

《密码学教程》

图书基本信息

书名：《密码学教程》

13位ISBN编号：9787307052314

10位ISBN编号：7307052318

出版时间：2006-9

出版社：武汉大学出版社

作者：张福泰、李继国、王晓明、林柏钢、赵泽茂

页数：225

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《密码学教程》

内容概要

本书全面系统地介绍了密码学的体系结构，主要的理论和技术，内容涉及：密码学概论、古典密码体制、现代分组密码、流密码、公钥密码体制、密钥管理、Hash函数、数字签名、身份识别、认证理论与技术、PKI技术、密码应用软件，以及密码学新进展。全书内容丰富，语言通俗，注重理论性与实用性的结合，可作为信息安全、计算机科学与技术、通信工程、数学与应用数学等本科专业密码学课程的教材，也可供初学密码学的研究生及相关的工程技术人员参考。

《密码学教程》

书籍目录

第1章 密码学概论1.1 密码学的基本概念1.2 密码学的体系结构1.3 密码学发展简史1.4 密码学的应用习题第2章 古典密码体制2.1 代换密码2.2 置换密码2.3 古典密码的破译2.4 无条件安全的一次一密体制2.5 实验习题第3章 现代分组密码3.1 分组密码的概念3.2 代换-置换网络3.3 分组密码原理与设计准则3.4 数据加密标准——DES3.5 国际数据加密算法——IDEA3.6 高级加密标准——AES3.7 分组密码的操作模式3.8 差分分析与线性分析3.9 实验：DES和AES分组密码算法习题第4章 流密码4.1 流密码的原理4.2 有限状态自动机4.3 线性反馈移位寄存器4.4 PC44.5 流密码算法A54.6 流密码算法SNOW2.04.7 实验附录 参考算法习题第5章 公钥密码体制第6章 密钥管理第7章 Hash函数第8章 数字签名第9章 身份识别第10章 认证理论与技术第11章 PKI技术第12章 密码应用软件第13章 密码学新进展参考文献

《密码学教程》

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:www.tushu000.com