

<<密码学基础与安全应用>>

图书基本信息

书名：<<密码学基础与安全应用>>

13位ISBN编号：9787563515912

10位ISBN编号：7563515917

出版时间：2008-10

出版时间：胡振宇、蒋建春 北京邮电大学出版社 (2008-10出版)

作者：胡振宇，蒋建春 著

页数：159

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>

## 前言

当今世界，随着信息技术在经济社会各领域不断深化的应用，信息技术对生产力以至于人类文明发展的巨大作用越来越明显。

党的“十七大”提出要“全面认识工业化、信息化、城镇化、市场化、国际化深入发展的新形势新任务”，“发展现代产业体系，大力推进信息化与工业化融合”，明确了信息化的发展趋势，首次鲜明地提出了信息化与工业化融合发展的崭新命题，赋予了我国信息化全新的历史使命。

近年来，日新月异的信息技术呈现出新的发展趋势，信息技术与其他技术的结合更加紧密，信息技术应用的深度、广度和专业化程度不断提高。

我国的信息产业作为国民经济的支柱产业正面临着有利的国际、国内形势，电子信息产业的规模总量已进入世界大国行列。

但是我们也清楚地认识到，与国际先进水平相比，我们在产业结构、核心技术、管理水平、综合效益、普及程度等方面，还存在较大差距，缺乏创新能力与核心竞争力，“大”而不强。

国际国内形势的发展，要求信息产业不仅要做大，而且要做强，要从制造大国向制造强国转变，这是信息产业今后的重点工作。

要实现这一转变，人才是基础。

机遇难得，人才更难得，要抓住本世纪头二十年的重要战略机遇期，加快信息行业发展，关键在于培养和使用好人才资源。

《中共中央、国务院关于进一步加强人才工作的决定》指出，人才问题是关系党和国家事业发展的关键问题，人才资源已成为最重要的战略资源，人才在综合国力竞争中越来越具有决定性意义。

## <<密码学基础与安全应用>>

### 内容概要

《密码学基础与安全应用》是“网络信息安全工程师高级职业教育”证书认证考试人员的必备教程。

《密码学基础与安全应用》参考和借鉴了广大网络信息安全人员的最新研究成果，吸收了网络信息安全最佳实践经验，并以作者自己在网络信息安全领域从事理论研究及技术创新的经历和体会，系统归纳总结了密码学网络安全应用所需知识和技能，同时给出了密码学网络安全应用的典型案例。

《密码学基础与安全应用》主要内容包括密码学基础知识、对称加密算法、非对称加密算法、散列算法及其应用、数字签名、PKI技术、SSL、SSH、IPSec、PGP加密文件系统等。

