第一图书网, tushu007.com

<<大众密码学>>

图书基本信息

书名：<<大众密码学>>

13位ISBN编号：9787040172676

10位ISBN编号：7040172674

出版时间：2005-6

出版时间：高等教育出版社

作者：毛明

页数：137

字数：170000

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

内容概要

密码学是建立在复杂的数学基础之上的一门学科。
然而，本书未将其编写为数学专著，而足以非数学专业的广大读者为对象，运用通俗易懂的语言，简明扼要地介绍密码学的发展历史、基本理论、古典密码、序列密码、分组密码、公钥密码、数字签名、密钥管理等主要知识。
刈于密码学重要的数学理论，本书在给出其结论的同时采用典型、浅显的实例来解释，小进行数学上的推导和证明。
全书共分为9章，每一章末均附有习题，以帮助读者复习本章中的重点内容。
　本书町作为高等学校非数学专业的密码学与信息安全课程的教材，特别适合作为信息安全领域存职干部的培训教材，同时也可作为在信息安全领域从事科学研究、工程开发的广大技术人员的参考书。

<<大众密码学>>

书籍目录

第1章　密码导论 1.1 引言 1.2 隐写术　1.2.1 暗示　1.2.2　隐语　1.2.3　隐形墨水　1.2.4　微缩技术　1.2.5　信息隐藏 1.3　简单的密码　1.3.1 密码情书　1.3.2　栅栏式密码　1.3.3　恺撒密码 1.4　密码学基本概念　1.4.1　密码通信原理　1.4.2　密码学基本概念　1.4.3　密码通信系统 1.5 密码学发展简史　1.5.1　古典密码时期　1.5.2　近代密码时期　1.5.3　现代密码时期 1.6　密码的时代意义　1.6.1　密码与国家安全　1.6.2　密码与电子商务　1.6.3　密码与电子政务　1.6.4　密码技术新特点 习题第2章　古典密码 2.1 换位密码　2.1.1　列换位密码　2.1.2　周期换位密码 2.2 代替密码　2.2.1　单表代替密码　2.2.2　多表代替密码 2.3 转轮密码机　2.3.1　转轮密码机原理　2.3.2　转轮密码机的典型代表 习题第3章　基本理论 3.1 密码体制　3.1.1 换位与代替密码体制　3.1.2　序列与分组密码体制　3.1.3　对称与非对称密钥密码体制 3.2 数学理论　3.2.1 数论　3.2.2　信息论　3.2.3　复杂度理论 3.3 密码破译　3.3.1　密码破译概述　3.3.2　密码破译规律　3.3.3　密码破译方式　3.3.4　密码破译方法　3.3.5　密码破译步骤　3.3.6　密码破译实例 3.4 Shannon保密理论　3.4.1　理论保密体制　3.4.2　实际保密体制　3.4.3　密码系统的评测 习题第4章　序列密码 4.1 序列密码概述　4.1.1　序列密码概念　4.1.2　序列密码工作原理 4.2　移位寄存器理论　4.2.1　移位寄存器　4.2.2　线性反馈移位寄存器　……第5章　分组密码第6章　公钥密码第7章　数字签名第8章　密钥管理第9章　最新进展参考文献

第一图书网, tushu007.com

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