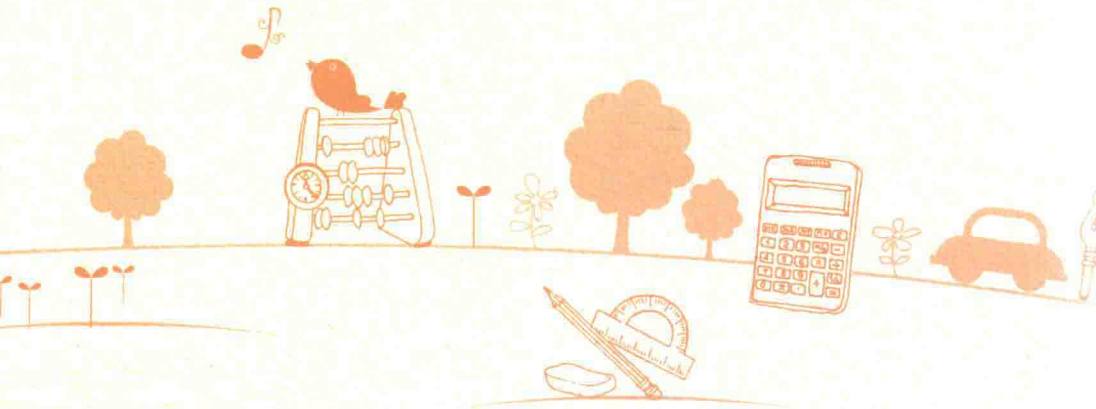
‖快乐阅读书屋‖

项昭　分册主编
严虹　编　著

情报保护神
——密码

happy reading 数学知识类



贵州出版集团
贵州人民出版社

情报保护神

——密　码

严　虹　编著

贵州出版集团
贵州人民出版社

图书在版编目(CIP)数据

情报保护神——密码 / 严虹编著. —贵阳：
贵州人民出版社，2013.9
ISBN 978-7-221-11368-9

Ⅰ.①情… Ⅱ.①严… Ⅲ.①密码-研究
Ⅳ.①TN918.2

中国版本图书馆 CIP 数据核字(2013)第 201343 号

情报保护神——密码

严 虹 编著

出版发行	贵州出版集团 贵州人民出版社
地 址	贵阳市中华北路 289 号
责任编辑	徐 一
封面设计	熊 锋
印 刷	贵阳经纬印刷厂
规 格	850mm×1168mm 1/16
字 数	150 千字
印 张	11.5
版 次	2014 年 7 月第 1 版
印 次	2014 年 7 月第 1 次印刷

书 号：ISBN 978-7-221-11368-9 定 价：23.00 元

出版说明

兴趣是最好的老师，知识的学习更是如此。如果学习者缺乏兴趣，阅读就将是一个枯燥无味的过程，轻松快乐的学习也就无从谈起。基于这样的事实，本着“兴趣阅读、快乐学习”的理念，我们经过深入调研，与国内的众多专家学者及一线教师全力合作，为所有希望将学习变得轻松愉快的朋友奉献上“快乐阅读”书屋。

“快乐阅读”书屋，以知识的轻松学习为核心，强调阅读的趣味性。它力求将各种枯燥无味的知识以轻松快乐的方式呈现，让读者朋友便于理解接受。它的各种努力，只有一个目标，即力图将知识学习过程轻松化、趣味化。读者朋友在阅读过程中，既能保持心情愉快，又能学有所得。在轻松愉快的氛围中学习，让知识学习成为读者朋友的兴趣，本身就是提高学习效率最有效的途径。

“快乐阅读”书屋首批图书分为“语文知识”、“作文知识”、“数学知识”、“文学导步”、“文学欣赏”、“语言文化”、“个人修养”七大板块，各个板块之下又有细分。英语、生物、化学等相关的知识板块将会在以后陆续推出。针对不同学科知识的特点，本书屋以不同的方式来达到轻松快乐的目的。要么是以故事的形式，在故事的展开之中融入相关知识；要么是理清该知识点的背景，追根溯源，让读者朋友知其然，更知其所以然，让理解更为轻松。总而言之，就是以最恰当的方式呈现相关的知识。

