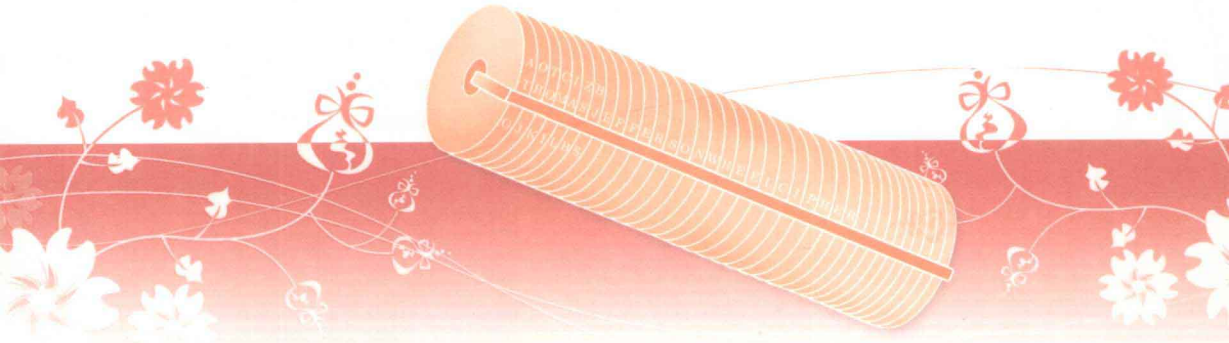
美妙数学花园

Meimiao Shuxue Huayuan



刘木兰 著

密码并不神秘

科学出版社

数学花园

密码

并不神秘

科学出版社

北京

内 容 简 介

本书是为中学生编写的科普读物，主要讲什么是密码和信息安全，目的是使大家了解密码并不神秘.

全书共分 7 章. 第 1 章介绍密码学的基本专业术语，包括密码、密钥、密码体制、数字签名、身份识别等. 第 2 章是关于古典密码体制，第 3 章和第 4 章分别讲述对称密码体制和公钥密码体制，第 5 章的数字签名是互联网环境下信息安全的重要内容. 第 6 章的密钥共享属于信息安全中密钥管理部分. 最后一章的电子商务是希望读者了解怎样才能使得参与电子商务活动的买家和卖家的权益得到保障.

本书除了可使读者走近密码和信息安全之外，一个“副产品”是使读者看到，在中学学过的整数运算、带余除法、辗转相除法求最大公因子等这些初等数学知识是多么有用.

图书在版编目（CIP）数据

密码并不神秘/刘木兰著. —北京：科学出版社，2011.6
(美妙数学花园)
ISBN 978-7-03-031534-2

Ⅰ. ①密… Ⅱ. ①刘… Ⅲ. ①密码-普及读物 Ⅳ. ①TN918.2-49

中国版本图书馆 CIP 数据核字（2011）第 113435 号

责任编辑：陈玉琢／责任校对：赵桂芬
责任印制：钱玉芬／封面设计：王 浩

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

中国科学院印刷厂印刷
科学出版社发行 各地新华书店经销
*
2011 年 6 月第 一 版 开本：B5(720×1000)
2011 年 6 月第一次印刷 印张：10 1/4
印数：1—5 000 字数：152 000

定价：28.00 元

（如有印装质量问题，我社负责调换）

《美妙数学花园》丛书序

今天，人类社会已经从渔猎时代、农耕时代、工业时代，发展到信息时代. 科学技术的巨大成就，为人类带来了丰富的物质财富和越来越美好的生活. 而信息时代高度发达的科学技术的基础，本质上是数学科学.

自从人类社会建立了现行的学校教育体制，语文和数学就是中小学两门最主要的课程. 如果说文学因为民族的差异各个国家之间有很大的不同，那么数学在世界上所有的国家都是一致的，仅有教学深浅、课本编排的不同.

