《现代密码学》

图书基本信息

书名：《现代密码学》

13位ISBN编号：9787302373779

出版时间：2015-2

作者：杨波

页数：282

《现代密码学》

内容概要

《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》全面而详细地介绍现代密码学的理论和相关算法，可帮助读者将所学知识应用于信息安全的实践中。全书共分10章，内容包括现代密码学的基本概念、流密码、分组密码、公钥密码、密钥分配与密钥管理、消息认证和哈希函数、数字签名和认证协议、密码协议、可证明安全及网络加密与认证。
《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》从教材使用的角度考虑，概念清晰、结构合理、通俗易懂、内容深入浅出，并充分考虑方便教师在教学过程中的实施，同时还注意与其他专业课教学的衔接。《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》取材新颖，不仅介绍现代密码学所涉及的基础理论和实用算法，同时也涵盖了现代密码学的最新研究成果，力求使读者通过《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》的学习了解本学科最新的发展方向。《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》可作为高等学校相关专业大学生和研究生的教材，也可作为通信工程师和计算机网络工程师的参考读物。

《现代密码学》

作者简介

杨波，北京大学学士，西安电子科技大学硕士、博士，陕西师范大学计算机科学学院教授，博士生导师，陕西省百人计划特聘教授，中国密码学会理事，中国密码学会密码算法专业委员会委员，《密码学报》编委。曾任华南农业大学信息学院，软件学院院长。2001年起在陕西师范大学计算机科学学院工作。2005年担任第四届中国信息和通信安全学术会议程序委员会主席，2009年担任中国密码学会年会副主席，2010年起担任The Joint Workshop on Information Security （JWIS） Co—General Chair。主持多项国家自然科学基金、863计划、国家密码发展基金、国防科技重点实验室基金，陕西省自认科学基金项目。

《现代密码学》

书籍目录

《现代密码学》

版权说明