《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

《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一一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

《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。从某种意义上来讲，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