<<密码协议基础>>

图书基本信息

书名：<<密码协议基础>>

13位ISBN编号：9787040251548

10位ISBN编号：704025154X

出版时间：2009-1

出版时间：高等教育出版社

作者：邱卫东　等编著

页数：254

<<密码协议基础>>

内容概要

本书较为全面、深入地介绍了信息安全体系中的基础密码协议、高级密码协议及应用密码协议，按照由浅人深的原则，将全书分为13章，内容包括三大部分：基础密码协议、高级密码协议及应用密码协议。
基础密码协议由引论、嗦钥协商、实体认证、比特承诺协议组成；高级密码协议部分包括高级签名协议、零知识、不经意传输、秘密分享和门限密码、安全多方计算协议；应用密码协议部分包括Kerberos协议、IKE密钥管理协议、电子现金及无线安全通信。
本书对各类密码协议及其相关应用进行了详细的论述和分析，可作为高校计算机、信息安全、电子信息与通信、信息与计算科学等专业高年级本科生和研究生的教学参考书，也可作为相关工程技术人员学习信息安全知识的入门读物。
通过阅读本书，读者不仅能够全面熟悉和r解各类密码协议的设计理念和安全机制，还可以提高密码及相关安全协议的独立设计和分析能力。

<<密码协议基础>>

作者简介

邱卫东，上海交通大学信息安全工程学院副教授。
长期从事信息安全、数据分析、密码学及其应用等方面的研究。
目前主持国家863专项项目“计算机取证关键技术研究”、国家自然科学基金项目“基于身份的可证安全密钥泄漏防护技术研究”等；曾参与国家863计划项目“密码协议工程方法与自动化验证研究”和国家自然科学基金重大研究计划“网上信息收集和分析基础问题模型研究”，负责信息分析、检测等子课题的研究：在德国做博士后期间，参与德国政府DAAD项目“IQN：Self Organization Network”，主要负责群签名及其在电子现金系统的应用研究。
合作出版专著《Contnibutions to Ubiquitous Computing》（Studiesin Computaional Inteligence Series42，Springer，2006）。
目前承担上海交通大学本科“信息安全数学基础”课程和研究生“密码算法与协议”课程的教学工作，其中作为主讲教师之一的“信息安全数学基础”课程被评为上海市精品课程。

<<密码协议基础>>

书籍目录

<<密码协议基础>>

版权说明