<<密码学理论与技术>>

图书基本信息

书名：<<密码学理论与技术>>

13位ISBN编号：9787302181958

10位ISBN编号：7302181950

出版时间：2008-10

出版时间：清华大学出版社

作者：范明钰，王光卫　编著

页数：167

<<密码学理论与技术>>

内容概要

本书从基本概念人手，通过手工密码算法、机械密码算法，建立密码算法的概念；从算法的设计和分析两条线索，指出密码学的对抗和发展状况。
全书主要分为以下4个部分：第1部分介绍与密码学相关的基本概念（第1章）。
第2部分介绍古典密码学，重点介绍古典密码设计和分析留下的经验和教训（第2、3章）。
第3部分介绍现代密码，包括对称密码中的分组密码（第4章）和序列密码（第5章）、Hash算法（第6章）和公钥密码（第7章）。
第4部分介绍密码算法的使用与发展，包括密钥管理过程（第8章）和网络时代的密码（第9章）。
本书可供工科类计算机、电子信息、通信等学科的本科学生和研究生使用。

<<密码学理论与技术>>

书籍目录

章节摘录

第1章 密码学中的基本概念　　本章主要内容是密码学的基本概念，包括密码学的应用、密码算法的基本概念、密码编码学和分析学中的基本概念、密码学的信息论基础、密码学的起源和发展以及密码算法的安全性和复杂性的概念。

密码学在公元前400多年就已经产生了，正如《破译者》一书中所言，人类使用密码的历史几乎与使用文字的时间一样长。

密码学的起源可以追溯到人类刚刚出现，并且尝试去学习如何通信的时候，为了确保相互间通信的机密，开始是有意识地使用一些简单的方法来加密信息，如通过一些（密码）象形文字相互传达信息。

接着由于表音和表意文字的出现和使用，确保通信的机密性就成为一种艺术。

而随着国家、政权、军事力量的建立．密码学在重要信息的交流传递方面起到了越来越重要的作用。

随着数字化和网络技术不断深入到社会各个方面，人们对信息安全的重要性认识不断提高，而在信息安全中起着举足轻重作用的密码学也就成为信息安全中不可或缺的重要部分。

今天密码学已经逐步揭开了神秘的面纱，进入了寻常百姓的日常生活之中。

密码学的研究应用前景十分广阔。

这个总是秘而不宣的重要角色，在人类的发展中将起到不可估量的作用。

当今世界各主要国家的政府都十分重视密码丁作，其中一些国家设立庞大机构，拨出巨额经费，集中数以万计的专家和科技人员，投人大量的高速电子计算机和其他先进设备进行工作。

与此同时，各民间企业和学术界也对密码学日益重视，不少数学家、计算机学家和其他有关学科的专家也投身于密码学的研究行列，更加快了密码学的发展。

版权说明