

<<PKI原理与技术>>

图书基本信息

书名：<<PKI原理与技术>>

13位ISBN编号：9787811142259

10位ISBN编号：7811142252

出版时间：2007-8

出版时间：电子科技大学出版社

作者：余遥 7 轿 编著

页数：239

字数：386000

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原理与技术>>

内容概要

本书为普通高等学校信息安全“十一五”规划教材之一。

全书共10章，主要讲述了PKI（公钥基础设施）理论基础、标准、应用及前景等，从工程的角度介绍了PKI体制和各关键技术的实施。

本书既可作为信息安全或计算机专业本科生、专科生的教材，也可作为相关领域专业技术人员的参考用书。

书籍目录

第1章 PKI概论 1.1 PKI的历史背景 1.2 PKI理论基础 1.3 公钥基础设施的内容 1.4 PKI标准 1.5 PKI的应用及前景第2章 数学准备 2.1 群论基础 2.2 数论基础 2.3 RSA密码体制 2.4 椭圆曲线加密算法概述第3章 数字证书 3.1 数字证书概述 3.2 数字签名的引入 3.3 数字证书 3.4 数字证书的层次 3.5 证书生命周期与CRL 3.6 PMI属性证书和OCSP介绍第4章 PKI的信任模型 4.1 信任模型的概念 4.2 多种信任模型介绍第5章 CA (CERTIFICATE AUTHORITY) 系统 5.1 产生背景及原理 5.2 CA的概念 5.3 CA系统结构第6章 CA系统功能 6.1 CA功能概述 6.2 CA和RA的相互验证 6.3 CA之间的交叉认证 6.4 CA与其他系统的消息传递 6.5 证书的更新 6.6 证书的撤销 6.7 证书存储和归档备份 6.8 密钥的生成以及备份 6.9 使用CA和处理证书的流程第7章 注册机关 (RA) 7.1 RA总述 7.2 RA功能 7.3 证书请求消息格式 7.4 传输协议 7.5 RA实现示例第8章 轻量级目录访问协议 (LDAP) 8.1 目录服务的概念 8.2 目录服务的特点 8.3 X.500目录标准 8.4 轻量级目录访问协议LDAP 8.5 轻量级目录访问协议的特点 8.6 LDAP基本模型 8.7 LDAP协议基本元素 8.8 LDAP协议操作 8.9 分布式LDAP 8.10 LDAP存储数字证书 8.11 LDAP应用程序接口第9章 无线PKI (wPKI) 9.1 WPKI的体系结构 9.2 WPKI与有线PKI的区别 9.3 WPKI的加密算法和密钥 9.4 WAP概述第10章 WTLS协议 10.1 WTLS基本过程 10.2 WTLS与TLS 10.3 WTLS提供的主要服务 10.4 WTLS的安全 10.5 WTLS结构附录

<<PKI原理与技术>>

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>