现代密码学趣味之旅

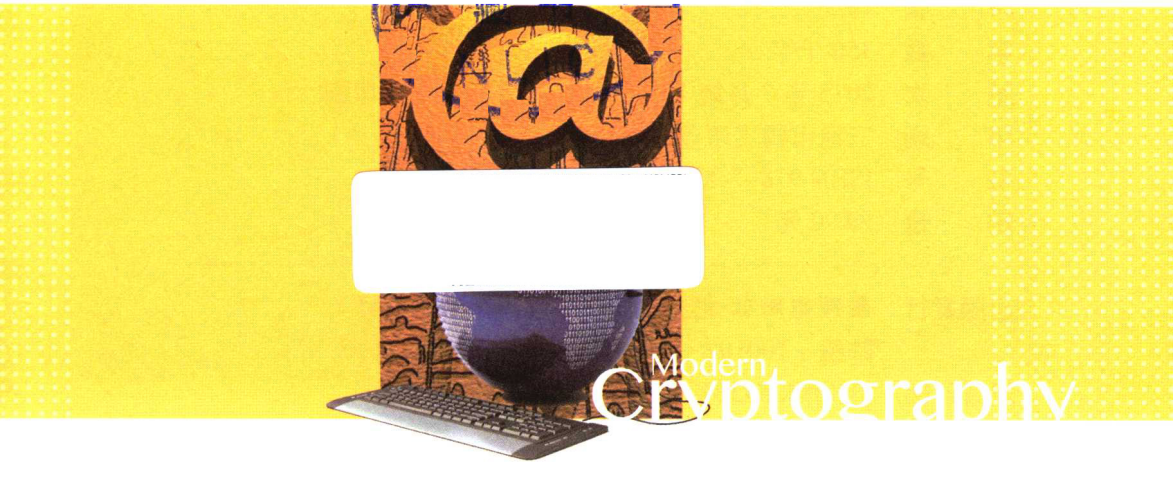
Modern Cryptography

彭长根◎编著

金城出版社
GOLD WALL PRESS

现代密码学趣味之旅

彭长根◎编著



金城出版社
GOLD WALL PRESS

图书在版编目（CIP）数据

现代密码学趣味之旅 / 彭长根编 著 . —北京 :
金城出版社，2015.5
ISBN 978-7-5155-1217-4

Ⅰ. ①现… Ⅱ. ①彭… Ⅲ. ①密码术－普及读物
Ⅳ. ① TN918.1-49

中国版本图书馆 CIP 数据核字（2015）第 070418 号

现代密码学趣味之旅

作　　者　彭长根
责任编辑　谢艳芳
开　　本　710 毫米 ×1000 毫米　1/16
印　　张　19.5
字　　数　350 千字
版　　次　2015 年 7 月第 1 版　2015 年 7 月第 1 次印刷
印　　刷　三河市腾飞印务有限公司
书　　号　ISBN 978-7-5155-1217-4
定　　价　60.00 元

出版发行　金城出版社 北京市朝阳区利泽东二路 3 号
　　邮编：100102
发 行 部　(010)84254364
编 辑 部　(010)64222699
总 编 室　(010)64228516
网　　址　http://www.jccb.com.cn
电子邮箱　jinchengchuban@163.com
法律顾问　陈鹰律师事务所　(010)64970501

商用密码应用丛书

编委会名单

序　言

密码有着数千年的悠久历史，经历了从手工、机械、电子到计算机作业的发展过程，从一种技巧演变成一门科学，特别是近年来，随着我国自主密码技术的迅速发展，密码已广泛应用到军事、外交、政府、能源、金融、交通等关键部门和重要领域，在保障我国网络和信息安全中发挥了重要作用，取得了很好的社会效益和经济效益。密码技术作为保障网络和信息安全的核心技术和基础支撑，在身份识别、安全隔离、信息保密、完整性保护和抗抵赖性等方面发挥着其他技术手段不可替代的重要作用，在当今云计算、物联网和大数据兴起的时代，亟须引起人们更多的关注。