《密码学基础与安全应用》侧重于密码学网络安全技术应用，避免了深奥的理论证明。书中配有练习题。

读者通过该书，能够快速掌握职业所需要的密码学知识和安全技能。

《密码学基础与安全应用》可以作为从事网络信息安全的广大技术人员和大专院校师生的参考用书，也可作为各类计算机信息技术培训和辅导教材。

## 书籍目录

第1章 密码学基础知识1.1 密码系统的组成1.2 密码学相关术语1.3 加密算法的分类1.3.1 对称加密算法1.3.2 公钥加密算法1.4 常见密码分析的攻击类型1.5 密码算法的破译等级1.6 本章小结1.7 本章练习第2章 对称加密算法2.1 DES算法2.1.1 DES加密2.1.2 DES解密2.1.3 DES实现过程分析2.2 IDEA算法2.2.1 IDEA算法简介2.2.2 算法框架2.2.3 评价2.3 AES算法2.3.1 AES加密2.3.2 AES解密2.4 分组密码的工作模式2.4.1 电码本模式2.4.2 密码分组链模式2.4.3 密码反馈模式2.4.4 输出反馈模式2.4.5 计数器模式2.5 对称加密算法的典型应用2.6 本章小结2.7 本章练习第3章 非对称加密算法3.1 RSA算法3.1.1 RSA算法描述3.1.2 RSA的安全性3.1.3 RSA的主要缺点3.2 ElGamal算法3.3 椭圆曲线加密算法3.3.1 密码学中的椭圆曲线3.3.2 椭圆曲线上的加法运算3.3.3 椭圆曲线上简单的加/解密3.4 对称和非对称加密算法的综合应用3.5 非对称加密算法的典型应用3.6 本章小结3.7 本章练习第4章 散列算法及其应用4.1 散列算法4.1.1 散列函数的属性4.1.2 散列函数的构造方式4.1.3 典型散列算法4.2 MD5算法原理分析4.2.1 基本描述4.2.2 MD5的非线性轮函数4.2.3 MD5相对MD4所作的改进4.2.4 关于MD5和SHA-1安全性的最新进展4.3 散列算法的典型应用4.3.1 用MD5校验和实现文件完整性保护4.3.2 文件系统完整性保护4.3.3 身份鉴别4.3.4 网页自动恢复系统4.4 本章小结4.5 本章练习第5章 数字签名5.1 数字签名5.1.1 基本概念5.1.2 数字签名的工作机制5.2 数字签名的实现技术5.2.1 利用RSA算法实现数字签名5.2.2 利用ElGamal算法实现数字签名5.2.3 利用椭圆曲线算法实现数字签名5.3 数字签名的应用案例5.3.1 椭圆曲线算法在软件保护中的应用5.3.2 电子印章5.4 本章小结5.5 本章练习第6章 PKI技术6.1 PKI技术概述6.2 PKI技术的安全服务及意义6.2.1 PKI技术的安全服务6.2.2 PKI技术的意义6.3 PKI技术的标准及体系结构6.3.1 PKI技术的标准6.3.2 PKI技术的体系结构6.4 PKI技术的应用与发展6.4.1 PKI技术的应用6.4.2 PKI技术的发展6.5 Windows Server 2003 PKI的证书管理6.5.1 添加证书模板6.5.2 委托证书模板管理6.5.3 颁发证书6.5.4 吊销证书6.6 本章小结6.7 本章练习第7章 SSL7.1 SSL协议概述7.2 SSL协议体系结构分析7.2.1 SSL协议的体系结构7.2.2 SSL的记录协议7.2.3 SSL的握手协议7.3 OpenSSL协议的工作过程7.3.1 OpenSSL概述7.3.2 OpenSSL的工作过程7.4 OpenSSL网站应用7.4.1 网站安全需求分析7.4.2 OpenSSL的安装7.5 Windows 2000中SSL的配置与应用7.6 SSL VPN7.6.1 VPN概述7.6.2 SSL VPN的工作原理7.6.3 SSL VPN的技术特点7.6.4 SSL VPN的实际应用7.7 本章小结7.8 本章练习第8章 SSH8.1 SSH概述8.2 SSH协议的基本框架8.3 SSH的工作原理8.4 SSH的身份认证机制8.5 SSH的应用分析8.6 OpenSSH应用实例8.6.1 OpenSSH简述8.6.2 OpenSSH的安装8.6.3 使用基于传统口令认证的OperLSSH8.6.4 配置并使用基于密钥认证的OpenSSH8.7 Windows平台下SSH的应用实例8.7.1 安装F Secure SSH软件8.7.2 SSH服务器端的设置8.7.3 客户端的设置与连接8.7.4 应用举例8.8 本章小结8.9 本章练习第9章 IPSec9.1 IPSec的体系结构9.1.1 AH协议结构9.1.2 ESP协议结构9.1.3 ESP隧道模式和AH隧道模式9.1.4 AH和ESP的综合应用9.2 IPSec的应用分析9.3 Linux环境下IPSec的应用实例9.3.1 手动密钥管理9.3.2 自动密钥管理9.3.3 建立IPSec安全隧道9.4 Windows 2000下基于IPSec的VPN9.4.1 Windows 2000中IPSec的配置9.4.2 测试IPSec策略9.5 本章小结9.6 本章练习第10章 PGP10.1 电子邮件安全需求10.2 PGP的工作机制10.2.1 PGP的安全服务10.2.2 加密密钥和密钥环10.2.3 公钥的管理机制10.3 PGP的应用实例10.3.1 PGP的安装10.3.2 生成密钥10.3.3 加密、解密应用10.4 本章小结10.5 本章练习第11章 加密文件系统11.1 Windows加密文件系统概述11.2 EFS的工作原理11.3 EFS的组成11.4 EFS与NTFS对文件保护的关系11.5 EFS的优势和局限11.6 EFS的设置11.7 EFS的恢复代理11.8 EFS操作实例11.8.1 加密和解密文件与文件夹11.8.2 复制和移动加密文件11.8.3 与其他用户共享加密文件11.8.4 备份证书和私钥11.8.5 指定恢复代理11.8.6 禁止加密功能11.8.7 注意事项11.9 EFS使用方法小结11.10 本章小结11.11 本章练习第12章 密码系统的安全测试与评价12.1 密码算法的安全性检测12.1.1 数据变换有效性测试12.1.2 算法对明文的扩散性检验12.1.3 密钥更换的有效性检验12.1.4 线性复杂度检验12.2 密码系统的评价12.2.1 保护程序与应用需求相符合12.2.2 对安全性的信心要建立在密码体制所依据的困难问题上12.2.3 实际效率12.2.4 采用实际可用的原型和服务12.2.5 明确性12.2.6 开放性12.3 本章小结12.4 本章练习参考文献

<<密码学基础与安全应用>>

章节摘录

插图：

## <<密码学基础与安全应用>>

### 编辑推荐

《密码学基础与安全应用》是“网络信息安全工程师高级职业教育(Network Security Advanced Career Education, NSACE)项目”的必备教材。

通过对《密码学基础与安全应用》的学习,读者既可以了解到密码学的基本原理和常用加密方法,又能掌握将常用的密码技术应用到实际中的最佳技巧。

密码学的历史源远流长,但长期以来它只在很少的范围内(如军事、外交、情报等部门)使用,因而对一般人来说是陌生的。

再加上它常常涉及晦涩的数学知识,因而它显得古老而深奥。

计算机密码学是研究计算机信息加密、解密及其变换的科学,是数学和计算机的交叉学科,也是一门新兴的学科。

随着互联网发展和信息技术的普及,网络和信息已经日渐深入到日常生活和工作当中。

密码学及应用技术在一个以信息化为主要特征的时代中将发挥越来越重要的作用。

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>