

<<密码学教程>>

图书基本信息

书名：<<密码学教程>>

13位ISBN编号：9787030349118

10位ISBN编号：7030349113

出版时间：2012-8

出版时间：科学出版社

作者：陈少真

页数：321

字数：424750

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>

<<密码学教程>>

内容概要

密码学教程全面讲解了密码学的基本知识，并对密码学近年来的最新研究成果作了介绍。特别是在序列密码体制、分组密码体制、公开密钥密码体制和密码学新进展的章节中，不仅介绍了经典的密码体制和算法，而且阐述了部分算法的安全性分析，并进一步介绍了网络安全协议及近几年密码发展的新成果，如量子密码、生物密码和云计算等。

为了使读者更好地掌握密码学知识，书中讲授了必要的数学背景，并在附录中提供了相关参考资料，以便读者进行相关研究。

密码学教程表达清晰，论证严谨，习题丰富，并穿插有密码学史上的趣闻轶事。

密码学教程可作为高等院校“信息安全”、“计算机安全”、“网络安全”、“通信安全”和“应用数学”等课程的教材或参考书，也可供信息安全系统设计开发人员、密码学和信息安全爱好者参考。

<<密码学教程>>

书籍目录

序言前言第1章 引论1.1 密码学与信息安全概述1.2 密码体制与密码分析1.3 密码体制的安全性1.4 香农理论简介*1.5 计算复杂性理论简介小结与注释习题1第2章 古典密码体制2.1 语言的统计特性2.2 单表代替密码2.3 单表代替密码的分析2.4 多表代替密码2.5 多表代替密码的分析2.6 转轮密码与M-2092.7 M-209的已知明文攻击小结与注释习题2第3章 布尔函数3.1 布尔函数的表示方法3.2 布尔函数的重量与概率计算3.3 布尔函数的非线性度3.4 布尔函数的相关免疫性及其构造3.5 严格雪崩准则和扩散准则*3.6 布尔函数的代数免疫小结与注释习题3第4章 序列密码4.1 线性反馈移位寄存器序列4.2 基于LFSR的序列生成器及其分析4.3 带进位的反馈移位寄存器序列小结与注释习题4第5章 分组密码与数据加密标准5.1 分组密码的基本概念5.2 数据加密标准DES5.3 KASUMI算法5.4 高级数据加密标准AES5.5 差分密码分析原理5.6 线性密码分析原理5.7 分组密码的工作模式和设计理论小结与注释习题5第6章 公开密钥密码体制6.1 公钥密码概述6.2 RSA公钥密码体制6.3 Rabin公钥密码体制6.4 基于离散对数问题的公钥密码体制*6.5 抗量子计算的公钥密码体制小结与注释习题6第7章 Hash函数与数字签名体制7.1 Hash函数概述7.2 Hash函数的安全性7.3 Hash函数标准SHA-17.4 数字签名体制概述7.5 数字签名体制的安全需求7.6 几种著名的数字签名体制7.7 具有隐私保护的数字签名体制小结与注释习题7第8章 密钥建立及管理技术8.1 密钥概述8.2 密钥分配8.3 密钥协商8.4 秘密共享8.5 密钥保护小结与注释习题8*第9章 零知识证明和身份识别体制9.1 零知识证明的基本概念9.2 识别个人身份的零知识证明9.3 Feige-Fiat-Shamir身份识别体制9.4 Guillou-Quisquater身份识别体制9.5 Schnorr身份识别体制9.6 Okamoto身份识别体制小结与注释习题9*第10章 SSL协议和IPsec协议10.1 网络安全概述10.2 SSL协议10.3 IPsec协议小结与注释习题10*第11章 密码学新进展11.1 概述11.2 量子计算与量子密码11.3 DNA计算与DNA密码11.4 基于同态加密的云计算小结与注释参考文献附录附录A 数论基础附录B 代数学基础附录C 有限域基础

<<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:<http://www.tushu007.com>