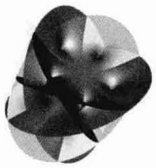
丘成桐中学数学奖
指定参考书

趣味密码术与密写术

Codes, Ciphers and Secret Writing

M. 加德纳 著
王善平 译

高等教育出版社
Higher Education Press



丘成桐中学数学奖
指 定 参 考 书

趣味密码术与密写术

Codes, Ciphers and Secret Writing

■ M. 加德纳 著
■ 王善平 译

高等教育出版社
Higher Education Press

图书在版编目 (CIP) 数据

趣味密码术与密写术 / (美) 加德纳 (Gardner, M.) 著; 王善平译. —北京: 高等教育出版社, 2008.10

书名原文: Codes, Ciphers and Secret Writing

ISBN 978-7-04-025383-2

I. 趣… II.①加… ②王… III. 密码—研究 IV. TN918

中国版本图书馆 CIP 数据核字 (2008) 第 143180 号

策划编辑 李 鹏 **责任编辑** 李 鹏 **封面设计** 张 楠

责任校对 杨凤玲 **责任印制** 陈伟光

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**免费咨询**	800-810-0598
邮政编码	100120	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	北京七色印务有限公司	**畅想教育**	http://www.widedu.com
开 本	889×1194 1/32	**版 次**	2008 年10月第 1 版
印 张	3.5	**印 次**	2008 年10月第 1 次印刷
字 数	70 000	**定 价**	15.00 元

本书如有缺页、倒页、脱页等质量问题, 请到所购图书销售部门联系调换。

物 料 号 25383-00

丛书序

任何科技发展都不能缺乏数学作为根基, 数学在科技年代, 地位日益重要. 而教育的目的不仅要学生懂得书本上介绍的基本知识, 也需要培养学生应变、创新和领导的能力. 学习基本知识可以在不断的考试中磨炼出来, 我想这方面中国的学生在考试里面磨炼不少了, 至于应变、创新和领导能力, 恐怕单从考试是不够的. 为激发全球华人青少年对数学的兴趣, 提升他们的学术水平, 并及早发掘与培养全世界的华人数学英才, 由我和泰康人寿保险股份有限公司共同主办的 "丘成桐中学数学奖" 竞赛于 2008 年在北京正式启动. 第一届 "丘成桐中学数学奖" 颁奖仪式定于 2008 年 10 月 24 日在北京举行, 届时, 美国哈佛大学、布朗大学、斯坦福大学等名校的本科招生主任将会出席仪式, 并面试部分

获奖学生.

为了配合这项活动,我们精心挑选了国外一批著名的数学科普读物,由高等教育出版社组织翻译并以丛书的形式出版. 这套丛书作为 "丘成桐中学数学奖" 的重要参考材料,涵盖了数学的各个分支学科,集知识性、趣味性于一体,对促进中学生的思维和创新能力都有很大的帮助. 希望同学们能从中汲取知识,开阔视野,在比赛中取得优异的成绩.

丘成桐 (Shing-Tung Yau)

2008 年 8 月

引　言

密码术 (cryptography, 也称为密码学) 是关于用密码写信文和解密码信文的技术和学问. 翻开任何国家的历史, 总能看到密码术——或者是其他形式的密写技术——在其中起着至关重要的作用. 时至今日, 情况仍然如此. 在我们这个疯狂的世界里, 政府和间谍们必须使用加密方法来传送特别的信息. 各大国同样必须设立由密码分析专家组成的专门机构, 这些专家们坐在电子计算机前, 夜以继日地工作, 试图破解其他国家使用的密码. 有关密码分析的历史太吸引人了 (正如戴维 · 卡恩 (David Kahn) 在他的大部头著作《密码破解者》(*The Codebreakers*) 中所精彩描述的那样), 其中充满了戏剧性的事件: 帝国和政治领袖的命运系于一小群专门从事于破解字谜这一古老而有趣行当的专家们工作的成

败.

我说 “一小群”, 是因为在古代这种破解密码的工作往往只由几位密码分析专家来完成, 有时甚至就一个人. 如今, 破解密码已经成为一个人数众多且发展迅速的职业. 没有人能准确地知道, 在美国有多少人在从事这种工作. 但他们肯定有好几万人, 而且每年要花费掉 10 多亿美元. 在第二次世界大战中, 仅在英国就有 3 万人被指派做此工作. 破解密码可能是美国政府收集情报的最可靠的方法.

