

<<密码学原理及应用技术>>

图书基本信息

书名：<<密码学原理及应用技术>>

13位ISBN编号：9787302256465

10位ISBN编号：7302256462

出版时间：2011-8

出版时间：清华大学出版社

作者：张健 等编著

页数：157

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>

<<密码学原理及应用技术>>

内容概要

应用密码技术是网络安全和信息安全中的关键技术，它主要用于实现信息的保密性、完整性和不可否认性。

《密码学原理及应用技术》内容包括密码算法及其在诸多方面的应用，如分组密码体制、公钥密码体制、序列密码体制等算法以及密码学在网络安全、电子邮件、电子商务和图像加密中的应用等，全书语言简练，通俗易懂，重点突出。

本书是作者在多年教学和科研工作基础上撰写而成的，可以作为高等学校计算机、通信工程、信息安全等专业的本科生和硕士生教材，也可以供相关领域的研究人员及工程技术人员参考。

<<密码学原理及应用技术>>

书籍目录

第1章 密码学概述

- 1.1 密码学与网络信息安全
 - 1.1.1 网络信息面临的威胁
 - 1.1.2 密码学在网络信息安全中的作用
- 1.2 密码学的基本概念
- 1.3 密码学的发展历史
- 1.4 密码学的应用范围
- 1.5 习题

第2章 古典密码

- 2.1 代替密码
 - 2.1.1 单表代替密码
 - 2.1.2 多表代替密码——playfair密码
 - 2.1.3 多表代替密码——vigenere密码
 - 2.1.4 多表代替密码——vernam密码
- 2.2 换位密码
 - 2.2.1 列换位
 - 2.2.2 周期换位
- 2.3 习题

第3章 密码学数学基础

- 3.1 素数
 - 3.1.1 整除
 - 3.1.2 素数的定义
 - 3.1.3 最大公约数
- 3.2 模运算
- 3.3 模逆元
- 3.4 费马?欧拉定理
 - 3.4.1 费马定理
 - 3.4.2 欧拉定理
 - 3.4.3 本原元
- 3.5 中国余数定理
- 3.6 单向函数与单向暗门函数
- 3.7 习题

第4章 分组加密体制

- 4.1 分组密码
 - 4.1.1 分组密码概述
 - 4.1.2 分组密码设计思想
- 4.2 s des方案
 - 4.2.1 s-des加密原理
 - 4.2.2 sdes的子密码生成过程
 - 4.2.3 s-des的 / 函数结构
- 4.3 美国数据加密标准(des)
 - 4.3.1 des加密原理
 - 4.3.2 des详细的加密过程
- 4.4 分组密码的运行模式
- 4.5 高级加密标准aes

<<密码学原理及应用技术>>

- 4.5.1 aes概述
- 4.5.2 aes的数学基础
- 4.5.3 aes算法
- 4.5.4 aes算法的密钥编排

4.6 习题

第5章 公钥密码体制

5.1 概述

- 5.1.1 公钥密码体制的提出
- 5.1.2 公钥密码体制的原理
- 5.1.3 diffie-hellman密钥交换算法

5.2 rsa概述

- 5.2.1 密钥生成
- 5.2.2 加密 / 解密算法
- 5.2.3 大数模幂乘的计算
- 5.2.4 素数判断
- 5.2.5 梅森素数
- 5.2.6 rsa的安全性

5.3 rabin密码系统

5.4 elgamal密码系统

5.5 椭圆曲线密码系统

- 5.5.1 椭圆曲线概述
- 5.5.2 利用elgamal的椭圆曲线加密法
- 5.5.3 利用menezes-vanstone的椭圆曲线加密法
- 5.5.4 椭圆曲线共享秘密推导机制
- 5.5.5 椭圆曲线密码体制的优点

