第一图书网, tushu007.com

<<密码并不神秘>>

图书基本信息

书名：<<密码并不神秘>>

13位ISBN编号：9787030315342

10位ISBN编号：7030315340

出版时间：2011-6

出版时间：科学

作者：刘木兰

页数：142

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

<<密码并不神秘>>

内容概要

本书是为中学生编写的科普读物，主要讲什么是密码和信息安全，目的是使大家了解密码并不神秘。

本书共分7章。
第1章介绍密码学的基本专业术语，包括密码、密钥、密码体制、数字签名、身份识别等。
第2章是关于古典密码体制，第3章和第4
章分别讲述对称密码体制和公钥密码体制，第5章的数字签名是互联网环境下信息安全的重要内容。
第6章的密钥共享属于信息安全中密钥管理部分。
最后一章的电子商务是希望读者了解怎样才能使得参与电子商务活动的买家和卖家的权益得到保障。

本书除了可使读者走近密码和信息安全之外，一个“副产品”是使读者看到，在中学学过的整数运算、带余除法、辗转相除法求最大公因子等这些初等数学知识是多么有用。

第一图书网, tushu007.com

作者简介

刘木兰女，中国科学院数学与系统科学研究院研究员。

1941年生于北京，1964年毕业于中国科学技术大学数学系，1964年至今先后在中国科学院数学研究所、中国科学院系统科学研究所、中国科学院数学与系统科学研究院任职，1993年被国务院学位委员会批准为博士生导师。
1979～1981年，在美国哥伦比亚大学作访问学者，作为访问教授，访问过美国、荷兰、意大利、日本等国的多所大学。
研究工作领域涉及矩阵几何、代数K理论、计算机代数和密码与信息安全。
发表学术论文数十篇，出版专著《Groebrler基理论及其应用》和《密钥共享体制和安全多方计算》等。

第一图书网, tushu007.com

<<密码并不神秘>>

书籍目录

《美妙数学花园》丛书序
前言
第1章 密码学术语和基本概念
1.1 保密通信
1.2 密码
1.3 密钥
1.4 密码体制
1.5 信息数字化
1.6 数字签名
第2章 古典密码体制
2.1 文字替换密码体制
2.2 机械密码体制
2.3 统计密码分析
第3章 对称密码体制
3.1 流密码的加密和解密算法
3.2 周期序列和伪随机性质
3.3 线性反馈移位寄存器序列
第4章 公钥密码体制
4.1 公钥密码体制
4.2 单向函数
4.3 RSA公钥密码算法
第5章 数字签名、身份识别和密钥交换
5.1 数字签名方案
5.2 离散对数问题
5.3 ElGamal数字签名算法
5.4 身份识别
5.5 棣菲-赫尔曼密钥交换算法
第6章 密钥共享
6.1 拉格朗日插值多项式
6.2 门限密钥共享体制
第7章 电子商务
7.1 电子商务系统的组成
7.2 电子商务的业务流程
参考文献
附录 辗转相除法、同余和原根
A.1 整数
A.2 辗转相除法
A.3 算术基本定理
A.4 同余式
A.5 欧拉函数
A.6 原根和指数

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