彭长根老师编写的《现代密码学趣味之旅》，通过创设应用场景，采用简单风趣的语言，深入浅出地描述了现代密码学发展历程和技术应用，让带有深深数学烙印且深奥难懂的密码学书籍，变得通俗易懂，非常适合高中生和非信息安全专业的大学生，以及从事相关工作的机关企事业单位人员阅读。

密码科普在我国还处在起步阶段，广大密码工作者有责任和义务花更多的时间来开展这方面的工作，多出一些浅显易懂、可读性强、面向社会公众的书籍，帮助人们更多地了解密码、用好密码，引领有志于密码研究的年轻人进入这个领域，提升我国密码技术自主创新能力，在保障我国网络和信息安全中发挥更大的作用。

中国工程院院士 沈昌祥

2015 年 4 月

前　言

作为中国密码学会理事兼教育工作委员会委员，一直想着为密码学的科普做点事情，这正是撰写此书的最初动机。不曾想在这过程中，渐渐喜欢上了写科普的感觉，科普工作居然出乎预料的如此有魅力。跟着这种感觉，2013 年我做了一个《Diffie-Hellman 密钥交换》的科普视频课，参加了全国高校微课教学比赛，更进一步意识到科普工作的价值，此书的撰写正是在这种感受的驱动下所做的一点事情。

曾几何时，“密码”一词不断地出现在影视作品中，密码技术也徐徐走进了大众的视野。影视剧中扣人心弦的情节，惊心动魄的密码对抗，神乎其神的破译技术，总是能给人们带来无限的好奇和遐想，也激起了越来越多爱好者的探究欲望。荧屏上的密码技术自然是做了艺术化处理的，但有一个不争的事实是：军事战争驱动了密码学的发展，密码学从艺术到科学，自古就与战争联系在一起，从古代战场到现代战争，始终未离开过密码技术的较量。从姜子牙的“阴符 · 阴书”保密之术，到古希腊的“石蜡密信”，从二战的恩尼格玛机，到现代信息战，无不彰显着密码技术的重要作用，甚至可以说，战争催生了密码技术，密码是没有硝烟的战场，是军事领域中的另类较量。其实，密码技术也正在走进我们的生活，不管你是否意识到，它就在我们的身边默默地保障着我们的信息安全。随着信息网络的飞速发展，现实中的业务将不断向网络空间延伸，从电子邮件到现在的电子商务和电子政务，无不依赖着密码技术的护航；我们所熟悉的网络银行、支付宝、证券交易……背后都有坚固的密码技术做后盾。信息网络在给人类社会带来巨大方便的同时，也在深刻地改变着人们的安全观念，网络信息空间的安全已被各国提升到国家安全的战略高度。2014 年，我国成立了“中央网络安全和信息化领导小组”，中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，李克强、刘云山任副组长，领导小组规格之高、力度之大，可谓是前所未有。由此可见，网络空间的安全已不可小视。

密码技术是信息安全的核心技术基础，它解决了信息的保密性和认证性，信息网络中防火墙、安全路由、虚拟专用网、身份认证、访问控制等，依靠的正是密码学中的保密算法和认证算法。然而有密码编码，就会有密码攻击，密

码学正是以密码编码和密码分析两大分支为研究的学科，密码编码和密码攻击总是在不断的博弈之中，可谓是“道高一尺、魔高一丈”。近年来的病毒、木马、黑客、蠕虫、后门等网络攻击的日益剧增，也在悄然促进着密码技术的发展。扣人心弦的密码剧情节，眼花缭乱的网络攻击手段，常让我们跃跃欲试，渴望有朝一日自己也变成一个密码高手，成为信息安全的保护神。可是，每当我们拿起密码书籍来读，才发现那里原来全是一些索然无味的抽象数学符号，顿时让我们的兴趣荡然无存。

