

<<现代密码学>>

图书基本信息

书名：<<现代密码学>>

13位ISBN编号：9787563525973

10位ISBN编号：7563525971

出版时间：2011-4

出版时间：北京邮电大学出版社

作者：任伟

页数：288

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>

<<现代密码学>>

内容概要

本书内容包括密码学概述、古典密码体制、信息理论安全、序列密码、分组密码、hash函数与消息鉴别、公钥加密（基础）、公钥加密（扩展）、数字签名、实体认证和身份识别、密钥管理。

《现代密码学》特点是注重介绍知识的内在逻辑性，展现密码学方案设计的内在规律和基本原理，注重使用比较和类比的方式探究一般规律和方法论，使学习者“知其所以然”。

本书面向的主要对象包括高等学校信息安全、密码学、电子对抗、应用数学等专业本科高年级学生和研究生。

对具有密码学基础的研究人员也有一定启发作用。

<<现代密码学>>

书籍目录

第1章 密码学概述

1.1 密码学的目标与知识构成

1.2 密码学的发展简史

1.3 对加密体制的攻击

小结

扩展阅读建议

第2章 古典密码体制

2.1 密码系统的基本概念模型

2.2 置换加密体制

2.3 代换加密体制

2.3.1 单表代换密码

2.3.2 多表代换密码

2.3.3 多表代换密码的统计分析

2.3.4 转轮密码机

小结

扩展阅读建议

第3章 信息理论安全

3.1 基本信息论概念

3.1.1 信息量和熵

3.1.2 联合熵、条件熵、平均互信息

3.2 保密系统的数学模型

3.3 完善保密性

3.4 冗余度、唯一解距离

3.5 乘积密码体制

小结

扩展阅读建议

第4章 序列密码

4.1 序列密码的基本原理

4.1.1 序列密码的核心问题

4.1.2 序列密码的一般模型

4.1.3 伪随机序列的要求

4.2 密钥流生成器

4.2.1 密钥流生成器的架构

4.2.2 线性反馈移位寄存器

4.2.3 非线性序列生成器

4.2.4 案例学习A5算法

4.3 伪随机序列生成器的其他方法

4.3.1 基于软件实现的方法(RC4算法)

4.3.2 混沌密码体制简介

小结

扩展阅读建议

第5章 分组密码

5.1 分组密码的原理

5.1.1 分组密码的一般模型

5.1.2 分组密码的基本设计原理

<<现代密码学>>

- 5.1.3 分组密码的基本设计结构
- 5.1.4 分组密码的设计准则
- 5.1.5 分组密码的实现原则
- 5.2 案例学习：DES
 - 5.2.1 DES的总体结构和局部设计
 - 5.2.2 DES的安全性
 - 5.2.3 多重DES
- 5.3 其他分组密码
 - 5.3.1 AES
 - 5.3.2 SMS4简介
 - 5.3.3 RC6简介
 - 5.3.4 IDEA简介
 - 5.3.5 E2和Camellia算法
 - 5.3.6 其他分组算法
- 5.4 分组密码的工作模式
 - 5.4.1 ECB模式
 - 5.4.2 CBC模式
 - 5.4.3 CFB模式
 - 5.4.4 OFB模式
 - 5.4.5 CTR模式
- 小结
- 扩展阅读建议
- 第6章 Hash函数和消息鉴别
 - 6.1 Hash函数
 - 6.1.1 Hash函数的概念
 - 6.1.2 Hash函数的一般模型
 - 6.1.3 Hash函数的一般结构(Merkle-damgard变换)
 - 6.1.4 Hash函数的应用
 - 6.1.5 Hash函数的安全性(生日攻击)
 - 6.2 Hash函数的构造
 - 6.2.1 直接构造法举例SHA-1
 - 6.2.2 基于分组密码构造
 - 6.2.3 基于计算复杂性方法的构造
 - 6.3 消息鉴别码
 - 6.3.1 认证系统的模型
 - 6.3.2 MAC的安全性
 - 6.3.3 案例学习：CBC-MAC
 - 6.3.4 嵌套MAC及其安全性证明
 - 6.3.5 案例学习：HMAC
 - 6.4 对称密钥加密和Hash函数应用小综合
- 小结
- 扩展阅读建议
- 第7章 公钥加密(基础)
 - 7.1 公钥密码体制概述
 - 7.1.1 公钥密码体制的提出
 - 7.1.2 公钥密码学的基本模型
 - 7.1.3 公钥加密体制的一般模型

