

<<无线通信网中的安全技术>>

图书基本信息

书名：<<无线通信网中的安全技术>>

13位ISBN编号：9787115110534

10位ISBN编号：7115110530

出版时间：2003-7

出版时间：人民邮电出版社

作者：徐胜波

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>

<<无线通信网中的安全技术>>

内容概要

本书主要介绍无线通信网络中的安全技术。

第1章对无线通信网中的安全问题作了一般介绍，第2章介绍了一些基本的密码知识，第3章主要介绍对称密码系统和算法，第4章主要介绍非对称密码系统与算法，第5章主要介绍认证系统与算法，第6章主要介绍密钥分配与管理方案，第7~9章分别详细介绍移动通信网络、无线局域网和无线个人区域网络的安全技术，第10章重点介绍无线应用协议所包含的安全技术，并分析其安全性，最后以网上支付为例介绍移动电子商务。

本书适合从事无线通信网络安全工作的工程技术人员和相关专业的学生学习参考，对该方面知识有兴趣的读者也可以阅读参考。

<<无线通信网中的安全技术>>

书籍目录

第1章无线通信网络安全概述

- 1?1无线通信网络的发展
- 1?2无线通信网络中的不安全因素
 - 1?2?1无线窃听的内容、方法和手段
 - 1?2?2假冒攻击
 - 1?2?3信息篡改
 - 1?2?4服务后抵赖
 - 1?2?5重传攻击
- 1?3无线通信服务中的安全业务
 - 1?3?1保密性
 - 1?3?2身份认证性
 - 1?3?3数据完整性
 - 1?3?4服务不可否认性
- 1?4无线通信网络的安全机制
 - 1?4?1无线通信网络与密码技术
 - 1?4?2无线通信中的密码技术
- 小结

第2章保密系统的基本知识

- 2?1数字通信系统模型
- 2?2密码系统模型和密码体制
 - 2?2?1单钥与双钥密码体制
 - 2?2?2密码系统定义和要求
- 2?3密码分析
- 2?4保密系统的保密性与随机性
 - 2?4?1信息量和熵
 - 2?4?2完善保密性与随机性
 - 2?4?3唯一解距离、理论保密性与实际保密性
- 2?5复杂性理论简介
 - 2?5?1算法复杂性
 - 2?5?2问题的复杂性及其分类
- 小结

参考文献

第3章对称密码体制

- 3?1流密码
- 3?2分组密码
 - 3?3Rijndael密码体制
 - 3?3?1数学基础
 - 3?3?2系数在GF(28)中的多项式
 - 3?3?3设计原则
 - 3?3?4密码体制说明
 - 3?3?5Rijndael密码的实现
 - 3?3?6Rijndael密码的适应性
 - 3?4IDEA
 - 3?4?1算法的基本运算
 - 3?4?2加密过程

<<无线通信网中的安全技术>>

3?4?3子密钥产生器

3?4?4解密过程

3?4?5对合性的证明

3?5CAST?256

3?5?1算法说明

3?5?2设计原理

3?6RC?6

3?6?1密钥表

3?6?2加密

3?6?3解密

3?7KASUMI分组密码

3?7?1有关记号

3?7?2子函数FL

3?7?3子函数FO

3?7?4函数FI

3?7?5S盒

3?7?6加密运算

3?7?7密钥调度

小结

参考文献

第4章非对称密码体制

4?1基本原理

4?2RSA

4?2?1算法描述

4?2?2RSA安全性分析

4?3Rabin算法

4?3?1算法的描述

4?3?2安全性分析

4?4ElGamal加密算法

4?4?1ElGamal算法描述

4?4?2速度

4?5椭圆曲线密码体制

4?5?1椭圆曲线

4?5?2椭圆曲线上点的加法

4?5?3椭圆曲线上有理点数的确定

4?5?4群的阶的确定

4?5?5椭圆曲线密码体制的攻击方法

4?6NTRU密码体制

4?6?1算法的描述

4?6?2安全性分析

4?6?3NTRU的实现

4?6?4与其他公钥密码体制的比较

4?7GH密码体制

4?7?1格中的难解问题

4?7?2陷门函数的定义

4?7?3一个新的陷门函数

4?7?4求逆算法

<<无线通信网中的安全技术>>

4.7.5 生成算法

4.7.6 加密算法

4.7.7 签名算法

小结

参考文献

第5章 认证系统

5.1 无条件安全认证码

5.2 单向杂凑函数

5.2.1 一些重要的杂凑算法

5.2.2 基于对称分组密码算法的单向杂凑函数

5.2.3 不安全的杂凑函数

5.2.4 基于公开密码算法的杂凑算法

5.2.5 单向杂凑函数的选取

5.3 消息认证码

5.3.1 CBC-MAC

5.3.2 消息认证算法

5.3.3 双向MAC

5.3.4 Jueneman方法

5.3.5 RIPE-MAC

5.3.6 IBC-Hash

5.3.7 序列密码MAC

5.3.8 单向杂凑函数MAC

5.4 数字签名

5.4.1 RSA签名方案

5.4.2 ElGamal 签名方案

5.4.3 美国签名标准 (DSS)

