

《应用密码学》

图书基本信息

书名：《应用密码学》

13位ISBN编号：9787302361665

出版时间：2014-11

作者：刘嘉勇,任德斌,胡勇,方勇

页数：265

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

《应用密码学》

内容概要

《重点大学计算机专业系列教材:应用密码学(第2版)》既可作为信息安全、计算机科学与技术、信息与计算科学、通信工程、信息管理以及电子商务等信息技术类专业密码学课程的教材,也可供从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

书籍目录

第1章密码学概述

1.1 信息安全与密码技术

1.2 密码技术发展简介

1.2.1 古典密码时期

1.2.2 近代密码时期

1.2.3 现代密码时期

1.3 密码学基本概念

1.3.1 密码学的主要任务

1.3.2 保密通信模型

1.3.3 密码系统的安全性

1.3.4 密码系统设计的基本原则

1.3.5 密码体制的分类及特点

思考题与习题

第2章古典密码技术

2.1 替代密码 (Substitution Cipher)

2.1.1 单表替代密码

2.1.2 多表替代密码

2.2 置换密码 (Permutation Cipher)

2.2.1 周期置换密码

2.2.2 列置换密码

2.3 转轮机密码

思考题与习题

第3章分组密码

3.1 概述

3.2 分组密码的设计原则与评估

3.2.1 分组密码的设计原则

3.2.2 分组密码的评估

3.3 分组密码常见的设计方法

3.3.1 Feistel结构

3.3.2 SPN结构

3.4 数据加密标准——DES

3.4.1 算法描述

3.4.2 DES的安全性分析

3.4.3 三重DES

3.5 高级加密标准——AES

3.5.1 AES算法的数学基础

3.5.2 算法的总体描述

3.5.3 算法的基本变换

3.5.4 密钥扩展算法

3.5.5 解密算法

3.6 分组密码的工作模式

3.6.1 电子密码本模式 (ECB)

3.6.2 密码分组链接模式 (CBC)

3.6.3 密码反馈模式 (CFB)

3.6.4 输出反馈模式 (OFB)

3.6.5 计数器模式 (CTR)

3.7 其他分组密码

3.7.1 IDEA加密算法

3.7.2 RC6加密算法

思考题和习题

第4章公钥密码体制

4.1概述

4.1.1公钥密码体制提出的背景

4.1.2公钥密码的基本思想

4.1.3公钥密码的应用

4.2 RSA公钥密码体制

4.2.1 RSA的算法描述

4.2.2 RSA的实现

4.2.3 RSA的安全性

4.2.4 RSA在应用中的问题

4.3 E1Gamal公钥密码体制

4.4椭圆曲线密码体制

4.4.1概述

4.4.2椭圆曲线的概念与运算

4.4.3椭圆曲线密码体制

思考题和习题

第5章散列函数与消息鉴别

5.1散列函数的概念

5.1.1散列函数的性质

5.1.2散列函数的应用

5.2散列函数的构造与设计

5.2.1迭代型散列函数的一般结构

5.2.2散列函数的设计方法

5.3安全散列算法SHA

5.3.1 SHA—1

5.3.2其他SHA算法

5.4对散列函数的攻击

5.4.1生日悖论

5.4.2生日攻击

5.5消息鉴别

5.5.1基于加密技术的消息鉴别

5.5.2基于散列函数的消息鉴别

5.5.3 HMAC算法

思考题与习题

第6章数字签名技术

6.1数字签名概述

6.1.1数字签名的特性

6.1.2数字签名的执行方式

6.2基于公钥密码体制的典型数字签名方案

6.2.1 RSA数字签名方案

6.2.2 E1Gamal数字签名方案

6.2.3数字签名标准DSS

6.2.4基于椭圆曲线密码的数字签名算法ECDSA

6.3特殊数字签名方案

6.3.1不可否认签名

6.3.2盲数字签名

6.3.3群签名

思考题与习题

第7章密钥管理技术

第8章身份鉴别技术

第9章序列密码

第10章密码技术应用

第11章密码分析基础

附录A密码学数学基础

附录B计算复杂性

附录C商用密码管理政策

参考文献

《应用密码学》

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