<<公钥基础设施>>

图书基本信息

书名：<<公钥基础设施>>

13位ISBN编号：9787111296553

10位ISBN编号：7111296559

出版时间：2010-4

出版时间：机械工业出版社

作者：李建华 主编

页数：208

<<公钥基础设施>>

前言

随着信息技术的迅速发展，信息已成为当今社会的一种重要资源。
计算机系统和通信网络的广泛应用，增加了人们在信息存储及信息交流中对这些系统的依赖性。
随着信息资源的不断开发利用，政府管理、企业生产、社会公共服务、金融、财税等的信息化、网络化已经在全世界范围内迅猛展开。
因此，信息系统的安全存储、传播、处理等问题越来越受到人们的关注。
同时，由于计算机网络的开放性、社会性和共享性，其安全性也已经成为人们关注的焦点，网络犯罪行为日趋严重，各种敏感信息（国家机密、商业机密、个人隐私等）面临着史无前例的巨大威胁。
因而保护重要敏感信息免遭泄露，确保网络信息系统的安全性极为重要。
传统的密码加密技术主要面向单个计算机，而针对整个网络体系而言，公钥基础设施（PKI）理论及应用是保证网络信息安全的关键技术。
PKI理论及应用是一门新兴的科学，是随着计算机及互联网的发展而壮大起来的。
该学科以密码学及其技术为基础，在网络信息的安全防护中起到了极其重要的作用。
密码学的不断发展，推动着信息安全基础设施的不断发展。
信息安全基础设施主要包括两个大的发展方向。

<<公钥基础设施>>

内容概要

公钥基础设施（PKI）理论及应用是一门年轻的学科。
本书概述了传统的密码学基础与技术，在此基础上详细地叙述了PKI体系结构、证书管理体系、PKI应用、密钥管理、密钥建立的实施、相关密钥协议、PMI体系结构、PMI的管理体系和PMI应用实施等方面的内容及相关进展情况。
本书可作为高等院校信息安全专业的教材，也可作为高等院校电子信息类、计算机类等相关专业的教材和参考资料。

<<公钥基础设施>>

书籍目录

<<公钥基础设施>>

章节摘录

插图：随着信息技术和网络技术的迅速发展，各种基于网络信息系统的应用服务蓬勃兴起，给人们的工作和生活带来了各种便利，同时也带来了新的挑战，网络信息系统中的安全问题越来越引起人们的重视。
当前，网络信息安全所面临的最大的问题就是如何保障开放式网络环境中各实体建立相互之间的信任关系，以及如何保证信息的真实性、完整性、机密性和不可否认性。
公钥基础设施（：Public Key Infrastructure，PKI）技术被认为是解决以上网络信息安全问题的重要技术，并在电子商务、电子政务以及安全电子邮件等众多安全领域得到了广泛的应用。
因此，学习和掌握PKI成为了现代网络维护人员和信息系统开发人员的迫切需求。
经过近20年的发展，作为提供信息安全服务的普适性基础设施，无论从理论上、技术上还是法律规范上，PKI技术体系发展都已经日趋成熟。
在理论上，以公钥密码学为基础的密码算法、协议、认证方法得到了全面发展，成为PKI技术安全性的保障；在技术上，数字证书生命周期管理、数字证书格式以及PKI实体间通信协议等方面的国内外相关标准的制定，为PKI技术解决互操作性难题奠定了基础；在法律规范上，国内以《电子签名法》、《电子认证服务管理办法》等为代表的PKI应用相关法律、法规的颁布进一步规范了PKI技术的应用行为。

<<公钥基础设施>>

编辑推荐

《公钥基础设施(PKI)理论及应用》：PKI的概念与理论基础PKI体系结构与应用密钥管理与实施PMI管理体系PKI相关组织和标准

<<公钥基础设施>>

版权说明