第一图书网, tushu007.com

<<信息系统的安全与保密>>

图书基本信息

书名：<<信息系统的安全与保密>>

13位ISBN编号：9787302032137

10位ISBN编号：7302032130

出版时间：1998-12

出版时间：清华大学出版社

作者：陈元

页数：150

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

内容概要

本书全面系统地论述了信息系统安全保密的基础理论及实用技术。
全书共分四部分，第一部分概述了计算机信息系统安全保密的重要性及研究内容；第二部分介绍了密码学的基础理论知识，讲述了传统密钥体制和公开密钥体制；第三部分详细讲述了信息系统安全保密的实用技术，并且重点强调了网络环境下防火墙安全措施的应用；第四部分通过对计算机病毒危害及症状的分析，论述了防止病毒的常用方法。
本书内容丰富，覆盖面广，适用于大专院校信息管理与信息系统、计算机应用等相关专业学生阅读，而且对从事计算机信息系统安全工作的技术人员也有极大的帮助。

<<信息系统的安全与保密>>

书籍目录

目录
第1章 信息系统安全概述
1.1信息系统安全的重要意义
1.信息系统的概念
2.信息系统受到的威胁
3.对信息系统攻击的主要手段
1.2信息安全技术的研究内容
1.信息安全技术的含义
2.信息系统安全模型
3.信息安全保密研究内容介绍
1.3计算机信息系统安全法规和机构
1.计算机信息系统安全的法规
2.国内外著名安全机构
第2章 预备知识
2.1数论基础
1.引言
2.Euclid算法
3.同余
4.二次剩余
2.2信息论基础
1.熵的概念
2.互信息
2.3 计算复杂性简介
1.算法复杂性
2.问题的分类
3.几个例子
第3章 传统密码体制
3.1密码学的基本概念
3.2保密系统的Shannon理论
1.保密系统的Shannon模型
2.理想保密与完善保密
3.3序列密码
1.序列密码的工作原理
2.线性移位寄存器（LFSR）
3.序列密码的设计
3.4分组密码
1.分组密码的工作原理
2.数据加密标准
第4章 公开密钥密码体制
4.1RSA体制和Rabin体制
1.RSA体制
2.Rabin体制
3.素性检测
4.2背包体制
1.密钥生成

2.加密过程
3.解密过程
4.3EIGamal体制
1.密钥生成
2.加密过程
3.解密过程
4.4概率加密体制
1.GM体制
2.BBS体制
第5章 信息安全与保密技术
5.1操作系统的安全与保密
1.安全操作系统设计
2.操作系统保护的对象及方法
3.访问控制
4.基于口令的用户认证
5.常用操作系统和工具软件的安全保护特例
5.2数据库的安全与保密
1.安全数据库的方法
2.数据库的加密方法
3.数据库的恢复
4.Microsoft Access数据库的安全保护
5.数据库安全保密实例——通用智能题库安全保密的实现
5.3数字签名
1.数字签名及其特点
2.数字签名算法DSA
3.使用DSA生成、验证签名的例子
4.数字签名算法GOST
5.4智能卡
1.智能卡的发展
2.智能卡的种类和特点
3.智能卡的应用前景
4.智能卡的安全问题
5.5EDI系统的安全与保密
1.EDI的基本概念
2.EDI系统的功能
3.EDI系统的安全问题
4.EDI系统安全对策
5.EDI安全服务实现机制
第6章 网络的安全与保密
6.1网络安全的威胁与对策
1.网络模型与协议
2.开放互联网络的安全服务
3.网络通信中的一般加密方式
4.网络安全的威胁及相应的对策
6.2网络系统的密钥管理方法
1.Diffie－Hellman密钥管理方法
2.基于公开钥加密体制的密钥管理方法

3.基于KPS（KeyPredistributionSystem，密钥预分配系统）的密钥管理方法
6.3Internet安全与防火墙技术
1.Internet服务及安全对策
2.防火墙的概念与体系结构
3.防火墙的优点与用途
4.防火墙的设计
6.4利用IP欺骗进行攻击及其预防策略
1.利用IP欺骗进行攻击
2.IP欺骗的预防策略
6.5面向对象的分布式环境的认证与加密系统
1.认证系统
2.加密系统
6.6秘密的电子邮件PEM
1.PEM信息的形成
2.密钥管理方式
第7章 计算机病毒理论
7.1计算机病毒的基本概念
1.病毒的产生
2.病毒的特征
3.病毒的分类
7.2计算机病毒的分析
1.病毒的破坏现象
2.病毒程序结构
3.感毒的症状
4.病毒的检测
7.3计算机病毒的防治
1.病毒的防范
2.清除计算机病毒的原则
3.常用杀毒软件介绍
7.4典型病毒的危害与清除
1.大麻病毒
2.黑色星期五病毒
3.N64病毒
4.米开朗基罗病毒
5.巴基斯坦病毒
附录一 中华人民共和国计算机信息系统安全保护条例
附录二 计算机信息系统保密管理暂行规定
附录三 面向对象分布式系统Oz加密系统中的密钥类程序

第一图书网, tushu007.com

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