错乱的文字

密码中的秘密

PASSWORD

破译密码术

张景山 杨子涵 杨旭刚 编著

黑龙江科学技术出版社

错乱的文字

密码中的秘密

PASSWORD

破译密码术

黑龙江科学技术出版社

图书在版编目(CIP)数据

错乱的文字：密码中的秘密/张景山，杨子涵，杨旭刚编著.—哈尔滨：黑龙江科学技术出版社，2011.5
ISBN 978-7-5388-6630-8

Ⅰ. ①错… Ⅱ. ①张… ②杨… 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 081906 号

责任编辑 刘 野
封面设计 刘 洋

错乱的文字
密码中的秘密
CUOLUAN DE WENZI
MIMA ZHONG DE MIMI
张景山 杨子涵 杨旭刚 编著

出 版 黑龙江科学技术出版社
地址：哈尔滨市南岗区建设街 41 号 邮编：150001
电话：0451-53642106 传真：0451-53642143(发行部)
发 行 全国新华书店
印 刷 三河市明华装订厂
开 本 700×940 1/16
印 张 17
版 次 2011 年 5 月第 1 版 • 2011 年 5 月第 1 次印刷
书 号 ISBN 978-7-5388-6630-8/Z • 825
定 价 26.00 元

序言

人多少都有些喜爱打探别人私事的天性，有的甚至发展成不遗余力地去窥探他人隐私的嗜好；另一方面，为了求得自保，人们又都有保留隐秘私事的需要，在特定的条件下，这已成为生存的要件之一。探密和反探密运用到政治、军事、商业等领域，就发展为一种特殊的技能——密码术。

密码术的历史几乎和文明的历史一样悠久。自从人们觉得有些东西应当保密以后，人类便发明并使用了密码。翻开数千年的人类文明史，不管是在的宏大巍峨的宫闱大内、静寂幽暗的教堂，还是在喧嚣嘈杂的闹市、硝烟弥漫的战场，甚至在千年古册的缝隙中、平民百姓的闺阁内，都有密码的影子在浮现和隐没。在这些诡秘莫测的字符背后，或是隐含着政客那冷酷阴毒的计谋、武士那阴森滴血的剑影，或是携带着智者狡黠的微笑、情人绵绵不绝的秋波……

可以说，密码是当一种文化在文学、科学和语言发达到一定的复杂程度，当秘密的、符号性的信息交流达到不可或缺的阶段应运而生的一种信息交流的特殊工具。

有宝藏的藏匿者，就有宝藏的探寻者。密码学的发展史，就是一部密码

的编码者和破译者相互逞强斗胜的历史。

最初，这些密码不过是对文字的简单操作。如古希腊人的“天书读法”、恺撒的“字母替换”等。公元476年，西罗马帝国灭亡，欧洲的密码学陷入了长达千年的衰落时期，而此时的阿拉伯世界却处于对密码追求的狂热期。阿拉伯人对密码学的最伟大的贡献是发明了频率分析法。他们从《古兰经》的研究中受到启发，找出了破译“替换密码”的关键——密码中最常出现的字母，也就是正常文本中最常出现的字母。

直到文艺复兴时期，密码学才在欧洲重放异彩。1466年，意大利建筑师莱昂·阿尔伯第发明了一种可以旋转的密码索引系统，使字母组合可以随意变化，实现了由过去的单字母替换向多字母替换的伟大跨越。阿尔伯第系统也成为现代密码系统的基础。

到了16世纪，有些密码已变得繁复无比，几乎到了无法破译的地步。1586年，法国外交家布雷·德·维热纳尔改进了阿尔伯第系统，发明了一种用26个字母形成的网络进行编码和解码的系统。这种密码极难破译，在当时曾号称是“不可破译的密码”。

然而，挂在密码编码者脸上的笑容没能持续长久。到了18世纪，维热纳尔密码这座看似无法攀越的高山被天才的英国数学家、现代计算机之父查尔斯·巴比奇踩在了脚下。

20世纪的两次世界大战，对密码使用的需求急剧增加，从而极大地促进了密码术的发展，密码的编制进入了机械化时代。第二次世界大战中，德军使用了当时世界上最难破译的密码机——英纳格码密码机，迫使盟军投入巨大的人力物力来建造巨型的密码破译机器——“炸弹”（因其工作时“滴滴”作响而得名），进而促进了日后现代电子计算机的问世。

今天，密码技术进入计算机时代。那些铺天盖地的神秘信息和不着头绪的变化形式已非人工所能对付得了的。那些使用性能先进的计算机试图进入别人“宝库”的人被称为“黑客”。不过，目前还是密码编写者技高一筹。我们所处的时代每天都在使用真正难以破译的密码。或许，今后人们期待的

