

《现代密码学》

图书基本信息

书名：《现代密码学》

13位ISBN编号：9787302373779

出版时间：2015-2

作者：杨波

页数：282

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

《现代密码学》

内容概要

《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》全面而详细地介绍现代密码学的理论和相关算法,可帮助读者将所学知识应用于信息安全的实践中。全书共分10章,内容包括现代密码学的基本概念、流密码、分组密码、公钥密码、密钥分配与密钥管理、消息认证和哈希函数、数字签名和认证协议、密码协议、可证明安全及网络加密与认证。

《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》从教材使用的角度考虑,概念清晰、结构合理、通俗易懂、内容深入浅出,并充分考虑方便教师在教学过程中的实施,同时还注意与其他专业课教学的衔接。《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》取材新颖,不仅介绍现代密码学所涉及的基础理论和实用算法,同时也涵盖了现代密码学的最新研究成果,力求使读者通过《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》的学习了解本学科最新的发展方向。《普通高等教育"十一五"国家级规划教材·高等院校信息安全专业系列教材:现代密码学(第3版)》可作为高等学校相关专业大学生和研究生的教材,也可作为通信工程师和计算机网络工程师的参考读物。

《现代密码学》

作者简介

杨波，北京大学学士，西安电子科技大学硕士、博士，陕西师范大学计算机科学学院教授，博士生导师，陕西省百人计划特聘教授，中国密码学会理事，中国密码学会密码算法专业委员会委员，《密码学报》编委。曾任华南农业大学信息学院，软件学院院长。2001年起在陕西师范大学计算机科学学院工作。2005年担任第四届中国信息和通信安全学术会议程序委员会主席，2009年担任中国密码学会年会副主席，2010年起担任The Joint Workshop on Information Security (JWIS) Co—General Chair。主持多项国家自然科学基金、863计划、国家密码发展基金、国防科技重点实验室基金，陕西省自认科学基金项目。

