

<<通信网的安全>>

图书基本信息

书名：<<通信网的安全>>

13位ISBN编号：9787560607115

10位ISBN编号：756060711X

出版时间：1999-4

出版时间：西安电子

作者：王育民

页数：651

字数：990000

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>

## <<通信网的安全>>

### 内容概要

本书研究和讨论通信网安全的理论与技术。

本书第1章介绍通信网安全概论，其余各章分为三大部分。

第一部分为第2-5章，介绍密码学的基础知识，包括古典密码、信息论、计算复杂度、流密码、分组密码和双钥密码的原理和算法以及一些新的密码体制。

第二部分为第6-9章，介绍认证理论与技术，包括认证、认证码、杂凑函数、数字签字、身份证明、认证和协议的理论与算法。

第三部分为第10-13章，介绍通信网的安全技术，包括网络安全的基础知识、网络加密方式与密钥管理、实际系统的安全与安全管理技术。

有关章未给出所需的数学基础知识。

书末给出一些重要的信息安全技术标准和有关的参考文献。

本书可作为有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。

## &lt;&lt;通信网的安全&gt;&gt;

## 书籍目录

序前言第1章 通信网络安全概念 1.1 开放(分布)网络环境 1.2 对网络安全的需求 1.3 通信网络的安全策略 1.4 安全威胁与防护措施 1.5 通信网络安全业务 1.6 开放系统互联(OSI)基本参考模型及TCP/IP协议第2章 密码理论与技术(一)——保密学基础 2.1 保密学的基本概念 2.2 密码体制分类 2.3 古典密码 2.4 初等密码分析 2.5 信息论与密码学 2.6 计算复杂性与密码学 附录2.A 素数与互素数 附录2.B 模 $q$ 算术第3章 密码理论与技术(二)——流密码及拟随机数生成器 3.1 流密码的基本概念 3.2 线性反馈移位寄存器序列 3.3 基于非线性反馈移位寄存器的流密码 3.4 拟随机数生成器的一般理论 3.5 快速软、硬件实现的流密码算法 3.6 混沌密码序列 3.7 量子密码 附录3.A 有限域的基本概念 附录3.B 有限域上的线性代数第4章 密钥理论与技术(三)——分组密码 4.1 分组密码概述 4.2 代换网络 4.3 迭代分组密码的分类 4.4 DES 4.5 Markov密码和差分密码分析 4.6 IDEA 4.7 SAFERK-64 4.8 GOST 4.9 RC-5 4.10 Blowfish 4.11 CRAB 4.12 用单向杂凑迭代函数构造分组密码算法 4.13 分组密码运行模式 4.14 分组密码的组合 4.15 其它分组密码第5章 密码理论与技术(四)——双(公)钥密码体制 5.1 双钥密码体制的基本概念 5.2 RSA密码体制 5.3 背包密码体制 5.4 Rabin密码体制 5.5 ElGamal密码体制 5.6 椭圆曲线密码体制 5.7 McEliece密码体制 5.8 LUC密码体制 5.9 秘密共享密码体制 5.10 有限自动机密码体制 5.11 概率加密 5.12 其它双钥密码体制 附录5.A 大素数求法 附录5.B 快速指数算法 附录5.C 离散对数的计算第6章 认证理论与技术(一)——认证、认证码、杂凑函数 6.1 认证与认证系统 6.2 认证码 6.3 杂凑函数 6.4 单向迭代杂凑函数的设计理论 6.5 MD-4和MD-5杂凑算法 6.6 安全杂凑算法(SHA) 6.7 GOST杂凑算法 6.8 其它杂凑算法第7章 认证理论与技术(二)——数字签字 7.1 数字签字基本概念 7.2 RSA签字体制 7.3 Rabin签字体制 7.4 ElGamal签字体制 7.5 Schnorr签字体制 7.6 DSS签字标准 7.7 GOST签字标准 7.8 ESIGN签字体制 7.9 Okamoto签字体制 7.10 OSS签字体制 7.11 离散对数签字体制 7.12 不可否认签字 7.13 防失败签字 7.14 盲签字 7.15 群签字 7.16 数字签字体制中的潜信道 7.17 其它数字签字第8章 认证理论与技术(三)——身份证明 8.1 身份证明 8.2 通行字(口令)认证系统 8.3 个人特征的身份证明技术 8.4 零知识证明的基本概念 8.5 零知识身份证明的密码体制 8.6 灵巧卡技术及其应用第9章 认证理论与技术(四)——安全协议 9.1 协议的基本概念 9.2 安全协议的分类及基本密码协议 9.3 秘密分拆协议 9.4 会议密钥分配和秘密广播协议 9.5 时戳业务 9.6 公平协议(一)——公平竞争 9.7 公平协议(二)——同时签约 9.8 公平协议(三)——安全选举 9.9 公平协议(四)——安全多方计算 9.10 密码协议的安全性及其设计规范 9.11 协议的形式语言证明第10章 通信网的安全技术(一)——基础 10.1 接入控制 10.2 客户机/服务器网络的安全 10.3 开放软件基础 10.4 防火墙 10.5 入侵的审计、追踪与检测技术 10.6 隐信道 10.7 网络病毒与防范 10.8 可信赖网络系统第11章 通信网的安全技术(二)——网络加密与密钥管理 11.1 网络加密的方式及实现 11.2 硬件加密、软件加密及有关问题 11.3 密钥管理的基本概念 11.4 密钥长度与安全性 11.5 密钥生成 11.6 密钥分配 11.7 密钥的证实 11.8 密钥的保护、存储与备份 11.9 密钥的泄露、吊销、过期与销毁 11.10 密钥控制 11.11 多个管区的密钥管理 11.12 密钥托管和密钥恢复 11.13 密钥管理系统第12章 通信网的安全技术(三)——实际系统的安全 12.1 Kerberos认证系统 12.2 X.509检索认证业务 12.3 PGP——E-mail安全保密系统之一 12.4 PEM——E-mail安全保密系统之二 12.5 Krypto?Knight认证系统 12.6 无线网的安全认证系统 12.7 Internet上电子商务系统的安全第13章 通信网的安全技术(四)——安全管理技术与标准 13.1 安全管理的概念 13.2 OSI安全管理概述 13.3 SNMP的基本概念 13.4 SNMPv2的安全管理 13.5 风险分析 13.6 安全性评估标准 附录13.A 信息安全技术标准参考文献

<<通信网的安全>>

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>