光子计算机和生物计算机出现了，密码学的历史又要续写新的篇章。

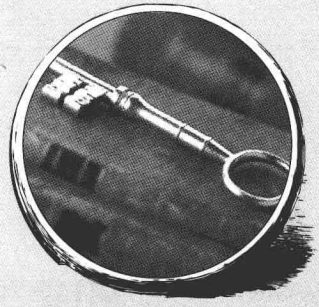
本书不是着眼于密码学的历史，而是以轻松的语言、详尽的步骤向大家介绍一些简便有趣的密码的编写、解读及破译的方法，使对密码感兴趣的朋友从中获得乐趣，也使大脑得到逻辑的“按摩”。

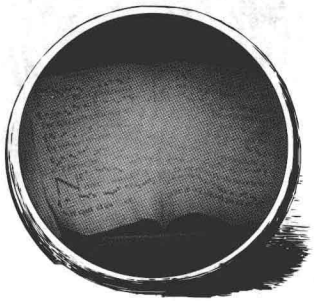
另外，本书还为人们在实际生活中使用密码提供了必要的提示和可行的方案，使大家在给自己的信息加密时，能够更安全、更实用。

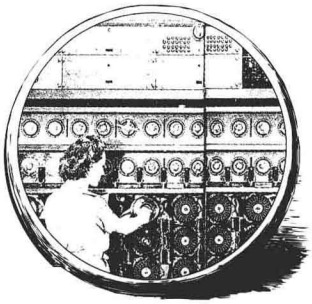
杨旭刚

2007年9月

目录







形形色色的简便的密码术

一 “瞒天过海”的隐文术

目前我们所知道的最早的密码是公元前1900年刻在埃及岩石上的密码。其实，这是一些特殊的符号，是通常象形文字的变体，描述了伽南·候特伯二世的故事。之所以使用难以辨认的变体字，并不是隐瞒什么，而是为了使后人在阅读时产生一种神秘感和崇敬的心理。

随着埃及文化的兴盛，随着书写文字的发展和贵族陵墓的增加，那些铭文的变形逐渐趋于更复杂、更巧妙、更普遍。这些虫书鸟迹不仅具有了密码学的一些要素——秘密性，也使其增加了令人敬畏的神秘色彩。

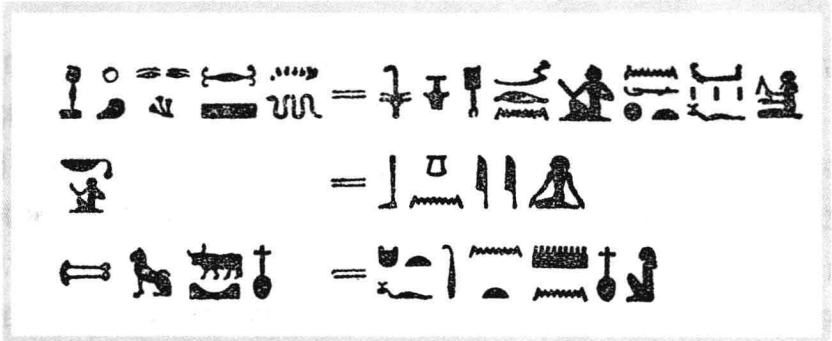
在我国，“密码”作为一个名词出现，最早见于明朝蒋一葵所著的《尧山堂外纪》一书中。过去，密码也称为“暗号”。

最早对密文作出一些说明的人可追溯到古希腊时的希罗多德。这位古希腊著名历史学家以编年史的形式记载了公元前5世纪希腊和波斯之间的战争。根据他的记载，古希腊人运用自己的智慧，以加密的方法传递信息，从而使希腊免遭被波斯君主薛西斯征服的厄运。

当时，希腊和强大的波斯之间长期的矛盾已到了动武的地步。不屈的希腊人拒绝向波斯进贡，从而激怒了薛西斯，他决定要给这个桀傲的小国一点颜色看看。薛西斯花了5年的时间秘密建立起一支强大的军事力量，打算出其不意地给对方以致命的打击。

谁知，波斯人的部署和装备被一位住在波斯的希腊人德马拉图斯探听到了，他决定要将这一重要信息告诉自己的祖国。可问题是波斯人把守很严，怎么将情报送出去呢？希罗多德在史书中写道：聪明的德马拉图斯终于想出了一个办法，就是利用一块已上蜡的可折叠的写字板，先将蜡刮去，再将薛西斯的意图刻在写字板的背面，然后再涂上蜡盖住字迹。这