书籍目录

第1章引言

1.1信息安全面临的威胁

1.1.1安全威胁

1.1.2入侵者和病毒

1.1.3安全业务

1.2信息安全的模型

1.3密码学基本概念

1.3.1保密通信系统

1.3.2密码体制分类

1.3.3密码攻击概述

1.4几种古典密码

1.4.1单表代换密码

1.4.2多表代换密码

习题

第2章流密码

2.1流密码的基本概念

2.1.1同步流密码

2.1.2有限状态自动机

2.1.3密钥流产生器

2.2线性反馈移位寄存器

2.3线性移位寄存器的一元多项式表示

2.4优序列的伪随机性

2.5m序列密码的破译

2.6非线性序列

2.6.1Geffe序列生成器

2.6.2J—K触发器

2.6.3Pless生成器

2.6.4钟控序列生成器

习题

第3章分组密码

3.1分组密码概述

3.1.1代换

3.1.2扩散和混淆

3.1.3Feistel密码结构

3.2数据加密标准

3.2.1DES描述

3.2.2二重DES

3.2.3两个密钥的三重DES

3.2.4三个密钥的三重DES

3.3差分密码分析与线性密码分析

3.3.1差分密码分析

3.3.2线性密码分析

3.4分组密码的运行模式

3.4.1电码本模式

3.4.2密码分组链接模式

3.4.3密码反馈模式

3.4.4输出反馈模式

3.5 IDEA

3.5.1 设计原理

3.5.2 加密过程

3.6 AES算法——Rijndael

3.6.1 Rijndael的数学基础和设计思想

3.6.2 算法说明

习题

第4章 公钥密码

4.1 密码学中一些常用的数学知识

4.1.1 群、环、域

4.1.2 素数和互素数

4.1.3 模运算

4.1.4 模指数运算

4.1.5 费马定理、欧拉定理和卡米歇尔定理

4.1.6 素性检验

4.1.7 欧几里得算法

4.1.8 中国剩余定理

4.1.9 离散对数

4.1.10 平方剩余

4.1.11 计算复杂性

4.2 公钥密码体制的基本概念

4.2.1 公钥密码体制的原理

4.2.2 公钥密码算法应满足的要求

4.2.3 对公钥密码体制的攻击

4.3 RSA算法

4.3.1 算法描述

4.3.2 RSA算法中的计算问题

4.3.3 一种改进的RSA实现方法

4.3.4 RSA的安全性

4.3.5 对RSA的攻击

4.4 背包密码体制

4.5 Rabin密码体制

4.6 NTRU公钥密码系统

4.7 椭圆曲线密码体制

4.7.1 椭圆曲线

4.7.2 有限域上的椭圆曲线

4.7.3 椭圆曲线上的点数

4.7.4 明文消息到椭圆曲线上的嵌入

4.7.5 椭圆曲线上的密码

4.8 基于身份的密码体制

4.8.1 引言

4.8.2 双线性映射

4.8.3 IBE方案描述

习题

第5章 密钥分配与密钥管理

5.1 单钥加密体制的密钥分配

5.1.1 密钥分配的基本方法

5.1.2 实例

5.1.3 密钥的分层控制

- 5.1.4会话密钥的有效期
- 5.1.5无中心的密钥控制
- 5.1.6密钥的控制使用
- 5.2公钥加密体制的密钥管理
 - 5.2.1公钥的分配
 - 5.2.2用公钥加密分配单钥密码体制的密钥
 - 5.2.3Diffie—Hellman密钥交换
- 5.3密钥托管
 - 5.3.1美国托管加密标准简介
 - 5.3.2密钥托管密码体制的组成部分
- 5.4随机数的产生
 - 5.4.1随机数的使用
 - 5.4.2随机数源
 - 5.4.3伪随机数产生器
 - 5.4.4基于密码算法的随机数产生器
 - 5.4.5随机比特产生器
- 5.5秘密分割
 - 5.5.1秘密分割门限方案
 - 5.5.2Shamir门限方案
 - 5.5.3基于中国剩余定理的门限方案

习题

第6章消息认证和哈希函数

- 6.1消息认证码
 - 6.1.1消息认证码的定义及使用方式
 - 6.1.2产生MAC的函数应满足的要求
 - 6.1.3数据认证算法
- 6.2哈希函数
 - 6.2.1哈希函数的定义及使用方式
 - 6.2.2哈希函数应满足的条件
 - 6.2.3生日攻击
 - 6.2.4迭代型哈希函数的一般结构
- 6.3MD5哈希算法
 - 6.3.1算法描述
 - 6.3.2MD5的压缩函数
 - 6.3.3MD5的安全性
- 6.4安全哈希算法
 - 6.4.1算法描述
 - 6.4.2SHA的压缩函数
 - 6.4.3SHA与MD5的比较
 - 6.4.4对SHA的攻击现状
- 6.5HMAC
 - 6.5.1HMAC的设计目标
 - 6.5.2算法描述
 - 6.5.3HMAC的安全性

习题

第7章数字签名和认证协议

- 7.1数字签名的基本概念
 - 7.1.1数字签名应满足的要求
 - 7.1.2数字签名的产生方式

- 7.1.3数字签名的执行方式
- 7.2数字签名标准
 - 7.2.1DSS的基本方式
 - 7.2.2数字签名算法
- 7.3其他签名方案
 - 7.3.1基于离散对数问题的数字签名体制
 - 7.3.2基于大数分解问题的数字签名体制
 - 7.3.3基于身份的数字签名体制
- 7.4认证协议
 - 7.4.1相互认证
 - 7.4.2单向认证
- 习题
- 第8章密码协议
 - 8.1一些基本协议
 - 8.1.1智力扑克
 - 8.1.2掷硬币协议
 - 8.1.3数字承诺
 - 8.1.4不经意传输
 - 8.2零知识证明
 - 8.2.1交互证明系统
 - 8.2.2交互证明系统的定义
 - 8.2.3交互证明系统的零知识性
 - 8.2.4零知识证明协议的组合
 - 8.2.5图的三色问题的零知识证明
 - 8.2.6知识证明
 - 8.2.7简化的Fiat—Shamir身份识别方案
 - 8.2.8Fiat—Shamir身份识别方案
 - 8.3安全多方计算协议
 - 8.3.1安全多方计算问题
 - 8.3.2半诚实敌手模型
 - 8.3.3恶意敌手模型
- 习题
-
- 第9章可证明安全
- 第10章网络加密与认证
- 参考文献

《现代密码学》

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