

<<信息安全理论与实务>>

图书基本信息

书名：<<信息安全理论与实务>>

13位ISBN编号：9787113040932

10位ISBN编号：7113040934

出版时间：2001-04

出版时间：中国铁道出版社

作者：陈彦学

页数：253

字数：393000

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>

## <<信息安全理论与实务>>

### 内容概要

在电子商务高速发展的今天，信息安全领域已倍受重视。

本书会让你在最短的时间内获得信息安全领域中的一些专业知识。

书中详细介绍了密码学的基本知识，及一些市面上常见的安全协议、标准内容，如：PKCS、SSL、X.509、LDAP等。

图文并茂的教学方式，可使读者轻松入门，详细地介绍了信息安全领域的基本知识，如密码学的基本知识；常见的安全协议、标准内容，如PKCS、SSL、X.509、LDAP等，层次清楚的范例程序，能使人快速有效地掌握安全领域的专业知识，书中提供了大量的专业网址，便于读者深入研究。

## 书籍目录

第1章 导论 1.1 什么叫信息安全 1.2 网络与信息安全 1.3 安全系统的基本概念第2章 密码学算法简介 2.1 对称密钥密码学简介 2.1.1 DES算法 2.1.2 IDEA加密算法 2.1.3 AES (Advanced Encryption Standards) 下一代对称密钥系统 2.1.4 对称密钥加密模式 2.2 公开密钥密码系统 2.2.1 公开密钥密码概论 2.2.2 RSA公开密钥密码技术 2.2.3 DSA数字签名技术 2.2.4 Diffie-Hellman密钥交换系统 2.2.5 单向杂凑函数 2.3 一些经验谈第3章 公开密钥密码标准 (PKCS) 3.1 PKCS简介 3.2 PKCS # 1 RSA加密标准 3.2.1 RSA公钥及密钥储存格式 3.2.2 数据转换程序 (Data Conversion Primitives) 3.2.3 密码相关程序 (Cryptographic Primitives) 3.2.4 编码程序 (Encoding Methods) 3.2.5 加解密作业程序 3.2.6 签名作业程序 3.3 PKCS # 3 Diffie - Hellman密钥交换标准 3.4 PKCS # 5使用密码的加密标准 3.4.1 密钥导出函数 3.5 PKCS # 6凭证扩充标准 3.6 PKCS # 7密码信息封装标准 3.7 PKCS # 8密钥数据格式标准 3.8 PKCS # 9可供选择的数据格式 3.9 PKCS # 10密钥凭证索取标准 3.10 PKCS # 11密码组件接口标准 3.11 PKCS # 12个人信息交换格式标准 3.12 PKCS # 15密码组件数据格式标准 3.13 小结第4章 公开密钥认证中心标准简介 4.1 前言 4.2 简单认证程序 (Simple Authentication Procedure) 4.3 强认证程序 (Strong Authentication Procedure) 4.3.1 使用者公钥的取得 4.4 凭证扩充及凭证废止列表扩充部分 (Certificate And CRL Extensions) 4.5 现行PKI的运作方式的简介 4.6 无线通信PKI (WPKI) 的介绍 4.6.1 WPKI概论 4.6.2 WPKI安全通信模式 4.6.3 密钥的使用 4.7 小结第5章 安全协议介绍 5.1 政府机关电子公文流转安全协议 5.1.1 协议目的 5.1.2 电子公文完整性及发文单位认证的验证协议 5.1.3 电子公文防窃取的验证协议 5.1.4 收文端认证及收文端已签收的证协议 5.1.5 电子公文佐证的验证协议 5.1.6 电子公文公证的验证协议 5.1.7 其它相关的想法 5.2 SET安全协议 5.2.1 协议目的 5.2.2 SET安全协议的介绍 5.3 TLS (SSL) 安全协议 5.4 S/MIME密码信息文法 5.4.1 SignedData安全模式数据封装格式 5.4.2 其它安全模式数据封装格式简介 5.5 IPsec (Internet Protocol Security) 5.6 安全协议的破解 5.6.1 PKCS # 1 1.5版的破解 5.6.2 SET安全未周全的地方 5.7 小结第6章 信息安全其它相关技术 6.1 IC卡规格简介 6.1.1 IC卡的实体规格 6.1.2 文件选取方法 6.1.3 数据选取方法 (Data Referencing Methods) 6.1.4 IC卡的安全体系 6.2 个人身份认证系统 6.2.1 UNIX密码认证系统 6.2.2 S/Key只用一次密码 (One - Time Password) 认证系统 6.2.3 其它认证系统 6.3 LDAP协议 6.3.1 什么叫目录 6.3.2 LDAP的四个Model 6.4 OCSP协议 6.5 密码模块标准FIPS 140 - 1简介第7章 也算结论

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>