我国在清末民初时期西学东渐，逐步从私塾科举过渡到现代的学校教育，一直十分重视数学. 中华民族的有识之士从清朝与近代科技完全隔绝的情况下起步，迅速学习了西方的科学文化. 在 20 个世纪前半叶短短的几十年间，在我们自己的小学、中学、大学毕业，然后留学欧美的学生当中，不仅产生了一批社会科学方面的

大师,而且产生了数学、物理学等自然科学领域对学科发展做出了重大贡献的享誉世界的科学家.他们的成就表明,有着五千年灿烂文化的中华民族是有能力在科学技术领域达到世界先进水平的.

在20世纪五六十年代,为了选拔和培养拔尖的数学人才,华罗庚与当时中国的许多知名数学家一道,学习前苏联的经验,提倡和组织了数学竞赛.数学家们为中学生举办了专题讲座,并且在讲座的基础上出版了一套面向中学生的《数学小丛书》.当年爱好数学的中学生十分喜爱这套丛书.在经历过那个时代的科学院院士和各个大学的数学教授当中,几乎所有的人都读过这套丛书.

诚然,我国目前的数学竞赛和数学教育由于体制的问题备遭诟病.但是我们相信,成长在信息时代的今天的中学生们,会有更多的孩子热爱数学;置身于社会转型时期的中学里,会有更多的数学教师渴望培养出优秀的科技人才.

数学家能够为中学生和中学教师们做些什么呢?数学本身是美好的,就像一个美丽的花园.这个花园很大,

我们并不能走遍她, 完全地了解她. 但是我们仍然愿意将自己心目中美好的数学, 将我们对数学的点滴领悟, 写给喜爱数学的中学生和数学老师们.

张英伯

2011 年 5 月

前　言

如今，“密码”这一词想必大家已不陌生了. 然而，除专业书籍以外，许多书报和媒体关于密码的介绍往往是通过与它相关的历史事件，突出了它的神秘感，乃至出现了“紫色密码”、“罪恶密码”、“达芬奇密码”、“蝴蝶密码”等设法与密码沾亲的文艺作品. 本书的目的是想告诉大家，密码并不神秘. 我们和大家一起走近密码看一看：到底什么是密码？它的奥妙何在？现代密码的特点是什么？本书立足于使具有中学数学知识的读者可以了解密码，以及对密码有兴趣的读者可以通过进一步的学习走入密码. 另一方面，由于信息安全与大众生活息息相关，同时信息安全和密码密不可分，因此，在走近密码的同时，也看看信息安全的一些相关内容，如数字签名、密钥共享、电子商务等.

密码学是一门既古老又年轻的学科，它有自己发生和发展的历史、特有的发展规律和所需要的基础知识. 密码学的历史最早可追溯到四千多年前. 当时，在尼罗

河畔的古埃及, 有些墓碑上刻的铭文是用一些奇怪的象形符号表示的. 这些铭文具备了两个性质: 文字书写的有意变形和变化后达到某种程度的秘密性. 这两个性质正是密码的两个要素. 在两千多年前, 古代文明大国美索不达米亚的碑文上已出现了直接采用将人名变换成数字的密文. 在我国, 三国时期已经使用 "暗语" (参见明朝蒋葵所著的《尧山堂外记》); 在 11 世纪已经出现了军用密码本 (参见《武经总要》). 关于西方近代的密码史, 在《破译者》一书中有详细讲述. 在文艺复兴时期的欧洲, 密码得到了比较广泛的应用. 16 世纪末期, 大多数欧洲国家已设立了专职掌管密码的秘书, 重要的文件都采用密写. 18 世纪, 各国普遍建立了破译密码的专门机构, 称之为 "黑屋". 设在维也纳的 "黑屋" 就曾破译过拿破仑的信件. 在第一次世界大战期间, 英国破译机构 "四十号房间" 的密码破译工作在战争中起到了重要作用. 它自 1914 年 10 月至 1919 年截取和密码的破译了 15000 份德国密码电报. 但是总的来说, 密码的最初发展阶段是非常缓慢的.