5.6 习题

第6章 序列密码

6.1 序列密码模型

6.2 随机, 陛

6.3 线性反馈移位寄存器

6.4 非线性反馈移位寄存器

6.5 基于lfsr的序列密码加密体制

6.6 随机数产生器的安全性评估

6.7 序列密码的攻击方法

6.8 rc4

6.9 习题

第7章 数字签名

7.1 数字签名概述

7.1.1 数字签名的产生

7.1.2 数字签名的原理

7.2 利用rsa公钥密码体制实现数字签名

7.3 数字签名标准

7.3.1 dss的基本方式

7.3.2 dsa算法

7.4 其他签名方案

7.4.1 gost数字签名算法

7.4.2 不可否认的数字签名算法

<<密码学原理及应用技术>>

- 7.4.3 fail-stop数字签名算法
- 7.4.4 基于离散对数问题的数字签名算法
- 7.4.5 ong-schnorr-shamir签名算法
- 7.4.6 esign签名算法
- 7.4.7 盲签名算法
- 7.4.8 代理签名算法

7.5 认证协议

7.6 散列函数

- 7.6.1 单向散列函数
- 7.6.2 无碰撞散列函数和离散对数散列函数
- 7.6.3 单向散列函数的设计
- 7.6.4 单向散列函数的安全性

7.7 md5和sha-1

7.8 习题

第8章 密钥管理

8.1 密钥管理技术的发展

8.2 密钥的管理、组织结构与分配

- 8.2.1 密钥管理的内容
- 8.2.2 密钥的组织结构
- 8.2.3 密钥分配技术

8.3 pki

- 8.3.1 pki综述
- 8.3.2 pki的基本组成
- 8.3.3 pki的目标
- 8.3.4 pki技术包含的内容
- 8.3.5 pki的优势

8.4 习题

第9章 密码学与网络安全

9.1 osi参考模型和tcp / ip分层模型

- 9.1.1 osi参考模型
- 9.1.2 tcp / ip分层模型
- 9.1.3 vpn

9.2 网络安全

- 9.2.1 网络安全特征
- 9.2.2 网络安全分析
- 9.2.3 网络安全技术手段

9.3 无线网络加密技术

9.4 习题

第10章 密码学在图像加密中的应用

10.1 图像加密概述

10.2 arnold cat均匀加密算法

10.3 加密效果分析

- 10.3.1 视觉效果分析
- 10.3.2 相关性分析
- 10.3.3 对比实验及分析
- 10.3.4 剪切实验及分析

10.4 习题

<<密码学原理及应用技术>>

第11章 密码学在ic卡上的应用

11.1 1c卡

11.1.1 1c卡概述

11.1.2 1c卡工作原理和技术

11.1.3 1c卡的安全

11.2 1c卡的密码算法

11.2.1 密钥交换算法

11.2.2 个体鉴别算法

11.2.3 信息鉴别算法

11.2.4 信息加密 / 解密算法

11.3 习题

第12章 密码学在电子邮件中的应用

12.1 电子邮件

12.1.1 电子邮件的工作原理

12.1.2 电子邮件的常见协议

12.2 pgp

12.2.1 pgp简介

12.2.2 pgp 32作原理

12.2.3 pgp密钥

12.2.4 pgp的安全性

12.3 pgp软件的安装与使用

12.3.1 pgp软件介绍

12.3.2 pgp软件的安装

12.3.3 pgp软件的使用

12.4 习题

第13章 密码学与电子商务

13.1 电子商务概述

13.2 安全电子交易set

13.2.1 安全电子交易的组成及特点

13.2.2 安全电子交易的工作原理

13.3 数字现金

13.4 软商品的传输安全性

13.5 习题

参考文献

<<密码学原理及应用技术>>

编辑推荐

教学目标明确，注重理论与实践的结合
内容先进，反映了电子信息学科的最新发展

教学方法灵活，培养学生自主学习的能力
教学模式完善，提供了配套的教学资源解决方案

<<密码学原理及应用技术>>

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>