面对渴望轻松了解密码技术及其应用的读者，面对日益严峻的网络攻击，作为密码学研究工作者，是到了该做点什么的时候，科普不失为一种不错的选择。近年来，国内外也陆续出版了几本密码学的科普书籍，但大多是介绍古典密码技术，或是战争中的密码故事，未曾见介绍现代密码技术及其应用的作品，这正是萌生撰写本书的初衷。本书是一本现代密码技术与应用的科普书籍，旨在用最通俗的语言、生动的方式和趣味的故事介绍现代密码学方法、技术与应用，如密码学的数学技术、加密、认证、秘密共享、安全多方计算、密钥管理、PKI/CA、轻量级密码和未来密码技术等及其应用场合。主要特色是突出“现代”、“通俗”、“趣味”，通过故事、采访和新闻报道等形式，以主角艾丽和柏彬在学习、生活和工作中遇到的信息安全问题为主线，介绍现代密码学的基础知识和技术，力求文字浅显、通俗、趣味，使读者既能了解实际信息安全问题的解决办法，又能激发对密码学的浓厚兴趣。

本书的读者对象定位为高中生、非信息安全专业大学生、信息技术及数学爱好者、关注信息安全的各行业工作人员和具有中等文化程度的广大民众等。作为一本入门读物，希望能透过浅显的介绍，让读者理解到一点密码学原理，掌握到一点现代密码技术，了解到一点现代密码技术的应用。云计算的风起云涌，大数据的悄然而至，又会有新的安全问题摆在我们面前，云端数据的安全存储亟待解决，大数据的隐私保护不可避免。面对不断涌现的信息技术，此书可作为抛砖引玉之尝试。

贵州大学李祥教授作为国内老一辈计算机科学研究学者，于 20 世纪 80 年代初在贵州大学开辟了可计算性理论和计算复杂性理论研究，并形成一定的优势，基于此基础，李祥教授于 20 世纪 90 年代初期开辟了密码学研究方向，在密码算法与密码协议、模型检测方面取得了不少的研究成果，在国内形成了一定的影响。自从被恩师李祥教授引领进入密码学研究的大门，我未敢放松对密码学研究的关注，尽管身处欠发达地区工作，但仍希望能贡献一点绵薄之力，本书若能为老一辈人创建的平台增加点色彩，我将欣慰之至。

本书得以完成，我首先要感谢亲如家人的研究生们，在中科院信息工程研究所做博士后的田有亮博士，为本书答辩和出版手续做了不厌其烦的工作。朝夕相处的周洲、杨玉龙、刘海（小）、任祉静、丁红发、杨震、徐志聘、张豹、吕桢、刘海（大）、王伟茹、原志龙、刘荣飞、张铎等研究生为本书的资料收集和整理做了大量的工作；更要感谢国家密码管理局和中科院信息工程研究所的支持，你们的支持是本书得以出版的重要基础；与此同时，我怀着深深的敬意感谢沈昌祥院士，您对本书的肯定是我撰写的动力。最后，衷心感谢为本书评审和提出宝贵建议的专家、学者和领导，本书包含了你们的智慧。

彭长根

2015 年 2 月

目录

第 1 章

漫步密码学的发展之路

乍一听“密码”这个词，也许你会对它充满好奇，自古以来，“密码”一词总是蒙着一层神秘的面纱，它给人们的感觉总是那么神乎其神，被认为是高智商的人才能玩的游戏。其实不然，密码学并不神秘，它就源于我们的生活，而且非常美妙，同时又反过来服务于我们，我们的身边就充满着密码技术的应用。还在大学读书的艾丽和柏彬，近来也忽然对密码学产生了浓厚的兴趣，艾丽更关注的是密码学的发展历程，而柏彬却对战争中的密码战更感兴趣。本章我们将与艾丽和柏彬一道，从密码学的起源出发，以有趣的故事，带您轻松愉快地漫步密码学发展之路，让您领略从古典密码学到现代密码学的历程。相信您也会和艾丽与柏彬一样，了解密码学，接受密码学，爱上密码学，那就拭目以待吧！