在电报发明之前, 保密的通信主要靠信使, 密码的主要形式是文字替换. 例如, 密码本就是将具体替换一一

列出来的一个大的替换表. 密码的加密与解密和密码的破译主要是靠用笔和纸的手工操作. 1844 年电报的发明和 1895 年无线电的诞生, 引起了通信技术的一场革命. 通信技术在战争中的使用促使密码学进入迅速发展阶段. 在第二次世界大战期间, 手工加密和解密已不能应对电报和无线电发出的大量电文, 于是出现了使用机械进行加密和解密的密码机. 日本的高级加密密码机 "九七式欧文打字机", 美国人称之为 "紫密", 就是典型的机械密码机. 在电视剧《对手》中要破译的密码就是指 "紫密" 密码. 破译人员用手工操作和经验已不能应对机械加密, 数学成为密码分析的有利工具. 当时, 美国就聘请出色的数学家作密码分析人员. 第二次世界大战期间, 密码工作者创造了密码史上值得大书特书的精彩篇章. 特别值得一提的是, 1943 年 4 月, 美国的密码学家破译了关于日本联合舰队长官山本五十六视察前线基地的电文. 根据破译的电文, 在 1943 年 4 月 18 日, 美国派出的飞行员在完全预定的时间和地点对山本五十六的座机截击成功. 情报的破译影响了战争的进程, 减少了人员的伤亡. 这段历史在《破译者》一书中有详细的记载. 事实上, 对于第二次世界大战的胜利, 中国的密码学家

也做出了很大贡献.

20 世纪 40 年代末, 美国的克劳德 • 埃尔伍德 • 香农 (Claude Elwood Shannon) 创立了一个著名的新理论 —— 保密系统的通信理论, 第一次从理论上确切地阐明了密码分析的可能性. 在这之前, 密码学是建立在经验和实验上的, 是一门实验科学. 香农的理论将密码编码学和密码分析学置于坚实的数学基础之上, 从根本上推动了密码学理论的发展. 20 世纪 60 年代, 微电子学的发展使得理论上有效但比较复杂的加密算法可以通过电子设备快速实现, 而计算机的使用使得密码分析者大有可为.

1976 年, 两个年轻人棣菲 (W. Diffie) 和赫尔曼 (M. Hellman) 提出了公钥密码的概念. 公钥密码与 60 年代以前使用的密码具有完全不同的思路, 导致了密码学的一场革命, 并使得密码在商业领域的广泛应用成为可能. 公钥密码不只用于加密, 它很大的一个优势是可用于数字环境下的签名和身份认证, 可以说, 它支撑了互联网上电子商务系统的数字签名和身份认证的功能. 公钥密码学是现代密码学的一个主要内容.

信息安全是本书的一个重要内容. 姑且不谈信息安全关乎到国家安全和国民经济的发展, 实际上, 它已与

人们的生活息息相关. 它不仅涉及个人财产安全, 而且涉及个人隐私保护. 信息安全的重要性在今天是众所周知的, 但是如何才能保障信息安全是一个非常复杂的问题. 它涉及人们掌握的知识、技术、人力、财力、软硬件环境, 大到国家、政治等. 事实上, 信息安全是一门年轻的学科. 一方面, 它与密码学密不可分, 同时它又有自己特有的研究目标和对象. 什么是信息安全? 学术界对这个问题至今还没有一个公认的定义或答案, 我们把这个问题留给专业人员去讨论. 但是它的基本内容可以简单归结为: 信息安全就是研究如何保证敏感信息或消息在公开信道上安全传输. 这一句话中包括了三个内容: 敏感信息、公开信道、保证安全传输. 公开信道包括无线通信、有线通信和互联网通信所用的信道. 信道是公开的就意味着谁都可以使用, 因此, 在公开信道上传输的信息就等于信息公开. 例如, 天气预报、股票价格、机场航班信息等, 这些信息本来就是完全公开的, 因此, 可以直接在公开信道上传输. 但是诸如公司的新技术材料、银行私人账号、电子现金转移, 乃至个人病历和法庭记录等, 除发送方和接收方之外, 不希望第三方能得到这些信息, 称之为敏感信息. 涉及国家政治、经济、军

