第一图书网, tushu007.com

<<应用密码学手册>>

图书基本信息

书名：<<应用密码学手册>>

13位ISBN编号：9787121013393

10位ISBN编号：7121013398

出版时间：2005-6

出版时间：电子工业出版社

作者：Menezes

页数：711

字数：1164000

译者：胡磊

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

内容概要

本书是目前最优秀的密码学书籍之一。
全书包含15章，内容覆盖了近20年来密码学发展的所有主要成就。
除了通常密码学书籍都会讲到的对称密码、杂凑涵数、公钥密码和签名、身份识别和密钥建立协议等内容外，本书首先提供了密码学的概貌，中间有三章专门讲述了公钥密码学的数学基础，最后两章给出了密码实现技巧和专利、标准等细节。
这些内容对研究者和工程师们都是十分有用的。
全书提供了丰富的密码学技术细节，包括200多个算法和协议、200多幅图表、1000多个定义、事实、实例、注释和评论。
书末列举了1200多篇关于密码学的主要文献，并在各章中对其做了简要评述。
　本书组织完美，表述清晰，适合密码学、计算机、通信、数学等领域折师生、专家和工程师们参考或作为教材使用。

作者简介

Alfred U．Menezes于1992年获得加拿大滑铁卢大学博士学位，现任滑铁卢大学教授，在椭圆曲线密码方面有很高的造诣。
Paul C．van Oorschot于1988年获得计算机科学博士学位，现任加拿大Carleton大学计算机科学学院教授，也是加拿大网络与软件安全研究主席，在密码学和网络安全方面具有深厚的学术功底。
Scott丸Vanstone干1974年获得博士学位，是加拿大滑铁卢大学教授，曾任杂志Designs，Codes and Cryptography的主编，滑铁卢大学数据加密研究组的主任。
他还是著名的Certicom信息安全公司的创始人。

书籍目录

第1章 密码学概述　1.1 引言　1.2 信息安全和密码学　1.3 函数知识　1.4 基本概念和术语　1.5 对称密钥加密　1.6 数字签名　1.7 认证与身份识别　1.8 公钥密码学　1.9 杂凑函数　1.10 协议和机制　1.11 密钥建立、管理和证书　1.12 伪随机数和序列　1.13 攻击类型和安全模型　1.14 注释与参考读物第2章 数学基础　2.1 概率论　2.2 信息论　2.3 复杂度理论　2.4 数论　2.5 抽象代数　2.6 有限域　2.7 注释与参考读物第3章 数论相关问题　3.1 引言　3.2 整数因子分解问题　3.3 RSA问题　3.4 二次剩余问题　3.5 Zn中平方根的计算　3.6 离散对数问题　3.7 Diffie-Hellman问题　3.8 合数模　3.9 单个比特计算　3.10 子集和问题　3.11 有限域上的多项式分解　3.12 注释与参考读物第4章 公钥参数　4.1 引言　4.2 概率素性测试　4.3 (真)素性测试　4.4 素数生成　4.5 Zp上的不可约多项式　4.6 生成元和高阶元素　4.7 注释与参考读物第5章 伪随机比特与伪随机序列　5.1 引言　5.2 随机比特生成　5.3 伪随机比特生成　5.4 统计测试　5.5 密码学意义安全的伪随机比特生成　5.6 注释与参考读物第6章 流密码　6.1 引言　6.2 反馈移位寄存器　6.3 基于LFSR的流密码　6.4 其他流密码　6.5 注释与参考读物第7章 分组密码　7.1 引言　7.2 背景与基本概念　7.3 古典密码及其发展史　7.4 DES　7.5 FEAL　7.6 IDEA　7.7 SAFER、RC5及其他分组密码　7.8 注释与参考读物第8章 公钥加密　8.1 引言　8.2 RSA公钥加密　8.3 Rabin公钥加密　8.4 EIGamal公钥加密　8.5 McEliece公钥加密　8.6 背包公钥加密　8.7 概率公钥加密　8.8 注释与参考读物第9章 杂凑函数和数据完整性　9.1 引言　9.2 分类和框架　9.3 基本构造和一般结果　9.4 不带密钥的杂凑函数(MDC)　9.5 带密钥的杂凑函数(MAC)　9.6 数据完整性和消息认证　9.7 杂凑函数的高级攻击　9.8 注释与参考读物第10章 身份识别和实体认证　10.1 引言　10.2 口令(弱认证)　10.3 挑战、响应身份识别(强认证)　10.4 自定义的和零知识的身份识别协议　10.5 对身份识别协议的攻击　10.6 注释与参考读物第11章 数字签名　11.1 引言　11.2 数字签名机制的框架　11.3 lISA和相关签名方案　11.4 Fiat-Shamir签名方案　11.5 DSA和相关签名方案　11.6 一次数字签名　11.7 其他签名方案　11.8 带附加功能的签名　11.9 注释与参考读物第12章 密钥建立协议　12.1 引言　12.2 分类和框架　12.3 基于对称加密的密钥传输　12.4 基于对称技术的密钥协商　12.5 基于公钥加密的密钥传输　12.6 基于非对称技术的密钥协商　12.7 秘密共享　12.8 会议密钥生成　12.9 密钥建立协议的分析　12.10 注释与参考读物第13章 密钥管理技术　13.1 引言　13.2 背景和基本概念　13.3 机密密钥分发技术　13.4 公钥分发技术　13.5 控制密钥使用的技术　13.6 多个域的密钥管理　13.7 密钥生命周期问题　13.8 可信第三方的高级服务　13.9 注释与参考读物第14章 有效实现　14.1 引言　14.2 多精度整数运算　14.3 多精度模算术　14.4 最大公因子算法　14.5 整数的中国剩余定理　14.6 指数运算　14.7 指数重编码　14.8 注释与参考读物第15章 专利与标准　15.1 引言　15.2 密码技术专利　15.3 密码标准　15.4 注释与参考读物附录A 精选密码学论坛文献目录参考文献索引

编辑推荐

本书是目前最优秀的密码学书籍之一。
全书提供了丰富的密码学技术细节，十分适合研究人员和工程师们学习。
本书的三位作者均是国际著名的密码学家和活跃的密码学研究者。
Alfred J.Menezes于1992年获得加拿大滑铁卢大学博士学位，现任滑铁卢大学教授，在椭圆曲线密码方面有很高的造诣。
Paul C.van Oorschot于1988年获得计算机科学博士学位，现任加拿大Carleton大学计算机科学学院教授，也是加拿大网络与软件安全研究主席，在密码学和网络安全方面具有深厚的学术功底。
Scott A.Vanstone于1974年获得博士学位，是加拿大滑铁卢大学教授，曾任杂志Designs,Codes and Cryptography的主编，滑铁卢大学数据加密研究组的主任。
他还是著名的Certicom信息安全公司的创始人。

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