希望这套“快乐阅读”书屋能陪伴每一位读者朋友度过美好的阅读时光。

编　者

2014 年 5 月

卷首语

亲爱的读者朋友们，从这首诗中你看出了什么？试一试把每句诗的第一个字连起来读一下。

对啦！前面就有本书书名“情报保护神——密码”。

密码是按特定法则编成，用以对通信双方的信息进行明密变换的符号。换而言之，密码是隐蔽了真实内容的符号序列。其实在公元前，秘密书信已用于战争之中，西方“史学之父”希罗多德的《历史》当中记载了一些最早的秘密书信故事。隐写术也出现在古代，希罗多德记载将信息刺青在奴隶的头皮上，较近代的隐写术使用隐形墨水、缩影术或数字水印来隐藏信息。中国古代秘密通信的手段，已有一些近于密码的雏形。中国周朝兵书《六韬·龙韬》也记载了密码学的运用，其中的《阴符》和《阴书》便记

载了周武王问姜子牙关于征战时与主将通讯的方式。

显而易见，有着悠久历史的密码学在信息安全大厦中起着无可替代的作用。事实上，在当今社会中密码是解决网络信息安全的关键技术，是现代数据安全的核心。像身份识别、信息在存储和传输过程中的加密保护、数字签名和验证等都要依靠密码技术才能得以实现。

本书通过三个虚拟人物所代表的加密者、解密者和非法破解者来讲述一系列的故事，向读者讲述了密码学的基本概念，回顾了密码的昨天、了解密码的今天、展望密码的明天！

你想知道《福尔摩斯探案集》中有关人形密码的故事吗？你想知道西方的恺撒大帝与咱们中国古代女皇帝武则天这两位密码能手谁更胜一筹吗？你想知道网络上的数字签名是怎么回事儿吗？你想知道未来信息世界里能让所有黑客失业的最安全的密码是什么吗？

那么，就让我们走进奇妙的密码世界，一起认识这位从古到今的情报保护神吧！

目 录

密码，其实并不神秘

2003 年 3 月 18 日，美国作家丹·布朗的一本畅销小说《达芬奇密码》出版，以 750 万册的成绩打破美国小说的销售记录，目前全球累计销售量更已突破 6000 万册，成为有史以来最卖座的小说之一。后来被改编成电影，也取得了不错的票房成绩。该书是关于男主角，哈佛大学的宗教符号学教授罗伯特·兰登解决巴黎卢浮宫声望卓著的馆长被谋杀一案的故事。馆长赤裸的尸体以达芬奇的名画维特鲁威人的姿态在卢浮宫被发现的，身边写下一段隐秘的信息并且用血在肚子上画下神秘的符号。在追查案件的过程中，一些达芬奇的著名作品中隐含的信息，包括《蒙娜丽莎》、《最后的晚餐》等，都逐渐浮出水面……

《达·芬奇密码》书籍封面及电影海报

近年来，与“密码”一词相关的书籍、影视作品越来越多地出现在公众的视野中。密码，一个既陌生又熟悉的名词。说她陌生，因为她总是戴着

一层神秘的面纱，在某个角落中默默地注视着我们；然而她又是那么的熟悉，在日常生活中，几乎天天都要接触到。

宽带连接需要输入密码

登录 QQ 需要输入密码

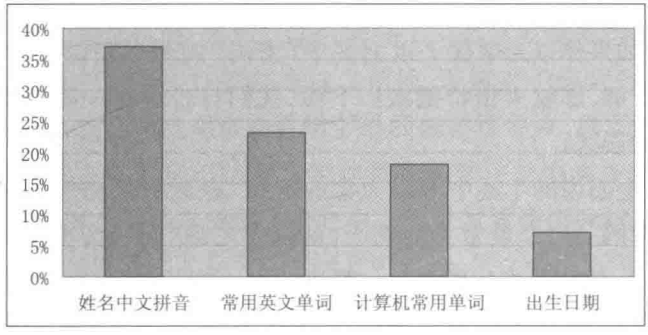
银行取款需要密码

密码锁

保险箱

通讯系统的迅猛发展提高了人们在互联网、自动取款机等设备使用密码进行信息保密的要求。随着通讯手段的丰富与发展，密码使用无处不在，与我们每个人的生活息息相关，作为个体，必须认真采取有效的防泄密措施，避免由此带来的不必要损失。

