

<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787121132902

10位ISBN编号：7121132907

出版时间：2011-4

出版时间：电子工业出版社

作者：胡向东

页数：366

字数：615000

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>

## <<应用密码学>>

### 内容概要

本书介绍了应用密码学的基本概念、基本理论和典型实用技术。

内容涉及密码学基础、古典密码、密码学数学引论、对称密码体制、非对称密码体制、HASH函数和消息认证、数字签名、密钥管理、流密码以及密码学的新进展；书中还介绍了密码学在数字通信安全、工业网络控制安全、无线传感器网络感知安全、无线射频识别安全以及电子商务支付安全等典型领域的应用方法和技术。

突出的特色是将复杂的密码算法原理分析得深入浅出，着重培养现代密码学方面的工程应用技能，便于读者花少量的时间入门并尽快掌握应用密码学的精髓。

本书可作为高等院校密码学、应用数学、信息安全、通信工程、计算机、信息管理、电子商务、物联网、网络化测控等专业高年级本科生和研究生教材，也可供从事网络和通信信息安全相关领域应用和设计开发的研究人员、工程技术人员参考。

尤其适合对学习密码学感到困难的初学者。

## &lt;&lt;应用密码学&gt;&gt;

## 书籍目录

## 开篇 密码学典故

## 第0章 密码故事

0.1 重庆大轰炸背后的密码战

0.2 “爱情密码”贴

## 上篇 密码学原理

## 第1章 绪论

## 1.1 网络信息安全概述

1.1.1 网络信息安全问题的由来

1.1.2 网络信息安全问题的根源

1.1.3 网络信息安全的重要性和紧迫性

## 1.2 密码学在网络信息安全中的作用

## 1.3 密码学的发展历史

1.3.1 古代加密方法（手工阶段）

1.3.2 古典密码（机械阶段）

1.3.3 近代密码（计算机阶段）

## 1.4 网络信息安全的机制和安全服务

1.4.1 安全机制

1.4.2 安全服务

1.4.3 安全服务与安全机制之间的关系

## 1.5 安全性攻击的主要形式及其分类

1.5.1 安全性攻击的主要形式

1.5.2 安全攻击形式的分类

## 思考题和习题

## 第2章 密码学基础

## 2.1 密码学相关概念

## 2.2 密码系统

2.2.1 柯克霍夫原则（Kerckhoff's Principle）

2.2.2 密码系统的安全条件

2.2.3 密码系统的分类

## 2.3 安全模型

2.3.1 网络通信安全模型

2.3.2 网络访问安全模型

## 2.4 密码体制

2.4.1 对称密码体制（Symmetric Encryption）

2.4.2 非对称密码体制（Asymmetric Encryption）

## 思考题和习题

## 第3章 古典密码

## 3.1 隐写术

## 3.2 代替

3.2.1 代替密码体制

3.2.2 代替密码的实现方法分类

## 3.3 换位

## 思考题和习题

## 第4章 密码学数学引论

## 4.1 数论

## &lt;&lt;应用密码学&gt;&gt;

4.1.1 素数

4.1.2 模运算

4.1.3 欧几里德算法 ( Euclidean Algorithm )

4.1.4 扩展的欧几里德算法 ( The Extended Euclidean Algorithm )

4.1.5 费马 ( Fermat ) 定理

4.1.6 欧拉(Euler)定理

4.1.7 中国剩余定理

4.2 群论

4.2.1 群的概念

4.2.2 群的性质

4.3 有限域理论

4.3.1 域和有限域

4.3.2 有限域中的计算

4.4 计算复杂性理论

4.4.1 算法的复杂性

4.4.2 问题的复杂性

思考题和习题

第5章 对称密码体制

5.1 分组密码

5.1.1 分组密码概述

5.1.2 分组密码原理

5.1.3 分组密码的设计准则

5.1.4 分组密码的操作模式

5.2 数据加密标准 ( DES )

5.2.1 DES概述

5.2.2 DES加密原理

5.3 高级加密标准 ( AES )

