

<<应用密码学>>

图书基本信息

书名：<<应用密码学>>

13位ISBN编号：9787121032264

10位ISBN编号：7121032260

出版时间：2006-11

出版时间：电子工业出版社

作者：胡向东、魏琴芳

页数：339

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

本书兼具专著和教材的双重属性,是作者从事多年的应用密码学相关教学和科研工作实践的结晶。本书全面介绍了应用密码学的基本概念、基本理论和典型实用技术。

全书共15章,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、序列密码、量子密码;书中还介绍了应用密码学在电子商务支付安全、数字通信安全、工业网络控制安全和无线传感器网络感知安全这四个典型领域的应用方法和技术。

语言简练,内容重点突出,逻辑性强,算法经?实用;突出的特色是将复杂的密码算法原理分析得透彻深入,便于读者花少量的时间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、检测技术、控制理论与控制工程、系统工程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。

## &lt;&lt;应用密码学&gt;&gt;

## 书籍目录

## 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

## 1.5 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 安全性攻击形式的分类

## 思考题和习题

## 第2章 密码学基础

## 2.1 密码学相关概念

## 2.1.1 惟密文攻击(Ciphertext Only)

## 2.1.2 已知明文攻击(Known Plaintext)

## 2.1.3 选择明文攻击(Chosen Plaintext)

## 2.1.4 选择密文攻击(Chosen Ciphertext)

## 2.1.5 选择文本攻击(Chosen Text)

## 2.2 密码系统

## 2.2.1 密码系统的定义

## 2.2.2 柯克霍夫(Kerckhoffs)原则

## 2.2.3 密码系统的安全条件

## 2.2.4 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

## 3.1.1 诗情画意传“密语”

## 3.1.2 悠扬琴声奏响“进军号角”

## 3.1.3 显微镜里传递情报

## 3.1.4 魔术般的密写术

## 3.1.5 网络与数字幽灵

## 3.1.6 “量子”技术隐形传递信息

## 3.2 代替

## &lt;&lt;应用密码学&gt;&gt;

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

4.1.1 素数

4.1.2 模运算

4.1.3 欧几里德(Euclid)算法

4.1.4 费马(Fermat)定理

4.1.5 欧拉(Euler)定理

4.1.6 中国剩余定理(CRT)

4.2 群论

4.2.1 群的概念

4.2.2 群的性质

4.3 有限域(Galois Field)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

第6章 非对称密码体制

第7章 HASH函数和消息认证

第8章 数字签名

第9章 密钥管理

第10章 序列密码

第11章 密码学与电子商务支付安全

第12章 密码学与数字通信安全

第13章 密码学与工业网络控制安全

第14章 密码学与无线传感器网络感知安全

第15章 密码学的新进展——量子密码学

部分习题参考答案

第3章 古典密码

第4章 密码学数学引论

第5章 对称密码体制

第6章 非对称密码体制

第8章 数字签名

参考文献

#### 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>