样，写字板看上去并没有写任何字，一路上就不会被波斯人发现。当写字板通过波斯人的层层盘查到达目的地后，希腊人开始积极备战，并于公元前480年在撒拉米斯海湾，给远征的波斯人以迎头痛击。仅一天工夫，强大的波斯军队便被击败了。



姓名和头衔的象形文字加密
左方是密码象形文字，右方是相应的明文象形文字。

就这样，一条密文拯救了希腊人。

那位可敬的爱国者德马拉图斯的这种秘密通讯方法就在于简单地将情报隐藏起来。希罗多德还给后人讲述了另一个例子。希腊领主塔亚乌斯，把一个奴隶的头发剃光，用墨汁在他的头皮上写下一段文字，意思是号召人们反抗波斯国王。等这个奴隶的头发重新长出来后，派他混进波斯人侵占的希腊城市。领主的指示得以到处传播，结果该城爆发了反波斯人的起义。等待头发长出是要花费较长时间的，显然这个办法不能用于传送急件。.

我国古代也有类似传送密文的例子。相传北宋时期，辽国派遣王钦若打入宋朝内部，在朝廷做官竟做到“枢密使”（中国古代官名，原先主要掌管接受朝臣以及四方表奏并宣达帝命，后来逐渐参与国家要务，位同宰相，专掌军政。）的高官。有一次，辽国有一封密信要送给王钦若，但是一路盘查严密，怎么送到呢？最后他们竟想出了一个残忍的办法。先将密信放入蜡丸

中，然后用刀划开送信人的大腿，把蜡丸塞进皮肉里，给他敷上药，等刀口长好后，再派进宋朝。就这样，密信最后送到了王钦若手中。然而，这种残害肉体的办法不仅不能送达急件，也太过于残酷。

通过把信息隐藏起来的秘密通讯方式称为“隐文术”。在希罗多德之后的2000多年时间里，更多的隐文术相继出现，可以说是千奇百怪、变化万千。

古代中国人把密件写在精美的丝绸上，再把丝绸塞进一个有蜡密封的小球内，让信使吞下蜡丸。另外，我国古代也早有以藏头诗、藏尾诗、漏格诗以及绘画等形式的隐文，将要表达的意思和“密语”隐藏在诗文或画卷中的特定位置，一般人只注意诗或画的表面意境，而不会去注意或破解隐藏其中的密语。

在15世纪，意大利科学家波尔塔记载过一种把信件隐藏在熟鸡蛋内的方法：用1盎司（约28.3克）的明矾和1品脱（约0.57升）的醋混合而成的特殊墨水把文字写在蛋壳上，墨水穿透多孔的外壳，不在表面留下任何痕迹，却留在凝固的蛋白上，剥开蛋壳后就能看到信息。

隐文术中最老和最重要的方法要算隐形墨水（也叫“密写墨水”）了。关于隐形墨水始于何时，已难以考证。早在公元前1世纪的时候，罗马博物学家普林尼就讲到过，一种叫 thithymallus的植物的汁液可以被用做密写墨水。这种汁液干了之后变得透明，用微火加热后，透明的汁液又变成棕色。许多有机物如醋、果汁等制作的液体都有类似的隐形特点，因为这些有机物质经文火加热后立即碳化，从而使字迹显影。许多现代间谍在专用密写药水用光后，情急之下也会用他们自己的尿液替代隐形墨水，利用的是相同的原理。另外，许多常用的药品，像阿司匹林、氨基比林等都可以用来作为隐形墨水。

有关隐形墨水的事例很多，我们就来讲一些典型的。

牛奶墨水 牛奶写在纸上没有颜色，收信人用火一烤，字迹就会清晰地显露出来。这是因为牛奶中含有蛋白质，蛋白质受热后会发生凝固，颜色就发

生了变化，字迹也就显露了出来。

清水墨水 清水写在纸上，干后什么也看不见，但是纸在被浸湿的地方发生了微小的变化。把这种纸用碘蒸汽一熏，密写的字迹就会显现出来。原因是纸张被水浸湿的地方变得蓬松和粗糙，极微小的碘颗粒会吸附在这里，碘受热变了颜色，字迹就出来了。

五倍子墨水 五倍子是一种可以在中药店里买到的药材，其中含有丰富的鞣酸，鞣酸溶液是透明的，用它的溶液做墨水写在纸上是没有字迹的。但它遇到铁盐化合物，就会变成清晰的字迹。这种密写方法长期用于密信的书写。时至今日，鞣酸铁一直是制造钢笔墨水的基本原料。