1942 年美国海军在中途岛取得了一场伟大的胜利, 其直接原因是由于美军已经破解了日本人的 “紫色” 密码机①; 本书第五章将介绍这一破解密码的出色业绩. 在同一场战争中, 1943 年德国的 U 潜艇不断地击沉盟国的船只, 是因为德国人已经破译了英国商船使用的密码. 直到后来美英两国的密码专家破解了德国潜艇使用的密码, 局面才得以扭转.

在第一次世界大战期间破译的一份密件曾经在近代史上产生了最重要的影响. 1917 年, 德国外交部长亚瑟 · 齐默曼给墨西哥政府发了一份电报, 他使用了代号为 0075 的外交密码. 电报中他声称德国计划将进行无限制的潜艇战. 如果美国介入战争, 电文继续说, 德国将承诺把 [美国的] 亚利桑纳州、得克萨斯州和新墨西哥州划给墨西哥, 只要墨西哥同意参加对美国作战. 这

①作者在此的叙述有误. 事实上, 美国海军取得中途岛战役的胜利是因为破译了日本海军使用的 JN-25 密码, 并非是破译了日本外交官使用的 “紫色” 密码. 详见第五章中有关说明.——译注

份电报被英国情报部门截获并破译,然后交给了当时的美国总统伍德罗 · 威尔逊.

美国在此之前并不愿意介入战争. 但是齐默曼电报令国会和公众极为愤怒,于是美国向德国宣战了. 如果当时不这样做,德国人很可能会赢得那场战争. 卡恩写道: "从来没有一次破译密信的成功,导致产生如此大的转折."

对于密码术感兴趣的,并不仅限于政府和职业间谍. 每个人都想保有自己的秘密,显然这就是有那么多的年轻人喜欢收发密码信件的原因,即使那些信件中并不含有什么特别的秘密. 密码信件对于加密者和解密者来说都是一种乐趣,但如果能够破解别人的密码那就更有趣了. 如果您属于一个秘密俱乐部,您和您的朋友可能会需要使用本书所介绍的某种加密方法来进行相互之间的通信. 如果您在写日记,您可能为了防止别人偷看而要使用密码.

许多名人在写日记时,全部或部分使用密码. 弗兰克林 · 德拉诺 · 罗斯福 (Franklin Delano Roosevelt, 1882—1945)[①] 在 21 岁时写的日记中,有 4 篇是用密码写的. 1971 年,这些加密日记首次交到了几位密码专家的手中,他们毫不费事地破解了它们. 这其实是一种简单的替换加密方法: 用数字替换元音,用另外一些符号替换辅音. 破译是如此的容易,以致有人觉得奇怪,罗斯福搞这么简单的加密究竟有何意义?

[①] 1933—1945年任美国总统.——译注

如果您既聪明又勤奋, 那您也能学会如何破解密码. 如今, 破译替换加密的信文已成为一种很受欢迎的字谜游戏, 有足够多的爱好者在热衷于破解每天刊登在美国几百种报纸上的 "密文". 甚至有一个 "全美密文协会" (American Cryptogram Association), 它出版一份双月刊, 刊名就叫《密文》(*The Cryptogram*). (如果您想订阅, 可写信给他们的财务主管, 地址是: 密苏里州墨西哥市西门罗大街 604 号, 邮编 65265.) 我们将在第三章中为您介绍破解替换密码的奇妙艺术.

然而, 本书的主要目的是要教会您如何使用从古至今所发明的最重要的密码方法, 以及其他的保密通信方法. 本书末尾选列了一些参考书, 这些书将会进一步介绍有关加密和破解别人密码的非凡技术.

我在此衷心地感谢小戴维 · 埃森德拉兹 (David B. Eisendrath, Jr.), 他提供了许多绝妙的建议, 已被我采纳于第六章中. 还要感谢戴维 · 卡恩, 他所写的《密码破解者》是本书的主要信息来源.

马丁 · 加德纳

目 录

第一章　易学易用的换位加密术

换位加密并不改变原信文的任何字母 (密码专家把未加密的原文称为 “明文” (plaintext), 但我们将简单地称之为 “信文” (message)). 它只是按照某个保密的规则把字母重排, 使得任何知道该规则的人都能够把字母放回原来的位置而读懂信文.

最简单的换位加密只是把信文回写. 如

AGENT 427 IS ON HIS WAY (间谍 427 正在路上)

回写就成了 YAW SIH NO SI 724 TNEGA. 如果信文本身正好是一段 “回文” (palindrome)—— 顺着读倒着读都一样的句子——那么信文回写后的字母顺序完全不变. 如

PULL UP IF I PULL UP (拉起, 如果我拉起)

和

TIS IVAN ON A VISIT (TIS IVAN 在访问).

不过, 真实的信文是不大可能出现这样情况的.

