Code Breaking

密码的故事

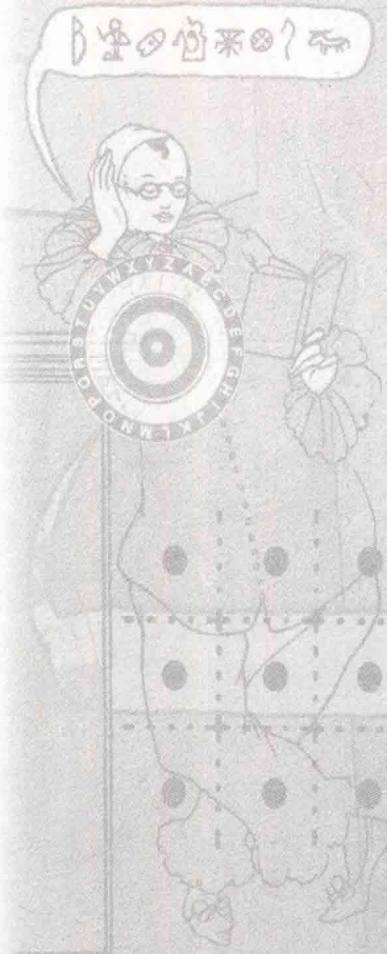
【韩】朴英秀 著

何元元 译

湖南科学技术出版社

密码的故事

【韩】朴英秀 著
何元元 译



湖南科学技术出版社

密码故事 ISBN: 9788991239326 by 朴英秀
The Original Korean edition © 2006 published by BOOKROAD Publishing Co.
The Simplified Chinese Language Translation © 200x Hunan Science & Technology Press by Arrangement with BOOKROAD Publishing Co. Seoul, Korea through EntersKorea Co.,Ltd.
All rights reserved.

湖南科学技术出版社通过韩国恩特思版权代理公司独家获得本书中文简体字版中国大陆地区出版发行权
著作权合同登记号：18-2009-129
版权所有，侵权必究

图书在版编目（CIP）数据

密码的故事 /（韩）朴英秀著；何元元译. -- 长沙：湖南科学技术出版社，2010.7
ISBN 978-7-5357-6311-2
Ⅰ. ①密… Ⅱ. ①朴… ②何… Ⅲ. ①密码－普及读物 Ⅳ. ①TN918.1-49
中国版本图书馆 CIP 数据核字(2010)第 133204 号

密码的故事

著　　者：[韩]朴英秀
译　　者：何元元
责任编辑：戴　涛
出版发行：湖南科学技术出版社
社　　址：长沙市湘雅路 276 号
　　http://www.hnstp.com
邮购联系：本社直销科　0731-84375808
印　　刷：长沙化勘印刷有限公司
　　（印装质量问题请直接与本厂联系）
厂　　址：长沙市青园路 4 号
邮　　编：410004
出版日期：2010 年 8 月第 1 版第 1 次
开　　本：710mm×1000mm　1/16
印　　张：14
字　　数：196000
书　　号：ISBN 978-7-5357-6311-2
定　　价：25.00 元
（版权所有 · 翻印必究）

前　言

不能读的文字——密码的重新发现

文字的发明在人类历史上称得上是一个划时代的创举，它不仅让古人可以通过文字进行记录，还令知识的传播成为可能。文字不仅是区分史前时代和历史时代的界线，更是连接一个国家、一个民族的纽带。对于个人而言，文字作为语言的游戏使人娱乐其中。除此之外，文字还具备另外一种特殊的功能，那就是人们可以利用文字“记录秘密”。通过充分利用文字的奥妙，即利用“密码”的方式来记录特殊事件，使得事件在暴露的情况下也能令秘密信息得到很好的保全。