火柴墨水 有一种特殊的火柴，火柴头溶到水里就是隐形墨水，火柴棍就是用来密写的笔。这种密写的字迹一干，字迹就会消失，用紫外线照射时，字迹又会重现。

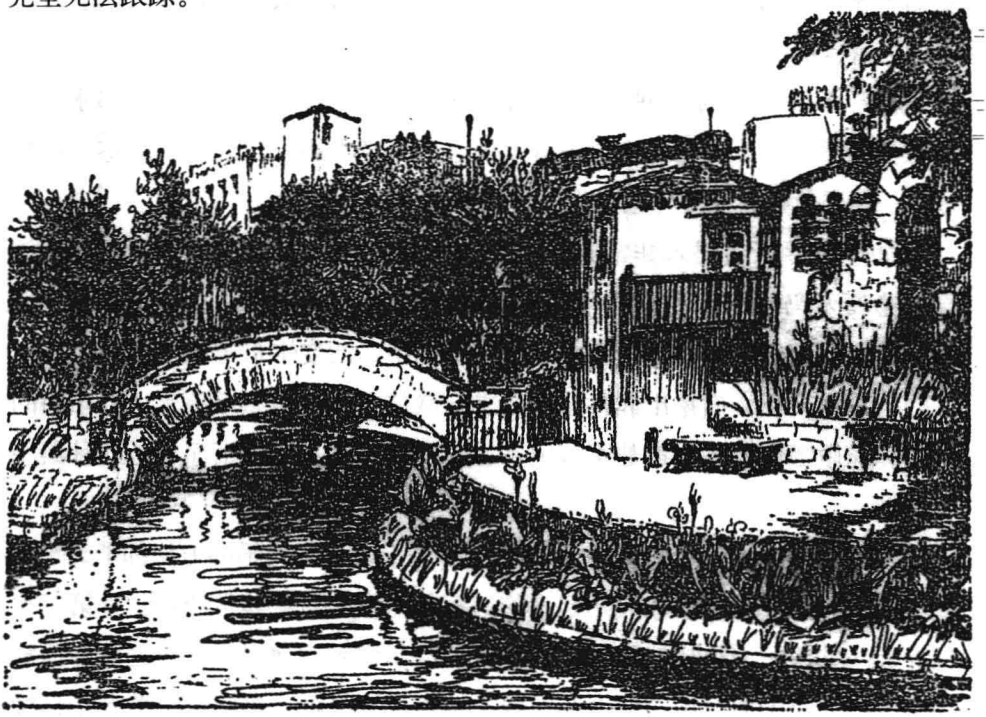
放射性墨水 这是一种专门对付化学检测的墨水。用笔蘸着这种墨水把情报写在衣服上后，用化学方法很难发现。如果把衣服和包着黑纸的感光胶片放在一起，射线会使胶片感光成像，在上面显现出字迹。

如今，尽管密码术非常先进，更加难以破译，但不被敌方发现秘密信息，隐写术仍是保密的首选措施，因而采用技术隐写术的方法还很多。比如：将信息隐藏在信使的鞋底或妇女的耳饰中，改变字母笔画的高度或在正文的字母上（下）面挖出非常小的洞来隐藏信息等。而隐写墨水、纸币中的水印和缩微图像技术也都是军事中常用的信息隐藏方法。下面就是几种典型的案例。

隐藏在乐曲中的“魔声” 历史上许多信息隐藏和传输的方法都是为了满足情报战的需要而发展和成熟起来的，有些信息的隐藏非常巧妙。如第二次世界大战期间，一位热情的女钢琴家常为盟军作慰问演出，并通过电台播放自己谱写的钢琴曲。由于盟军在战场上接连遭到失败，反间谍机关开始怀疑到这位女钢琴家，可一时又因找不到钢琴家传递情报的手段和途径而迟迟不能决断。原来，这位德国忠实的女间谍，每当从盟军军官那里获得军事情报

后，就按照事先规定的密码巧妙地将其编成乐谱，并在电台演奏时一次次公开将重要情报通过悠扬的琴声传递出去。

德国的一家电台在每晚播出新闻后，总要发出一些莫名其妙的信号，其速度之快使人以为是某种试验信号。有一天，在一艘英国军舰的军官餐厅里，一位军官在唱机上放上一张特殊的唱片，即那家德国电台播放的莫名其妙的滑稽声。由于这位军官多喝了几杯，他在放该唱片时，竟忘了给留声机上发条，结果唱片发出的不再是莫名其妙、毫无意义的无线电信号，而是一连串周密排列的密码。事后查阅这些密码记录发现，这是德国统帅部发给指挥德国驻东非部队将军的电报。它是以极高的速度拍发的，使对方不能破译。此法后来还用在第二次世界大战中，只不过速度更快，使一般的窃听站完全无法跟踪。