每个人都以为自己想的密码不会被别人知道，有趣的是，大部分人使用的密码可以轻易地被猜出来。有人对 100 个大学生做过一个调查测试，结果发现，在密码设置中：用自己姓名的中文拼音者最多。通过调查发现，人们设置密码的原则是简单、易记，能够很快地敲出来。于是，有了诸如“123456”的“超级简单密码”，有“昵称 +888”之类的“幸运数字密码”，还有手机号、电话号等“懒惰型密码”等等，当然也有一些如同@ #123 这样的“聪明型密码”。



密码设置偏好统计

那么我们应该如何设置密码呢？不妨听听网络安全专家设置密码的诀窍：

1. 使用大写字母和小写字母、标点和数字的集合。

2. 在不同账号里使用不同的密码，有规律性地更换密码。为了容易记得更换密码，将它和一件事联系起来。例如在每月的第一天或发薪日更换密码。

3. 使用一个方便你记忆的密码，那么你便不必写下来了。

4. 不要使用任何和你有关的姓名和数字，如出生日期或是绰号。

5. 不要使用任何语言的字词作为密码。

6. 不要使用可轻易获得的关于你的信息，包括电话号码、手机号码、你所居住的街道的名字等。

选好了密码，剩下的工作就是不要忘记它。

如何记住密码？一个好的密码应该是你自己容易记住但别人不太容

易猜到的，看看下面的例子吧：

1. 找一首熟悉的歌，使用句中每个汉字拼音的首字母作为密码的一部分。

2. 选择两个没有任何共同点的短词，将它们用标点或数字连接起来，如：*Teacher* 6 *Apple*。

3. 使用一个熟悉的短语，但是要用数字 0 来代替字母 O，采取一些诸如此类的措施。

然而，如果你以为掌握了以上关于“密码”的基本知识，就对密码学有了基本的了解，那就大错特错啦！下面，我们将告诉你一些大多数人关于密码认识的误区。

其实，上面说的生活中习以为常的这些“密码”，严格来说并不能算是数学中的密码。一个最常见的例子，就是使用银行卡时，机器要求我们输入的“密码”，就不是真正的密码。精确地说，它应该被称为“口令”，它没有隐藏任何信息，所有人得到它都可以使用，它只是提供了一个额外的身份验证信息而已。因为“口令”并不是依照正常的加密规则对“用户名”之类的信息进行加密后得到的，而且也不能通过正常的解密规则“还原”出初始的用户名。而类似这种并非使用标准加密变换机制生成的所谓“密码”，当然也就根本不能算是真正的密码。类似的“用户名 - 口令”体系在我们的生活中经常可以碰到，除去上面说的银行卡以外，还包括登录计算机、登录电子邮箱、登录 QQ 之类及时通信软件等。实际上，在这些需要“密码”的场合，密码都没有出现，尽管口令有时会被加密以便安全传输，但那与口令本身是不是密码毫无关系。从普遍意义上讲，口令仍然与用户名信息没有充分必要的关联。