在宗教领袖作为统治者的时代，统治阶级为了营造神秘感开始使用密码，后来密码作为提高军事作战效率的手段得到了积极的研发。有些民族为了向后代炫耀先祖的历史，以难以理解的文字记录先祖的辉煌。其中至今仍在繁衍生息的民族，他们的后代通过这些密码找到了先祖的踪迹；而那些如今已经湮灭的民族，他们利用密码所记录下来的历史则连同他们语言一起被带进了坟墓。

这本书在研究密码的同时，把古代文字也纳入到共同研究的范畴，因为笔者认为无法阅读的文字等同于密码。时至今日，还有许许多多的古代文字正处于被解读的过程当中，正是因为有了考古学者的不懈努力，一个又一个的神秘事件才得以浮出水面。事实上，古代文字和谜语一样非常难解，所以细心留意考古学者解读古代文字的过程，从中也可以学到不少破

译密码的方法。

放眼近代历史，密码同样发挥了极为重要的作用。因为很多情况下泄露了密码就等于暴露了自己的私生活。举个例子来说，《红与黑》的作者司汤达在年轻时就因为脱发成了光头，但他并没有因此对自己的外貌丧失信心，并且为了吸引女人而作了大量的研究。生活中的司汤达风流成性，每当他写日记的时候，为防止泄密，他总是习惯性地把每个女人的名字用 V·A·M·C·G 等密码文字来记录。还有因为撰写《性报告书》而名声大振的阿尔弗莱德·金赛（Alfred Charles Kinsey，1894～1956）博士在与助手交谈时也会使用暗语，例如“新的实验对象比起 Cm 更喜欢 Z，另外对于 Cx 的 Go 会很 er”。这句话的实际意思是“新的实验对象比起与伴侣性交更喜欢兽交，还有他在与伴侣以外的其他人性交时表现得十分兴奋”。他们在谈论这些秘密话题时，使用了如同元素周期表般令人难解的词语。

现代社会人们对于身份的确认已经从“脸庞”进化到了“密码”，这令密码的作用更加不容小觑。随着通讯的发达，密码的重要性与日俱增，破译密码也陡然成为了一件极为重要的事情。在密码解读领域，把解密过程统称为“magic（魔力）”。美国政府的高级官员正是通过阅读这些魔力情报，然后在会议上讨论，最终以此为基础制定出新的国家政策。举个例子，由麦克阿瑟将军担任司令官的远东美国陆军司令部之所以能够成立，正是缘于 1941 年初美国所窃听到的一条秘密情报。这条情报透露出德国企图煽动日本攻击英国在亚洲的殖民地，进而把美国也卷入战争的秘密计划。美国为了应对德国的这个计划，成立了远东军司令部。

破译密码绝不是一件容易的事情，在不知道密码编写原则的情况下很难把握密码所要传达的真实内容。下面就让我们来了解一下密码的几种基本形式。最简单的密码方式应该算是通过变换文字顺序来隐藏原文信息的“转字密码”。比如说你想表达“现在上司生气了”这个意思，为了隐藏原句中的信息，可以把它改写为“在现司上了气生”。当然一般来说，密码编写人和阅读人之间通常会就密码的编写原则事先进行约定。

“文字交换”也是一种很常见的密码形式。在保证叙述顺序不变的情

此为试读，需要完整PDF请访问：www.ertongbook.com

况下，将关键词语替换为另外的事物。利用这种方法，“现在上司生气了”这句话可以改写为“现在长白山在喷火”。

“乘积密码”则是更为先进的密码方式，它是由转字密码和文字交换密码联袂表现的一种密码形式。乘积密码首先将原文中的关键信息替换为其他的事物，然后再将这些指代特殊信息的词语重新加以排列组合，形成一条具有双保险的密码。这种密码因为破译难度大，应用范围十分广泛。

最难解的密码要数“外语密码”。它是在前面介绍的密码编写原则的基础上再应用外语，其破译难度也随之更上一层楼。遇到外语密码时，密码解读者需要拥有与密码专家相差无几的智力水平，因为原文只是一些音节的简单罗列，你需要找出这些音节所对应的真实意思。