事等方面的内部重要信息的传输不是本书要讲的内容. 一般来说, 敏感信息的泄露会给通信双方带来很大损失, 因此, 不能直接在公开信道上传输. 但是, 如果使用专用信道则因通信成本太高而不现实. 一个自然的想法就是使用密码将要传输的敏感信息加密后传给接收方, 接收方收到后, 能够进行解密和得到原始信息, 而第三方从公开信道上得到加密后的信息, 他不能解密, 从而得不到原始信息, 于是通信双方通过加密、解密达到安全传输的目的. 这里的关键问题是如何保障第三方不可能从加密后的信息取得原始信息. 例如, 一个计算机用户为防止在电脑中存放的信息被别人窃取, 他设置了密码口令. 对一般非专业人员来说, 很难拿到他的密码口令, 但是对于某些电脑高手或专业人士而言, 可能很快破解出他的密码口令. 因此, 对 "安全" 要有一个合理的, 即符合实际情况且又有理论根据的提法. 在讨论安全性时, 对第三方或攻击方的能力要有充分的估计. 攻击者的能力与他掌握的知识和技术密切相关. 在古代, 加密的方法往往很简单, 但同时攻击者的能力也很差, 因此, 简单的加密方法还是相当安全的. 在今天, 攻击者可使用计算机和互联网, 具有很强的计算能力, 并掌握很深的数学

及相关学科知识, 具有很强的攻击能力, 显见, 简单的加密在今天肯定是不安全的. 但是, 复杂的加密方法也不一定能保证安全. 因此, 必须研究什么样的加密方法或算法在什么样的条件下是安全的. 由此可见, 密码学是信息安全的核心. 另一方面, 接收者如何能拿到完整的 (即没有任何丢失的) 和正确的 (即没有被篡改过的) 信息是信息安全工作者要解决的问题. 与此同时, 注意到随着通信技术、计算机和互联网的迅速发展和广泛使用, 每天都有海量的信息在互联网上传输 (海量信息是指以 T 为单位的信息量, 1T=1024G, 而 1G=1024M), 其中不乏有大量涉及政治、经济、金融、商业及个人隐私的敏感信息. 要使大量的敏感信息通过加密的方法达到安全传输, 必须满足高效的要求, 人们没有耐心在电脑前长时间等待. 因此, 安全与效率必须同时考虑. 此外, 成本因素是不可忽视的.

信息安全有丰富的内容, 包括防火墙、病毒、入侵检测等. 但是, 鉴于本书的篇幅及主旨, 在本书中只讲述信息安全的基本内容, 如数字签名等.

本书的顺序是按密码学发展的进程安排的. 第 1 章密码学术语和基本概念是全书的基础部分, 是了解密码

和信息安全必读的部分,它起到密码和信息安全核心内容的小字典的作用. 第 2 章古典密码体制,主要是通过简单的例子分析,使读者对密码有一些感性的认识. 第 3 章对称密码体制,这是自 20 世纪五六十年代至今仍使用的一种重要的密码体制. 第 4, 5 章, 公钥密码体制及其应用,讲述公钥密码体制基本原理,进而将公钥密码体制用于数字签名、身份识别和密钥交换. 第 6 章密钥共享,属于密钥管理的重要内容,而且在信息安全领域中被广泛应用. 最后一章介绍与现代人密切相关的电子商务的基本原理和框架. 看第 4~6 章的内容时,最好先浏览一下附录. 在附录中,重点讲述辗转相除法和公钥密码所需要的原根和指数的基本概念. 虽然在中学就学过辗转相除法,但是能够完整透彻地了解它还要花些力气. 在附录中,给出了该算法的框图和例子.

阅读本书有两种选择,一是按章节的顺序阅读,二是对电子商务感兴趣的读者可在读完第 1 章后直接读第 4~7 章. 对密码专业感兴趣的人,施奈尔的《应用密码学》是一本权威之作. 对西方密码学历史感兴趣的读者,《破译者》是一本内容丰富的参考书.

最后,作者在此衷心地感谢对本书的出版给予支持

和帮助的各位专家和同仁, 感谢张志芳博士对本书初稿提出的宝贵意见和建议.

作 者

2011 年 4 月于北京

目 录