以便读者对书中所论述的内容加深理解和掌握，或做进一步的探讨之用。

本书可作为高等院校数学、信息与计算科学等专业的教材或教学参考书，也适用于中学数学老师作为奥林匹克数学竞赛培训或教学的参考教材。
从事密码学、信息安全及通信等专业的工程技术人员也可用本书作为参考资料。

第一图书网, tushu007.com

<<初等数论及其在密码学中的应用与M>>

书籍目录

第一图书网, tushu007.com

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