<<现代密码学与金融信息安全技术>>

图书基本信息

书名：<<现代密码学与金融信息安全技术>>

13位ISBN编号：9787810794077

10位ISBN编号：7810794078

出版时间：2004年9月1日

出版时间：第1版 (2004年9月1日)

作者：王泽辉

页数：312

内容概要

《现代密码学与金融信息安全技术》系统介绍密码学的基本原理、核心技术及其在金融信息系统安全服务方面的实用技术。
内容包括密码学的数学基础与算法分析基础，金融领域的安全需求，适合普通大众的加密技术和现代密码体制的设计技巧，DES、IDEA、AES等对称密码算法，RSA、EIGamal、ECC等公匙密码算法，信息完整性鉴证、数学签章与抗抵赖技术，密匙重构、数学现金、隐私权保护等金融信息安全实用技术，公匙密码制攻击算法与改进算法，NTRU密码技术、量子密码学、概率加密技术。
《现代密码学与金融信息安全技术》内容翔实，表达严谨，提供了大量具体的算法伪代码和许多追踪算法的实例，读音可以据以编成计算机程序进行模拟实验，领会信息安全技术的精华。
《现代密码学与金融信息安全技术》可作为高等院校计算机科学、信息科学、金融学、通信工程、应用数学等专业的本科生教材及研究生教学参考书，也可以作为通信系统、金融系统、网络与电子商务系统的技术培训教材和实用工具书。

<<现代密码学与金融信息安全技术>>

书籍目录

版权说明