一张隐藏着密信的风景画

（画面是一条小河，玄机就隐藏在岸边的绿草中。画中沿河岸的短草叶代表莫尔斯电码的“点”，长草叶代表“线”，拼出文字为：Compliments of CPSA MA to our chief Col Harold R.Shaw on his visit to Antonio May 11th 1945）

显微镜里传递情报 第二次世界大战期间，德国情报机关还曾利用微缩原理和照相方法，将秘密文件、资料情报缩小至数十或数百乃至数千分之一，制成很薄的显微点膜片，然后再把它们“埋藏”在书报杂志中某个字及标点符号上，或是将超微膜片藏在邮票、信封内进入邮路传递。对方收到后，按照双方约定好的位置和标记，通过技术手段再重新将显微点还原成像。

保密粉末、保密涂料 将一种特殊粉末撒在保密文件上，可防止拍照、复印，一旦被拍照或复印，文字会立即消失或变黑，还可在规定的保密时间期满后使文字自动消失。法国发明一种专门用于珍贵艺术品和名画的涂料，这种涂料对艺术珍品不产生任何伤害，但对警犬的嗅觉却有极强的刺激作用，能使警犬在150米以外的地方准确嗅出。这样，在艺术品失窃后警犬更容易跟踪追击，即使艺术品密封于汽车中、仓库的货物堆中，也能被其嗅出。

网络与数字幽灵 现代信息隐藏技术的研究建立在信息理论、统计理论、认识心理学和现代信息技术手段的基础之上。而现代电子加密技术和数字技术的发展，又为信息隐藏提供了更为先进、高效的技术手段。数字信息隐藏的最大特征，就是由公开信息作掩护，第三方很难感觉到秘密信息的存在。计算机网络的出现和广泛使用是信息技术发展的一个突破性成就。而一些情报机构、恐怖组织或犯罪集团正是利用这一渠道，将秘密信息经过加密技术处理后，通过电子邮件、数字文件或图表在网上公然传输，犹如若隐若现的“幽灵”，很难跟踪、截获和破解。

“密写”和“微缩”技术变迁 激光技术和水印技术用于“密写”后，使信息隐藏更为隐蔽。利用微缩技术，可以在厚度仅1.0微米、面积仅1平方毫米的显微点上，制作几百甚至上千字的信息。倘若把经过技术处理的显微点隐藏在一本厚厚的书中、一株植物的根、叶或一只动物的皮毛里，要想发现它，真如同大海捞针一样难。

“量子”技术隐形传递信息 在科幻电影或神话小说中，常常有这样的场面：某人突然在某地消失掉，而后却在别的地方莫名其妙地显现出来。这种

来无影去无踪的过程，从物理学角度可以想像或解释为隐形传递的过程。量子隐形信息传递是发送者利用量子的独特功能，对所提取的信息运用量子技术突破经典信息系统的极限，超水平进行信息传递，这便是量子力学和信息科学相结合的重要产物。因此，截获隐藏信息的过程，也是信息的处理与控制能力不断提高的过程，从而在一定意义上促进了加密与解密技术的发展。

信息隐藏技术将是未来信息对抗的焦点之一，是敌对双方借以获取和破解信息的制高点，因此备受各国关注。

隐文术确实能起到一定的保密作用，不过一旦密信被发现，其中的内容就立即会暴露无遗。可见仅靠隐文术保密是远远不够的，于是另一种传递密信的方法也在发展，那就是密码术。

密码术的目的不是隐藏密信本身，而是要隐藏它的内容，即通过给信息加密，即使密信被截获，对方也很难明白密信的真实含义。

历史上曾经出现过各种各样的隐藏密信真实含义的方法，我们不妨将它们看作是现代密码术的雏形。下面我们就来回顾一下这些或许已经不被人们使用的各种“密码术”。

二 阴符

我国古代有一位著名的人物名叫姜子牙，也叫吕尚、太公望。人们常说的“姜太公钓鱼——愿者上钩”，说的就是他。姜子牙非常有才能，他帮助周武王灭掉了商纣王，建立了统一的王朝——周朝，因此不愧为中国古代的大政治家、大军事家。从目前的记载来看，他还最早制定了军队秘密通讯密码——阴符。