

<<密码学简明教程>>

图书基本信息

书名：<<密码学简明教程>>

13位ISBN编号：9787302260561

10位ISBN编号：7302260567

出版时间：2011-8

出版时间：清华大学出版社

作者：邓元庆，龚晶，石会 编著

页数：298

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>

## <<密码学简明教程>>

### 内容概要

邓元庆、龚晶、石会编著的《密码学简明教程》介绍现代密码学的基础理论及典型应用，是作者长期从事密码学教学和研究的结晶。

全书共分10章，内容包括绪论、密码学的数学基础、古典密码技术、对称密码体制与典型算法、非对称密码体制与典型算法、hash函数与消息认证码、消息认证与数字签名、密钥管理、电子邮件安全系统PGP、密码学的知识拓展。

各章配有大量例题、习题和思考题，书末附有计算性习题的参考答案和AES算法的教学演示程序及雪崩效应特性测试数据。

《密码学简明教程》选材新颖，逻辑严密，使用方便，适用面广，既可作为电子、信息、计算机、通信等专业的密码学教材，也可作为信息安全领域相关技术人员的学习与参考用书。

## &lt;&lt;密码学简明教程&gt;&gt;

## 书籍目录

## 第1章 绪论

## 1.1 引言

## 1.2 密码学的发展简史

## 1.2.1 古典密码阶段

## 1.2.2 近代密码阶段

## 1.2.3 现代密码阶段

## 1.3 密码学的基本概念

## 1.3.1 基本术语

## 1.3.2 密码体制

## 1.3.3 密码系统的安全性

## 1.4 信息安全概述

## 1.4.1 信息系统面临的安全性攻击

## 1.4.2 信息系统应该具备的信息安全特性

## 1.4.3 信息系统的信息安全模型

## 思考题与习题1

## 第2章 密码学的数学基础

## 2.1 初等数论

## 2.1.1 最大公约数

## 2.1.2 模运算

## 2.1.3 素数

## 2.2 有限域理论

## 2.2.1 群、环、域的基本概念

## 2.2.2 有限域

## 2.2.3 素域GF

## 2.2.4 有限域GF

## 思考题与习题2

## 第3章 古典密码技术

## 3.1 代换密码技术

## 3.1.1 单表代换密码

## 3.1.2 多表代换密码

## 3.2 置乱密码技术：

## 3.3 密码分析技术

## 3.3.1 密码分析的基本概念

## 3.3.2 密码分析举例

## 思考题与习题3

第4章 对称密码体制与典型算法<sup>^</sup>

## 4.1 分组密码体制

## 4.1.1 分组密码算法的基本要求

## 4.1.2 分组密码算法的典型结构

## 4.1.3 分组密码的操作模式

## 4.2 AES密码算法

## 4.2.1 AES的诞生背景

## 4.2.2 AES的算法结构

## 4.2.3 AES的基本运算

## 4.2.4 AES的解密运算

## <<密码学简明教程>>

4.2.5 AES的密钥扩展

4.2.6 AES的加、解密实例

4.3 Camellia密码算法

4.3.1 Camellia的诞生背景

4.3.2 Camellia的算法结构

4.3.3 Camellia的变换函数

4.3.4 Camellia的加密实例

4.4 序列密码

4.4.1 序列密码的基本结构

4.4.2 密钥流产生器

4.4.3 密钥流的局部随机性检验

思考题与习题4

第5章 非对称密码体制与典型算法

5.1 公钥密码体制概述

5.1.1 公钥密码体制的基本思想

5.1.2 陷门单向函数

5.2 RSA算法

5.2.1 RSA算法描述

5.2.2 RSA算法的实现问题

5.3 ElGamal算法

5.3.1 离散对数问题

5.3.2 ElGamal算法描述与示例

5.4 椭圆曲线密码体制

5.4.1 椭圆曲线及其运算

5.4.2 椭圆曲线密码体制

思考题与习题5

第6章 hash函数与消息认证码

6.1 概述

6.1.1 hash函数

6.1.2 消息认证码MAC

6.1.3 生日攻击

6.2 安全hash函数算法SHA-512

6.2.1 算法原理

6.2.2 轮函数

6.2.3 算法举例

6.3 欧洲hash函数算法Whirlpool

6.3.1 算法原理

6.3.2 分组密码Whirlpool

6.4 MAC算法

6.4.1 HMAC算法

6.4.2 CMAC算法

思考题与习题6

第7章 消息认证与数字签名

7.1 概述

7.1.1 消息认证概述

7.1.2 数字签名概述

7.2 消息认证

## <<密码学简明教程>>

7.2.1 认证函数

7.2.2 认证协议

7.3 数字签名

7.3.1 数字签名原理

7.3.2 直接数字签名

7.3.3 可仲裁数字签名

7.4 数字签名方案

7.4.1 RSA数字签名方案

7.4.2 数字签名算法(DSA)

7.4.3 ECDSA数字签名方案

7.5 特殊的数字签名

7.5.1 盲签名

7.5.2 代理签名

7.5.3 基于身份的数字签名

思考题与习题7

第8章 密钥管理

8.1 概述

8.1.1 密钥的种类与层次结构

8.1.2 密钥管理的生命周期

8.1.3 密钥的生成与保护

8.1.4 密钥的协商与分配

8.2 密钥协商

8.2.1 Diffie—Hellman密钥交换协议

8.2.2 Diffie—Hellman密钥预分配协议

8.2.3 Diffie—Hellman密钥交换协议的中间人攻击

8.2.4 端到端密钥交换协议

8.3 密钥分配

8.3.1 对称密码体制的密钥分配

8.3.2 公钥密码体制的密钥分配

思考题与习题8

第9章 电子邮件安全系统PGP

9.1 PGP概述

9.1.1 PGP的发展历程

9.1.2 PGP的主要功能

9.2 PGP的工作原理

9.2.1 PGP的密钥

9.2.2 PGP消息的发送与接收

9.2.3 PGP的公钥管理

9.3 PGP软件的使用

9.3.1 PGP软件的安装

9.3.2 PGP的密钥管理组件PGPkeys

9.3.3 电子邮件的加密、解密与签名

9.3.4 文件的加密、解密与签名

9.3.5 PGP的其他功能

思考题与习题9

第10章 密码学的知识拓展

10.1 混沌密码

<<密码学简明教程>>

10.1.1 混沌理论基础

10.1.2 混沌密码学

10.2 量子密码

10.2.1 量子密码学的基本原理

10.2.2 BB84协议

10.2.3 量子密码的研究现状

10.3 公钥基础设施(PKI)

10.3.1 PKI的基本概念

10.3.2 PKI的主要功能

10.3.3 PKI的证书与信任模式

思考题与习题10

附录A AES加密算法教学演示程序

附录B AES算法的雪崩效应特性测试

附录C 部分习题参考答案

参考文献

<<密码学简明教程>>

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>