<<现代密码学>>

- 7.1.4 公钥加密体制的设计原理
- 7.1.5 公钥加密体制的分类
- 7.2 一个故事和三个案例体会
 - 7.2.1 Merkle谜题(Puzzle)
 - 7.2.2 Pohlig—Hellman非对称秘密密钥分组加密
 - 7.2.3 Merkle—Hellman背包公钥密码方案
 - 7.2.4 Rabin公钥密码体制
- 7.3 RSA密码体制
 - 7.3.1 RSA方案描述
 - 7.3.2 RSA加密体制的安全性
- 7.4 RSA的因子分解攻击
 - 7.4.1 Pollard Rho方法
 - 7.4.2 Pollard p-1分解算法
 - 7.4.3 随机平方法
- 7.5 素性检测
 - 7.5.1 产生RSA素数参数的可行性
 - 7.5.2 Fermat测试
 - 7.5.3 Solovay-Strassen测试
 - 7.5.4 Miller-Rabin测试
- 小结
- 扩展阅读建议
- 第8章 公钥加密(扩展)
 - 8.1 Elgamal密码体制
 - 8.1.1 离散对数问题与Diffie—Hellman问题
 - 8.1.2 Diffie—Hellman密钥交换协议
 - 8.1.3 Elgamal方案描述
 - 8.2 Elgamal安全性讨论
 - 8.2.1 小步大步算法
 - 8.2.2 PollardRho算法
 - 8.2.3 指数演算法
 - 8.2.4 Pohlig—Hellman算法
 - 8.3 椭圆曲线密码系统
 - 8.3.1 椭圆曲线群
 - 8.3.2 ECDLP以及ECDHP
 - 8.3.3 e1gamal的椭圆曲线版本
 - 8.3.4 Manes-Vanstone椭圆曲线密码体制
 - 8.3.5 ECC密码体制
 - 8.4 概率公钥加密体制Goldwasser-Micali
 - 8.4.1 语义安全
 - 8.4.2 Goldwasser-Micali加密体制
 - 8.4.3 Blum-Goldwasser概率加密体制
 - 8.5 其他新密码体制简介
 - 8.5.1 NTRU密码体制
 - 8.5.2 多变量公钥密码体制简介
- 小结
- 扩展阅读建议
- 第9章 数字签名

<<现代密码学>>

9.1 数字签名概述

9.1.1 数字签名的一般模型

9.1.2 数字签名的分类

9.1.3 数字签名的设计原理

9.1.4 数字签名的安全性

9.2 体会三个经典方案

9.2.1 lamport——次签名

9.2.2 Rabin数字签名

9.2.3 RSA数字签名

9.3 基于离散对数的数字签名

9.3.1 Elgamal签名体制

9.3.2 Elgamal签名设计机理的探讨

9.3.3 Schnorr签名体制

9.3.4 数字签名标准dss

9.3.5 Neberg-Rueppel签名体制

9.3.6 基于离散对数问题的一般签名方案

9.3.7 扩展讨论

9.4 椭圆曲线数字签名

9.4.1 ECDSA

9.4.2 EC-KCDSA

9.5 基于身份识别协议的签名

9.5.1 Feige-Fiat-Shamir签名方案

9.5.2 Guillou-Quisquater签名方案

9.5.3 知识签名

小结

扩展阅读建议

第10章 实体认证与身份识别

10.1 实体认证与身份识别概述

10.1.1 实体认证的基本概念

10.1.2 身份识别的基本概念

10.1.3 对身份识别协议的攻击

10.2 基于口令的实体认证

10.2.1 基于口令的认证协议

10.2.2 基于Hash链的认证协议

10.2.3 基于口令的实体认证连同加密的密钥交换协议

10.3 基于“挑战应答”协议的实体认证

10.3.1 基于对称密码的实体认证

10.3.2 基于公钥密码的实体认证

10.3.3 基于散列函数的实体认证

10.4 身份识别协议

10.4.1 Fiat-Shamir身份识别协议

10.4.2 Feige-Fiat-Shamir身份识别协议

10.4.3 Guillou-Quisquater身份识别协议

10.4.4 Schnorr身份识别协议

10.4.5 Okamoto身份识别协议

小结

扩展阅读建议

<<现代密码学>>

第11章 密钥管理

11.1 密钥管理概述

11.1.1 密钥管理的内容

11.1.2 密钥的种类

11.1.3 密钥长度的选取

11.2 密钥生成

11.2.1 伪随机数生成器的概念

11.2.2 密码学上安全的伪随机比特生成器

11.2.3 标准化的伪随机数生成器

11.3 密钥分配

11.3.1 公钥的分发

11.3.2 无中心对称密钥的分发

11.3.3 有中心对称密钥的分发

11.3.4 Blom密钥分配协议

11.4 密钥托管

11.4.1 密钥托管简介

11.4.2 密钥托管主要技术

11.5 PKI技术

11.5.1 PKI的概念

11.5.2 PKI的组成

11.5.3 X.509认证业务

11.5.4 PKI中的信任模型

小结

扩展阅读建议

参考文献

<<现代密码学>>

编辑推荐

《普通高校信息安全系列教材：现代密码学》也是一本旨在让学习者能够“真正学懂密码学”的密码学教材。

“密码学”是信息安全专业、密码学专业、电子对抗专业中一门最重要的专业课，在学科知识体系中占据重要的地位。

但多年的教学实践以及学生的体会表明，它也是一门非常难学（和难讲授）的综合课程，其数学基础涉及算法数论、计算复杂性、抽象代数、信息论、概率论等，讲授的内容覆盖面广，各知识点均具有一定难度和深度。

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>