

《对称密码学及其应用》

图书基本信息

书名：《对称密码学及其应用》

13位ISBN编号：9787563517176

10位ISBN编号：7563517170

出版时间：2009-4

出版社：北京邮电大学出版社

作者：李晖 李丽香 邵帅

页数：277

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《对称密码学及其应用》

内容概要

本书全面介绍了对称密码学的基本理论、主要方法和应用实例，内容涉及古典密码学、现代对称密码学及最新进展。本书在介绍密码学的历史的同时，介绍了密码学的基础知识和基本概念，然后重点描述了分组密码算法和序列密码算法，包括它们的设计准则、典型算法和主要分析方法，在此基础上介绍了密钥管理基础知识，讨论了对称密码学在数字通信系统中和工业控制系统中的应用，最后介绍了两种新型密码体制——量子密码和混沌密码。

本书适合作为高校计算机安全与信息安全专业的本科教材，也可供对密码学、信息安全、通信安全等内容感兴趣的技术人员或科研人员阅读参考。

《对称密码学及其应用》

书籍目录

第1部分 密码学简介和古典密码学	第1章 绪论	1.1 密码学简史	1.2 密码学的基本概念
	1.3 密码体制的安全性要素	1.4 对称密码体制的概念与分类	1.5 对称密码学的应用领域
	1.6 本章小结	习题	第2章 古典密码学
		2.1 单码加密法	2.1.1 移位密码 (Shift Cipher)
		2.1.2 仿射密码 (Affine Cipher)	2.2 多码加密法
		2.2.1 Vigenere加密法	2.2.2 Nihilist加密法
		2.3 经典多图加密法	2.4 经典换位加密法
		2.4.1 列置换密码	2.4.2 周期置换密码
		2.5 古典密码分析	2.5.1 穷举法
		2.5.2 统计法	2.6 本章小结
		习题	第2部分 分组密码
		第3章 分组密码简介与设计准则	3.1 分组密码概述
		3.2 分组密码的一般设计原理	3.2.1 一般设计原理
		3.2.2 扩散和混乱原则	3.3 分组密码的结构
		3.3.1 SPN结构	3.3.2 Feistel结构
		3.4 S-盒的设计准则及其构造	3.4.1 S-盒的设计准则
		3.4.2 S-盒的构造方法	3.5 P置换的设计准则及构造方法
		3.5.1 P置换的设计准则	3.5.2 P置换的构造
		3.6 轮函数的设计准则及其构造	3.6.1 轮函数的设计
		3.6.2 轮函数的构造	3.7 密钥扩展算法的设计
		3.8 分组密码的工作模式	3.8.1 电子密码本模式
		3.8.2 密码分组链接模式	3.8.3 密码反馈模式
		3.8.4 输出反馈模式	3.8.5 计数器模式
		3.8.6 选择密码模式	3.9 本章小结
		习题	第4章 典型分组密码简介
		4.1 DES算法	4.1.1 DES的历史
		第5章 分组密码的统计测试原理与攻击方法	第3部分 序列密码
		第6章 序列密码概述	第7章 序列密码的设计与分析
		第8章 典型序列密码	第4部分 密码技术及应用
		第9章 密钥管理	第10章 对称密码学与数字通信安全
		第11章 对称密码学与工业控制安全	第5部分 对称密码学新进展
		第12章 量子密码学	第13章 混沌密码学
		附录A 概率及统计测试相关知识	附录B 术语索引
		参考文献	

《对称密码学及其应用》

章节摘录

第1章 绪论 1.1 密码学简史 密码学是一门既古老又年轻的学科，其历史可以追溯到几千年以前。在古代，保守一项秘密似乎要容易一些，因为只有少数人具有读书、写字的特权。如果一项秘密是书写下来的，那么只有数量极少的人才知道它的意义。只需要通过限制人们学习书写文字，即可做到保密。然而，这种保密机制显然具有很大的局限性。随着越来越多的人掌握了读写文字的能力，越来越有必要研究如何在某些人中间保守秘密。这种需要在战争期间愈发迫切。尽管当时真正打仗的人可能大多不具备读写文字的能力，但那些发动战争的所谓“军事家”们却并非如此，而且战争双方无疑都会雇佣一些能够读写敌方语言的士兵。从某种意义上讲，古战场上军队进行的秘密通信就是加密学的起源。早期的加密方法非常简单。据说凯撒大帝曾用一种初级的方法来加密他所要传达的消息。只有那些他认为能够分享秘密的人，他才会告诉他们如何能够重新组合回原来的消息。这种密码便是著名的“凯撒密码（The Caesar Cipher）”。

《对称密码学及其应用》

精彩短评

1、一般，读起来有点生硬的

《对称密码学及其应用》

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:www.tushu111.com