

<<网络与信息安全>>

图书基本信息

书名：<<网络与信息安全>>

13位ISBN编号：9787113070588

10位ISBN编号：7113070582

出版时间：2006-6

出版单位：中国铁道

作者：王凤英，程震主编

页数：367

字数：578000

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>

## <<网络与信息安全>>

### 内容概要

本书力求理论研究与实际应用相结合,内容新颖而丰富,系统地阐述了计算机安全的各个方面,内容包括网络与信息安全的概念和术语;密码学及加密技术的使用;操作系统、数据库和网络的安全:公钥基础设施、访问控制、系统审计、入侵检测、计算机病毒的防御、电子邮件的安全性及匿名转发、加密的新型研究方向等。

本书注重介绍信息安全领域一些最新的研究成果,包括现代加密的新型研究方向,混沌密码和量子密码;近几年的研究热点,信息隐藏与数字水印;用于密码分析的模差分方法;基于角色的访问控制;PKI和PMI;IPV6的安全等。

本书可作为计算机、信息安全、通信、计算机网络等专业本科生、研究生的教材,也可作为相关专业领域研究人员和专业技术人员的参考书。

## &lt;&lt;网络与信息安全&gt;&gt;

## 书籍目录

第1章 网络与信息安全综述 1.1 网络安全的基本概念 1.2 网络安全的层次结构 1.2.1 物理安全  
1.2.2 安全控制 1.2.3 安全服务 1.3 网络安全威胁 1.3.1 网络安全威胁的类型 1.3.2 网络安全威胁的动机 1.4 安全模型 1.5 基本安全技术 1.5.1 防火墙 1.5.2 加密 1.5.3 身份认证 1.5.4 数字签名 1.6 网络安全的评价标准 1.6.1 国际标准 1.6.2 国内标准 1.7 研究网络与信息安全的意义  
1.7.1 网络安全与政治 1.7.2 网络安全与经济 1.7.3 网络安全与社会稳定 1.7.4 网络安全与军事 小结 习题1  
第2章 对称密钥密码体系 2.1 密码体系的原理和基本概念 2.1.1 专业术语 2.1.2 安全密码 2.1.3 对称密码和非对称密码 2.1.4 密码分析 2.2 数据加密标准(DES) 2.2.1 DES的历史 2.2.2 DES的算法 2.2.3 DES的工作模式 2.2.4 三重DES 2.3 高级加密标准(AES) 2.3.1 RC6算法 2.3.2 SERPENT算法 2.3.3 Rijndael算法 2.4 序列密码 2.4.1 一次一密乱码本 2.4.2 A5算法 2.5 其他对称密码算法 2.5.1 IDEA算法 2.5.2 Blowfish算法 2.5.3 PKZIP算法 小结 习题2  
第3章 单向散列函数 3.1 单向散列函数概述 3.2 MD5算法 3.2.1 算法 3.2.2 举例 3.3 SHA.1算法 3.3.1 算法 3.3.2 举例 3.3.3 SHA-1与MD5的比较 3.4 消息认证码(MAC) 3.5 对单向散列函数的攻击 3.5.1 字典攻击 3.5.2 生日攻击 小结 习题3  
第4章 公钥密码体系 4.1 公钥密码概述 4.2 RSA密码系统 4.3 Diffie-Hellman密钥交换 .....第5章 混沌密码与量子密码第6章 信息隐藏技术第7章 操作系统安全第8章 因特网安全第9章 数据库系统安全第10章 PKI技术第11章 电子邮件安全及PGP第12章 Web电子商务安全第13章 防火墙技术第14章 访问控制与系统审计第15章 计算机病毒与防范第16章 入侵检测第17章 网络安全管理参考文献

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>