

<<PKI技术>>

图书基本信息

书名：<<PKI技术>>

13位ISBN编号：9787111141686

10位ISBN编号：7111141687

出版时间：2004-6-1

出版时间：机械工业出版社

作者：陈昕,宁宇鹏

页数：136

字数：219000

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>

<<PKI技术>>

内容概要

PKI（公钥基础设施）是一种利用密码技术为网上安全通信提供一整套安全服务的基础平台。如同其他基础设施（电力、水利基础设施）一样，公钥基础设施也一样能为各种不同安全需求的用户、提供各种不同的安全服务。

本书分为四部分，共10章。

第一部分为基础知识，主要介绍了PKI的概念、主要内容、理论基础；第二部分为PKI体系结构，主要介绍了PKI体系和服务功能，以及PKI建设使用中所遇到的问题；第三部分PKI技术标准，主要介绍了现有的PKI技术标准体系；第四部分为应用案例，主要介绍了现有利用PKI实现的安全协议，以及网上银行、网上证券及电子税务的PKI应用系统。

本书适用于准备参加“国家信息化安全教育认证（ISEC）”考试的人员，还适合信息产业相关管理部门人员、PKI建设运营人员、IT人员及有关业务人员学习和参考，也可作为大专院校有关专业的参考教材和电子政务、电子商务的培训教材。

<<PKI技术>>

书籍目录

出版说明前言第一部分 基础知识第1章 绪论1.1 什么是PKI1.2 为什么需要PKI1.3 PKI的理论基础1.4 PKI技术发展现状及趋势1.5 PKI体系现存问题1.6 练习题第2章 密码和密钥2.1 密码学基础2.2 对称密钥密码2.2.1 概述2.2.2 对称密码的分类2.2.3 一次一密乱码本 (One-time pad) 2.3 非对称密钥密码2.3.1 概述2.3.2 非对称密码算法的分类2.4 Hash算法2.4.1 概述2.4.2 Hash算法的分类2.5 使用公钥算法的加密与数字签名2.5.1 使用公钥算法的加密2.5.2 数字签名2.5.3 完整的公钥加密与签名2.6 密钥管理2.6.1 概述2.6.2 密钥的生存周期2.7 练习题第3章 数字证书和目录服务3.1 数字证书概述3.1.1 什么是数字证书3.1.2 X.509数字证书3.2 证书验证3.3 数字证书的使用3.4 数字证书的存储3.5 数字证书生命周期3.6 目录服务3.6.1 概述3.6.2 X.500协议3.6.3 LDAP协议3.7 练习题第二部分 PKI体系结构第4章 PKI及其构件4.1 综述4.2 CA、RA与EE4.3 PKI运作4.4 CA的体系结构4.5 RA的体系结构4.6 PMI4.7 练习题第5章 PKI系统实际运作5.1 交叉认证5.2 CPS5.3 PKI的构建5.3.1 构建PKI的两种模式5.3.2 两种模式的比较5.4 练习题第6章 PKI涉及到的法律问题6.1 国外PKI相关法律建设状况6.2 我国PKI相关法律建设状况6.3 如何构建我国的PKI法律体系6.3.1 立法考虑6.3.2 涵盖的内容6.4 练习题第三部分 技术标准第7章 PKI技术标准7.1 ITU - T X.509及相关标准7.1.1 概述7.1.2 ITU-T X.509 Edition 17.1.3 ITU - T X.509 Edition 27.1.4 ITU - T X.509 Edition 3 (1997) 7.1.5 ITU - T X.509 Edition 4 (2000) 7.1.6 ITU - T的其他标准7.2 PKIX系列标准7.2.1 PKIX系列协议7.2.2 PKI的实体对象说明7.3 WPKI标准7.4 SSL / TLS协议7.5 SET协议7.6 OpenPGP和S / MIME协议7.7 PMI标准简介7.8 练习题第四部分 应用案例第8章 PKI应用及案例8.1 PKI应用8.1.1 Web安全8.1.2 安全电子邮件8.1.3 VPN8.2 PKI案例8.2.1 电子税务8.2.2 网上银行8.2.3 网上证券8.3 成熟PKI系统简介8.3.1 商业应用8.3.2 政府应用第9章 电子商务认证机构管理基础9.1 电子商务认证机构的管理9.2 电子商务认证机构的安全9.3 认证机构的安全需求9.3.1 CA系统安全9.3.2 通信安全9.3.3 信息系统安全9.3.4 数据安全9.4 认证机构安全性的实现9.4.1 物理安全实现9.4.2 密码安全实现9.4.3 密钥安全实现9.4.4 通信安全实现9.4.5 信息系统安全实现9.4.6 人员安全实现9.4.7 环境安全实现9.4.8 用户数据保护9.4.9 安全审计实现第10章 电子商务认证机构可信评估10.1 CA系统安全性评估10.2 认证机构安全评估流程附录附录1 术语表附录2 习题答案

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>