5.3.1 算法描述

5.3.2 基本运算

5.3.3 基本加密变换

5.3.4 AES的解密

5.3.5 密钥扩展

5.3.6 AES举例

5.4 SMS4分组密码算法

5.4.1 算法描述

5.4.2 加密实例

思考题和习题

第6章 非对称密码体制

6.1 概述

6.1.1 非对称密码体制的提出

6.1.2 对公钥密码体制的要求

6.1.3 单向陷门函数

6.1.4 公开密钥密码分析

6.1.5 公开密钥密码系统的应用

6.2 Diffie-Hellman密钥交换算法

6.3 RSA

6.3.1 RSA算法描述

## &lt;&lt;应用密码学&gt;&gt;

6.3.2 RSA算法的有效实现

6.3.3 RSA的数字签名应用

6.4 椭圆曲线密码体制ECC

6.4.1 椭圆曲线密码体制概述

6.4.2 椭圆的概念和分类

6.4.3 椭圆的加法规则

6.4.4 椭圆曲线密码体制

6.4.5 椭圆曲线中数据类型的转换方法

思考题及习题

第7章 HASH函数和消息认证

7.1 HASH函数

7.1.1 HASH函数的概念

7.1.2 安全HASH函数的一般结构

7.1.3 HASH填充

7.1.4 HASH函数的应用

7.2 散列算法

7.2.1 散列算法的设计方法

7.2.2 SHA-1散列算法

7.2.3 SHA-256

7.2.4 SHA-384和SHA-512

7.2.5 SHA算法的对比

7.3 消息认证

7.3.1 基于消息加密的认证

7.3.2 基于消息认证码 (MAC) 的认证

7.3.3 基于散列函数 (HASH) 的认证

7.3.4 认证协议

思考题及习题

第8章 数字签名

8.1 概述

8.1.1 数字签名的特殊性

8.1.2 数字签名的要求

8.1.3 数字签名方案描述

8.1.4 数字签名的分类

8.2 数字签名标准 (DSS)

8.2.1 DSA的描述

8.2.2 使用DSA进行数字签名的示例

思考题和习题

第9章 密钥管理

9.1 密钥的种类与层次式结构

9.1.1 密钥的种类

9.1.2 密钥管理的层次式结构

9.2 密钥管理的生命周期

9.3 密钥的生成与安全存储

9.3.1 密钥的生成

9.3.2 密钥的安全存储

9.4 密钥的协商与分发

9.4.1 秘密密钥的分发

## &lt;&lt;应用密码学&gt;&gt;

## 9.4.2 公开密钥的分发

## 思考题和习题

## 第10章 流密码

## 10.1 概述

## 10.1.1 流密码模型

## 10.1.2 分组密码与流密码的对比

## 10.2 线性反馈移位寄存器

## 10.3 基于LFSR的流密码

## 10.3.1 基于LFSR的流密码密钥流生成器

## 10.3.2 基于LFSR的流密码体制

## 10.4 典型流密码算法

## 10.4.1 RC4

## 10.4.2 A5/1

## 思考题和习题

## 附：RC4算法的优化实现

## 第11章 密码学的新进展——量子密码学

## 11.1 量子密码学概述

## 11.2 量子密码学原理

## 11.2.1 量子测不准原理

## 11.2.2 量子密码基本原理

## 11.3 BB84量子密码协议

## 11.3.1 无噪声BB84量子密码协议

## 11.3.2 有噪声BB84量子密码协议

## 11.4 B92量子密码协议

## 11.5 E91量子密码协议

## 11.6 量子密码分析

## 11.6.1 量子密码的安全性分析

## 11.6.2 量子密码学的优势

## 11.6.3 量子密码学的技术挑战

## 思考题和习题

## 下篇 密码学应用与实践

## 第12章 密码学与数字通信安全

## 12.1 数字通信保密

## 12.1.1 保密数字通信系统的组成

## 12.1.2 对保密数字通信系统的要求

## 12.1.3 保密数字通信系统实例模型

## 12.2 第三代移动通信系统（3G）安全与WAP

## 12.2.1 第三代移动通信系统（3G）安全特性与机制

## 12.2.2 WAP的安全实现模型

## 12.3 无线局域网安全与WEP

## 12.3.1 无线局域网与WEP概述

## 12.3.2 WEP的加、解密算法

## 12.3.3 无线局域网的认证

## 12.3.4 WEP的优、缺点

## 12.4 IPSec与VPN

## 12.4.1 IPSec概述

## 12.4.2 IPSec安全体系结构

<<应用密码学>>

12.4.3 VPN

12.5 基于PGP的电子邮件安全实现

12.5.1 PGP概述

12.5.2 PGP原理描述

12.5.3 使用PGP实现电子邮件通信安全

思考题和习题

#### 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>