《公钥密码学的数学基础》

图书基本信息

书名：《公钥密码学的数学基础》

13位ISBN编号：9787030351364

10位ISBN编号：7030351363

出版时间：2013-1

出版社：王小云，王明强，孟宪萌 科学出版社 (2013-01出版)

作者：王小云,王明强,孟宪萌

页数：154

《公钥密码学的数学基础》

内容概要

王小云、王明强、孟宪萌所著的《公钥密码学的数学基础》是根据作者多年的教学经验，在原有讲义的基础上经过修改、补充而成的。书中介绍了公钥密码学中涵盖的数论代数基本知识与理论体系：第1章至第6章分别介绍了初等数论基础知识，主要包括同余、剩余类、原根和连分数的基本理论以及在公钥密码中的应用等；第7章至第9章描述了群、环、域三个基本的代数结构及其性质；第10章介绍了与密码学相关的计算复杂性理论及基本数学算法；第11章简单介绍了格理论及格密码分析的基本方法。

《公钥密码学的数学基础》适合信息安全专业本科生、研究生使用，也适合从事信息安全的工程技术人员和教师参考。

《公钥密码学的数学基础》

作者简介

王小云，教授，1966年出生，1983年至1993年就读于山东大学数学系，先后获得学士、硕士和博士学位，博士生导师潘承洞教授。1993年毕业后留校任教。现为清华大学杨振宁讲座教授，中国密码学会副理事长。2005年国家杰出青年基金获得者，2006年被聘为清华大学“长江学者特聘教授”。主要研究方向是密码理论研究。在密码分析领域，给出了多个重要Hash函数算法MD5与SH：A-1等的碰撞攻击。
王明强，博士，1970年生，2004于山东大学数学系获得博士学位，导师展涛教授。现为山东大学副教授，中国密码学会会员。主要研究方向是数论、算术几何，在可证明安全密码体质研究及椭圆曲线密码快速实现方面取得多个重要研究成果。
孟宪萌，博士，1971年生，1989年起先后就读于吉林大学数学系和山东大学数学系获学士、硕士和博士学位，攻读硕士博士学位期问的导师为展涛教授。毕业后从事教学与科研工作，现为山东财经大学教授，中国密码学会会员。主要研究方向是数论与密码，在数论中的加性问题研究以及公钥密码算法RSA的安全性分析方面取得多个重要研究成果。

《公钥密码学的数学基础》

书籍目录

《公钥密码学的数学基础》

《公钥密码学的数学基础》

编辑推荐

王小云、王明强、孟宪萌所著的《公钥密码学的数学基础》的内容主要有以下三方面的特色：一是数论与代数基本理论涵盖了一些重要的密码基础数学理论。二是注重理论与实践的紧密结合，并突出实践。在讲到比较重要的算法时，我们都配备一定数量的实践题目，使学生能体会到理论在实践中的应用。三是将算法复杂性理论贯穿全书，介绍与数论代数基本理论相关的算法及其复杂性，让读者初步体会数学理论在密码算法中的应用。

《公钥密码学的数学基础》

精彩短评

1、薄薄一本小册子，内容很多，不适合用来学习，备在手头用来复习还是不错的。

《公钥密码学的数学基础》

版权说明