既然如此，那么什么才是真正的密码呢？《辞海》中是这样描述的：按特定法则编成，用以对通信双方的信息进行明密变换的符号。

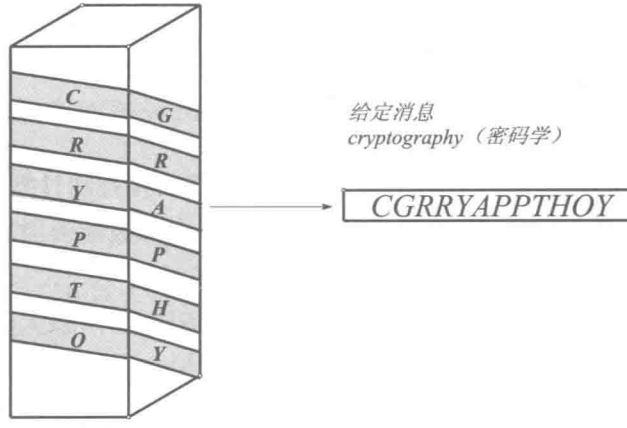
其实，密码是一门有着悠久历史的科学。相传在公元前 405 年，雅典和斯巴达之间的伯罗奔尼撒战争已进入尾声，斯巴达军队逐渐占据了优势地

位，准备对雅典发动最后一击。这时，原来站在斯巴达一边的波斯帝国突然改变态度，停止了对斯巴达的援助，意图是使雅典和斯巴达在持续的战争中两败俱伤，以便从中渔利。

在这种情况下，斯巴达急需摸清波斯帝国的具体行动计划，以便采取新的战略方针。正在这时，斯巴达军队捕获了一名从波斯帝国回雅典送信的雅典信使。斯巴达士兵仔细搜查这名信使，可搜查了好大一阵，除了从他身上搜出一条布满杂乱无章的希腊字母的普通腰带外，别无他获。情报究竟藏在什么地方呢？斯巴达军队统帅莱桑德把注意力集中到了那条腰带上，情报一定就在那些杂乱的字母之中。他反复琢磨研究这些天书似的文字，把腰带上的字母用各种方法重新排列组合，怎么也解不出来。最后，莱桑德失去了信心，他一边摆弄着那条腰带，一边思考着弄到情报的其他途径。当他无意中把腰带呈螺旋形缠绕在手中的剑鞘上时，奇迹出现了。原来腰带上那些杂乱无章的字母，竟组成了一段文字。这便是雅典间谍送回的一份情报，它告诉雅典，波斯军队准备在斯巴达军队发起最后攻击时，突然对斯巴达军队进行袭击。斯巴达军队根据这份情报马上改变了作战计划，以迅雷不及掩耳之势攻击毫无防备的波斯军队，并一举将它击溃，解除了后顾之忧。随后，斯巴达军队回师征伐雅典，终于取得了战争的最后胜利。

雅典间谍送回的腰带情报，就是世界上最早的密码情报，具体运用方法是，通信双方首先约定密码解读规则，然后通信方将腰带（或羊皮等其他东西）缠绕在约定长度和粗细的木棍上书写。收信方接到后，如不把腰带

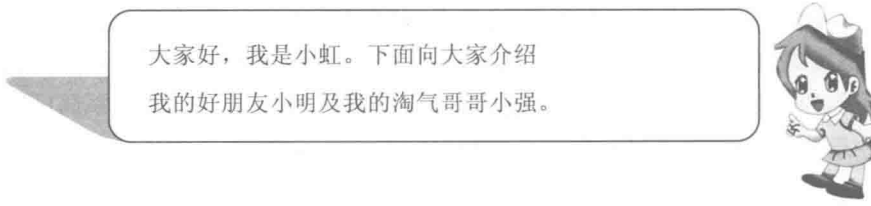
缠绕在同样长度和粗细的木棍上，就只能看到一些毫无规则的字母。后来，这种密码通信方式在希腊广为流传，被称为 *Skytale* 加密法。现代的密码电报，据说就是受了它的启发而发明的。



Skytale 加密法示意图

这就是密码学发展的雏形时期，古希腊墓碑的铭文志、隐写术、古代的行帮暗语以及一些文字猜谜游戏等都是古代加密方法。这种加密方法通过原始的约定，把需要表达的信息限定在一定的范围内流通，已体现出了密码学的若干要素，但只能限制在一定范围内使用。