5.4.4 Lamport签名方案

5.4.5 不可否认签名

5.4.6 故障停止式签名方案

5.5 身份认证方案

5.5.1 Schnorr身份认证方案

5.5.2 Okamoto身份认证方案

5.5.3 Guillou-Quisquater身份认证方案

5.5.4 基于身份的身份认证方案

小结

参考文献

第6章 密钥交换

6.1 密钥的产生与管理

6.1.1 通行短语

6.1.2 X.917 密钥产生

6.1.3 DoD 密钥产生

6.1.4 密钥的存储

6.1.5 密钥备份

6.1.6 密钥的泄露和有效期

6.2 密钥交换

6.2.1 基于对称密码学的密钥交换

6.2.2 基于公开密钥密码学的密钥交换

<<无线通信网中的安全技术>>

- 6?2?3 联锁协议
- 6?2?4 具有认证功能的密钥交换方案
- 6?2?5 密钥和消息传输
- 6?2?6 密钥和消息广播
- 6?3 认证和密钥交换
 - 6?3?1 Wide?Mouth Frog 协议
 - 6?3?2 Yahalom 协议
 - 6?3?3 Needham?Schroeder 协议
 - 6?3?4 Otway?Rees 协议
 - 6?3?5 Kerberos 协议
 - 6?3?6 KryptoKnight
 - 6?3?7 SESAME
 - 6?3?8 IBM 通用密码体系
 - 6?3?9 ISO 密钥分配和认证框架
 - 6?3?10 保密增强邮件
- 6?4 公开密码密钥交换方案
 - 6?4?1 Diffie?Hellman 算法
 - 6?4?2 三方和多方 Diffie?Hellman
 - 6?4?3 扩展 Diffie?Hellman
 - 6?4?4 不用交换密钥的密钥交换
 - 6?4?5 站间协议
 - 6?4?6 Shamir 的三次传递协议
 - 6?4?7 加密密钥交换
 - 6?4?8 加强的密钥协商
 - 6?4?9 会议密钥分发和秘密广播
 - 6?4?10 会议密钥分发
 - 6?4?11 Tatebayashi?Matsuzaki?Newman
- 小结
- 参考文献
- 第7章 移动通信网络中的安全技术
 - 7?1 移动通信网络简介
 - 7?1?1 发展概述
 - 7?1?2 网络结构
 - 7?2 不安全因素分析
 - 7?2?1 无线接口中的不安全因素
 - 7?2?2 网络端的不安全因素
 - 7?2?3 移动端的不安全因素
 - 7?2?4 攻击风险分析
 - 7?3 安全业务
 - 7?3?1 保密性业务类
 - 7?3?2 认证性业务类
 - 7?3?3 应用层安全业务
 - 7?3?4 移动电话保护
 - 7?4 GSM 网络中的安全技术
 - 7?4?1 身份认证与密钥分配方案
 - 7?4?2 语音和数据加密方案的实现算法
 - 7?4?3 安全性分析

<<无线通信网中的安全技术>>

7.5.3 GPP网络中的安全技术

7.5.3.1 GPP网络的基本结构

7.5.3.2 身份认证和密钥分配方案

7.5.3.3 GPP中的加密技术

7.5.3.4 完整性检测方案与算法

7.5.3.5 安全性分析

7.6 公钥密码技术在移动通信网络中的应用

7.6.1 为什么移动通信网络需要公钥密码技术

7.6.2 基于公钥密码技术的身份认证与密钥分配方案

7.6.3 公钥密码技术在移动通信网络中的应用前景

小结

参考文献

第8章 无线局域网中的安全技术

8.1 概述

8.1.1 IEEE 802.11b 标准简介

8.1.2 无线局域网络架构

8.1.3 无线局域网络的应用

8.2 无线局域网中的安全技术

8.2.1 扩展服务组身份号ESSID

8.2.2 访问表

8.2.3 认证

8.2.4 加密

8.3 关于WEP的安全性

8.3.1 统计攻击

8.3.2 完整性攻击

8.3.3 假冒无线站攻击

8.3.4 RC4密钥方案攻击

8.4 改进措施

8.4.1 WEP2算法

8.4.2 增强安全网络

8.4.3 IEEE 802.1x标准

8.5 无线局域网应用

小结

参考文献

第9章 无线个人区域网络中的安全技术

9.1 无线个人区域网络概述

9.1.1 蓝牙技术

9.1.2 网络拓扑

9.1.3 蓝牙协议栈

9.1.4 基于蓝牙技术的无线个人区域网络

9.2 蓝牙规范中的密码算法

9.2.1 加密算法E0

9.2.2 认证算法E1和加密密钥生成算法E3

9.2.3 密钥生成算法E21和E22

9.3 蓝牙规范中的密钥管理

9.3.1 密钥类型

9.3.2 初始密钥Kinit生成

<<无线通信网中的安全技术>>

- 9?3?3设备密钥KA的生成
- 9?3?4组合密钥KAB的生成
- 9?3?5主密钥Kmaster的生成
- 9?3?6连接密钥的使用与修改

9?4认证方案

9?5蓝牙规范中的加密

9?5?1加密密钥Kc的生成

9?5?2加密密钥长度协商

9?5?3加密方式

9?5?4加密过程

9?6安全性分析

9?6?1加密算法E0的安全性

9?6?2初始化密钥的安全性

9?6?3设备密钥的安全性

9?6?4蓝牙设备地址的安全性

小结

参考文献

第10章无线应用协议与移动电子商务

10?1无线应用协议概述

10?1?1WAP协议结构

10?1?2WAP网络模型

10?1?3WAP应用

10?2WAP安全框架

10?2?1安全威胁与安全服务需求

10?2?2WAP承载网络的安全性

10?2?3WAP安全框架

10?2?4无线个人身份模块和无线公共密钥设施

10?3WTLS中的握手协议

10?3?1密钥交换

10?3?2身份认证

10?3?3握手协议的分类

10?3?4主密钥的生成

10?3?5加密与MAC

10?4WAP应用中的端到端安全性

10?4?1WAP应用网络的端到端安全性

10?4?2实现WAP传输层的端到端安全性

10?5WAP电子转帐

10?5?1服务准备阶段

10?5?2WAP电子转帐过程

10?5?3安全性分析

<<无线通信网中的安全技术>>

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>