1.1 追溯古代信息保密之术

密码技术的历史起源很难追溯，戴维·卡恩（David Kahn）在《破译者》一书中就曾说道：“人类使用密码的历史几乎与使用文字的时间一样长。”

一天，艾丽去另一所学校看望同学，被同学带到该校的文化书院参观，艾丽随手从书架上拿出一本战国时期的《六韬》翻阅，居然发现第三卷的《六韬·龙韬》是一本中国古代兵书，它通过武王和姜子牙的对话，阐述了用兵作战的原则。该卷还记载了采用“阴书”方法来传递军情，其中有一句话为“敌虽圣智，莫之能识”，正是一种秘密传递军情的方法。

阴书这种保密之术可以看作是密码学的萌芽，也标志着中国古代的秘密通信方法已具有了密码学的雏形。密码学就是一种将公开信息转化为秘密信息的技术或者方法，简单地说，密码学是研究密码设计和密码破译的科学。加密是密码学中最重要的技术方法之一，它是从古至今的一种保密通信的技术手段。作为四大文明古国之一的中国，在古代就已发明出种种加密手段，内容丰富，形形色色，多种多样，《六韬·龙韬》正是我国古代密码技术应用的佐证。

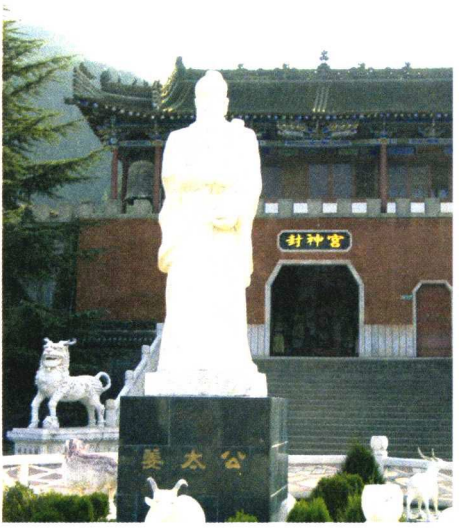


图 1.1 姜子牙塑像

有了上次文化书院的经历，艾丽对古代中国保密之术的兴趣油然而生。有时间她就上网浏览，发现宋代的兵书《武经总要》中也记载了一些军事保密方法，宋代的军事活动有请刀、请弓、请马、请甲、请牛车、请添兵、请进军、请固守、贼多、贼少等四十多项。为了传递军事情报的安全，宋代军队常用一首共有 40 个字的诗传递情报，用其中不同的字代替不同的军事活动，也就是说，用“字验”的方式实现军事的秘密通信。杜甫的《春望》就是其中的一首，在杜甫的《春望》中，诗句“家书抵万金”的“金”字表示“贼多”，那么当指挥官在传递情报时，就可以在“金”字上做一个记号，收到军事情报的人，根据“字验”的方法获得敌人秘密的军情。

的确，在浩瀚的中国历史文化中，有许多保密技术的记载。常在影视作品中出现的隐写墨水技术，我国古代就有之。南宋时期，据《三朝北盟汇编》记载，公元 1126 年，开封被敌军围困时，宋钦宗“以矾书为诏”发出指令，就是采用“以矾书帛，入水方见”的隐写技术，它是在布条上，用明矾溶于水得到的“矾水”来书写秘密情报，收到该情报的人将布条浸水后可看见军事情报，隐写术成为了另一种重要的秘密军事情报传递的形式。另外，藏头诗也是我国古代常用的一种保密技术，藏头诗有不同的书写方式，但最常用的是将消息分藏于诗句之首，每句的第一个字连起来读，就是隐藏的消息。