为了接下来更好地进行本书的阅读，我们通过一个虚拟的故事来介绍一下密码学中几个重要的基本概念，同时，故事中的三个主人公（小明、小虹、小强）将会伴随我们直到本书阅读结束：



大家好，我是小明，小虹的好朋友。
我经常给小虹写信。

大家好，我是淘气鬼小强，小虹的哥哥。
我经常偷看小明和小虹的通信，好奇嘛！

小明和小虹是一对好朋友，由于父母工作调动，分居两地。基本设定之一就是：他们联系彼此的手段，只有写信——不提手机和互联网。可是小虹的哥哥小强非常调皮，总是私拆这对好朋友的信件。令他们头疼的是，来往信件必须经过小强过目，这就是故事的基本设定之二。

为此，小明与小虹约好，开始使用“特定代码”炮制天书——这就是说，他们要开始使用密码了。具体来说，小明先写好一封信，然后找来《现代汉语词典》，把信中的每个字都查出来，然后把这些字在字典中对应的页码数和行数都记录下来，再按行文顺序抄录在另一张纸上，最后寄出。小强成功地截获了这封信，但是完全没有看懂里面的一串串数字在说什么。最后，小虹成功地拿到信，又拿出《现代汉语词典》，把文字翻译出来，成功地读到了一封来信。

故事讲到这里，“密码学”的几个最重要概念都已经先后呈现：

小男孩小明：加密方、发送方

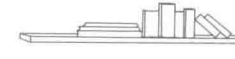
小女孩小虹：解密方、接收方

小虹哥哥小强：非法接收方

原文：明文

《现代汉语词典》：密本

根据《现代汉语词典》转抄：加密过程



抄录的信:密文

寄信:密码通信

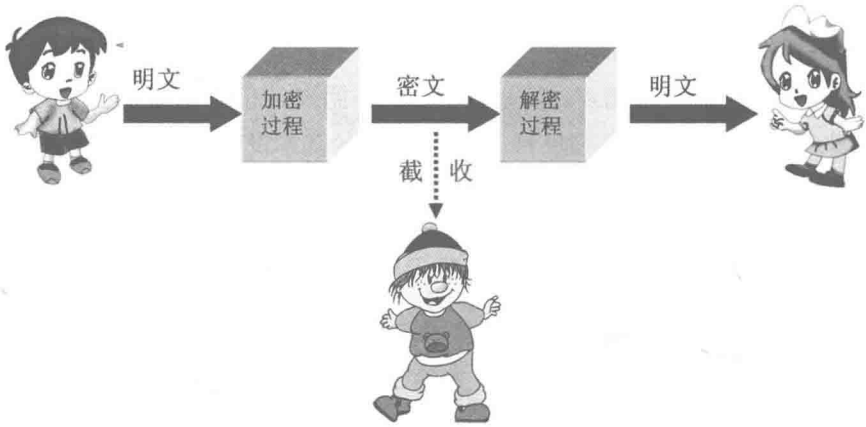
小强收到信:截获

小强读信:密码破译

小虹读信:解密过程

如此一来,上面那个故事,就可以用密码术语重新改写成一句“冷冰冰”的话:

发送方(小明)使用密本,对明文进行加密或密码编码,发送后遭到非法接收方(小强)的截收;但非法接收方破译或密码分析失败,而接收方(小虹)成功解密。



加密规则与解密规则互为逆运算,由于他们事先约定好了运算规则,并且高度保密,所以这一对运算分别被称为**加密密钥、解密密钥**。

密码无处不在,在数字化时代的今天,我们每个人更是被一大堆编码所加密。围绕密码所展开的斗争甚至远胜于战争本身,它既是人类智力的另类较量,又是数学神秘之美的比拼。

如果你既聪明又勤奋,那你也能学会如何破解密码。我们将大致按照

密码学发展的时间线索，向你展开密码发展长达几千年的瑰丽画卷；使你了解并学会使用一些从古至今最重要的密码方法，以及其他保密通信的基本方法。

你准备好了吗？让我们跟随着小明、小虹和小强一起进入奇妙的密码世界吧！