回写加密方法的主要问题在于, 它太容易被别人识破了. 如果您保持信文中词的顺序, 只是把其中每个词分别进行回写, 这样做会增加一点破解的难度, 但也不会太难. 以下介绍的换位加密方法要更好些, 而且也很容易记住和使用.

1 栅栏加密法 (The Rail Fence Cipher)

假设您要加密这样一段信文:

MEET ME TONIGHT

(今晚见我)

数一下其中字母的个数. 如果个数正好是 4 的倍数, 那么很好. 否则的话, 在信文的末尾补加足够的哑字母 (dummy letters), 使其字母个数正好为 4 的倍数. 在我们的例子中, 这段信文共有 13 个字母, 所以再加上 3 个哑字母 QXZ, 使总数达到 16. 这些哑字母叫做 "空" (null). 等一下我们就会看到, 为什么要加上这些 "空".

把信文中的字母写成一上一下的样子, 使它看上去就像铁路两旁的栅栏:

M E M T N G T X
E T E O I H Q Z

把上面一行抄下来, 然后再抄下面一行. 我们就得

到:

M E M T N G T X E T E O I H Q Z

如果您把密文分成4个或5个字母一组,这样加密和解密就会更简单更准确;因为您在一组一组地写信文时较容易记住那么多的字母. 另外, 这也使 "敌人" 更难 "破解" 密文,因为这里看不出词与词之间的间隔.本书将采用 4 个字母一组的方法. 这就是要在上面的信文中加 3 个 "空" 的原因. 通过把字母数增加到 16 个,我们可以保证密文中的最后一组有 4 个字母,同其他组一样.

密文的最后形式将会是这样的:

MEMT　NGTX　ETEO　IHQZ

解密就像加密一样容易. 首先,用一根竖线把整个密文对分:

MEMT　NGTX | ETEO　IHQZ

现在,依次检出如下字母: 左半边第 1 个字母,右半边第 1 个字母,左半边第 2 个字母,右半边第 2 个字母……这样一直下去,就读出了原文. 末尾的三个 "空" 被忽略. 很容易猜到词与词之间的间隔在哪里.

如果您愿意,您可以把栅栏加密的上下两行位置颠倒;也可以把其中的一行顺写,而另一行回写. 当然,解密的过程也要作相应的改变,您可以很容易地自己确定此过程.

另一种栅栏加密的变形是把它写成多行锯齿形. 例如, 一个 3 行栅栏加密的样子会是这样的:

```
M   M   N   T
 E T E O I H Q Z
  E   T   G   X
```

从而得到密文:

MMNT ETEO IHQZ ETGX

学习一种加密术的最好方法就是用它来解密一个实际的信文. 您会在本书各节之后看到一些 "谜语" 以及加密的答案, 只有通过解密才能看到答案. 请不要直接在书页上进行解密. 把答案密文抄在另外的纸上, 然后在那张纸上做所有的解密工作. 这样就不会损坏书, 因而也不会扫了下一位读者的兴致 (如果这是一本图书馆的书的话), 或让一个想向您借书的朋友感到无趣了.

谜语 1

What goes "Tee, he, he, he, he, plop!"? ("嘻, 他, 他, 他, 他, 扑落!" 发生了什么?)

AALU HNHS EDFY MNAG IGIH AOFZ

(这是一个用两行栅栏加密的密文. 读的顺序是从左到右.)

2　曲路加密法 (The Twisted Path Cipher)

这是用“字母置乱技术” (letter-scrambling technique) 来改进栅栏加密法. 它需要使用一张矩形网格, 我们把它称之为 “矩阵” (matrix), 就像是由空白方格组成的棋盘. 让我们取一段比前面稍长一点的信文作为例子:

MEET ME THURSDAY NIGHT

(周四晚见我)

这段信文有 19 个字母. 同前面一样, 我们要加上足够的 “空” (这次只需加一个), 使之成为 4 的倍数. 因为有 20 个字母正好可使用一个 4×5 矩阵. 末尾带有哑字母 X 的这段信文写在这 20 个空格中, 按从左到右、从上到下的顺序:

M	E	E	T	M
E	T	H	U	R
S	D	A	Y	N
I	G	H	T	X

下一步是要沿着一条特定的路线走遍整个矩阵, 该路线的形状是所有要使用这种密码的人在事前商定的. 如果选定的路线是沿着第一行开始, 从左到右地水平行进, 这显然不好, 因为得到的密文就会以 MEET 起头, 很容易被认出是一个单词, 从而提供了破解您的密码体系的线索. 有一种好的路线, 称为 “犁路” (plow path), 因为农民犁地时就是走这样的路, 本例中的犁路如下图