藏头诗应该算是艾丽最感兴趣的一种信息隐写方式了，她记得在中学阅读中国四大名著之一的《水浒传》时，有一个故事叫“吴用智赚玉麒麟”，这个故事说的是巧用藏头诗将卢俊义逼上梁山。水泊梁山头领宋江对人称“河北玉麒麟”的豪杰卢俊义仰慕已久，一心想让他上梁山，共谋大业。可对朝廷忠心耿耿的卢俊义偏偏不如宋江所想，宋江为此感到很苦恼。宋江的军师“智多星”吴用，利用卢俊义正为躲避“血光之灾”的惶恐心理，给卢俊义算了一卦并写了四句卦歌：“芦花丛中一扁舟，俊杰俄从此地游。义士若能知此理，反躬难逃可无忧。”巧妙地把“卢俊义反”四个字藏于四句卦歌之首，这正是藏头诗的手法，而这却成了官府治罪的证据，最后官府到处追捕卢俊义。实在没办法的卢俊义，最终被逼上了梁山。

“吴用智赚玉麒麟”的故事就是采用藏头诗实现古代密码术的一个具体佐证。在明朝时期，著名的军事家戚继光发明了反切密码，它采用中国汉字注音方法中的“反切法”来设计。戚继光的反切密码，为他在抗倭战争中秘密传递军事情报提供了重要安全保障。事实证明，戚继光的反切密码是相当难以破译的。其实在东汉末年，就出现了反切注音法，戚继光的反切密码是否参考了这种方法已难以考证。

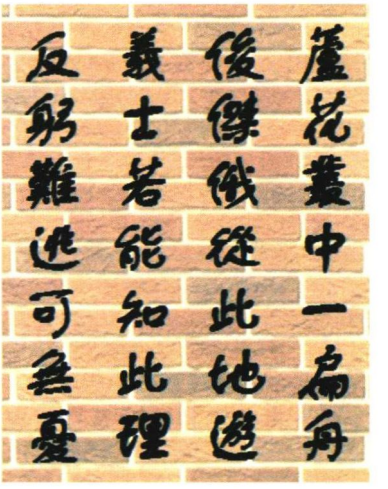


图 1.2　《水浒传》中的藏头诗

国外的密码起源最早可追溯到数千年前的古希腊、古罗马时代。早在公元前 2000 年，有人发现古埃及贵族墓碑上的象形文字很奇特，人们猜测那是一种保密方法，是书法家经过变形处理之后写的。记载最早的保密通信的应用是在公元前 480 年，一个希腊人将军事情报写在木板上并用一层蜡遮盖，以此将情报巧妙地秘密传递。另一种隐写方式是在公元前 440 年的古希腊战争中，用一种“光头刺字”的隐写术来传递情报：先找一个自己家的奴隶，把他的脑袋剃成光头，然后将情报写在他的头上，待头发长出之后，让奴隶前往收信方。奴隶见到收信方之后，收信方剃掉奴隶的头发就可以看到情报了。除了隐写密码术外，雅典和斯巴达战争中的腰带密码，使用的是一种置乱式密码技术。

有了对古代保密技术的了解，艾丽对前人的智慧十分佩服，对我国璀璨的古代文化充满了自豪。一天，她猛然记起课本中曾提到过“恺撒密码”，莫非也有什么典故？她查阅了有关资料，知道在恺撒大帝用于记录军事行动的《高卢战记》对此有所记载：公元前 54 年，恺撒的爱将西塞罗遭到维尔纳人的围攻，情况十分危急，恺撒需要传递作战计划给他的爱将，就以极高的报酬说服了一个士兵，送一封作战计划给西塞罗将军。

其实，恺撒送去的是用密码写的一封特殊信件，他送的是什么密信呢？用的是怎样的密码呢？这正是历史上广为流传的“恺撒密码”，在后面将有详细介绍。

以上所介绍的这些都是密码技术的雏形，一定程度上体现了密码技术的源远流长！