不添加任何标点符号在某种程度上也会增加破译密码的难度。但即便如此，密码仍旧在不断地被破解，同时又以更为难解的姿态重新出现。笔者希望读者们能通过本书了解到一些密码的基础知识，如果它还能为开启人类的不解之谜提供一些思路的话，那就再好不过了。

朴英秀

2006 年 5 月

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

1

“顺利产子！”

1945 年 7 月 16 日，美国总统杜鲁门收到这则短消息后兴奋不已，并迅速将这则消息告诉英国首相丘吉尔。到底是谁生下了怎样的孩子会让杜鲁门如此高兴呢？

2

“我与目标在街上碰面并打招呼，一切顺利！”

1975 年 10 月 8 日，苏联谍报部门收到这则由斯塔申斯基发回的电报，欣喜异常，这则电报的内容到底指的是什么呢？

1. 密码的历史和由来

最早破解敌国密码的女人

密码起源于埃及尼罗河边的一个小村子，大约4000年前，一位作家为了记录下统治者的生平在石板上刻下了象形文字，这就是密码的起源。那时这位作家为了在语句中表现出危险和暴力，使用了“转字”这种密码方式，从而把真实的文字内容隐藏起来。

另外，在埃及的宗教著述当中，为了增加其神秘性，也往往会通过“转字”用隐喻的方式来表达文字的意思。在印度性典《迦摩须多罗》中也有利用“转字”来表述的部分。在希罗多德撰写的《历史》一书中有关于密码的具体描述，书中提到波斯出征希腊计划的密文是用铅制成的秘匿文，而破解这封密文的正是斯巴达名将利奥尼达斯的妻子歌果（Gorgo）。对于那时的具体情形，希罗多德是这样描述的：

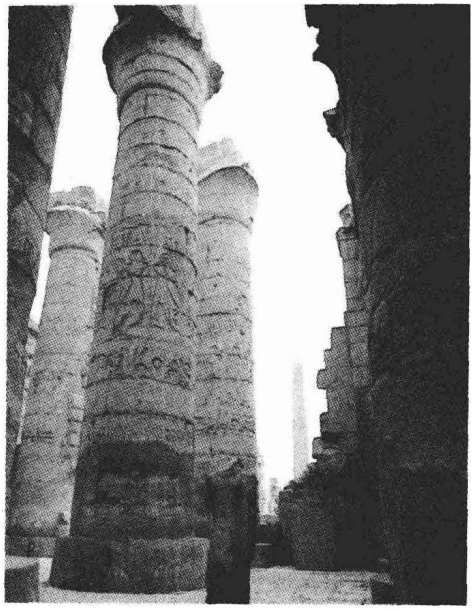
> 在希腊城邦中，最先知道波斯国王企图侵略希腊的是斯巴达。而斯巴达获知这则情报的途径更是令人匪夷所思。流亡到波斯的阿里斯顿（Ariston）的儿子狄马拉图斯（Demaratos）认为波斯似乎对斯巴达人心存歹意。那么波斯到底是斯巴达人的朋友还是敌人呢？

最终，当薛西斯决定远征希腊的时候，狄马拉图斯决定要想尽办法将这个消息告知斯巴达。可万一事情败露怎么办，再说要如何传递这个消息呢？必须想出一个两全其美的办法。狄马拉图斯最终找到一个双层的书版，去掉蜜蜡，在书版的木头上刻上了波斯国王的企图，之后又在上面涂上蜜蜡，将文字掩盖住。这样一来，即使在运送途中受到卫兵的盘查也绝不会露出马脚。

虽然书版被安然无恙地送抵了斯巴达，但起初斯巴达人并没能破解这个秘密。正在他们一筹莫展的时候，克列欧美涅斯（Cleomenes）的女儿，也就

是利奥尼达斯的妻子歌果揭穿了书版的谜底。她告诉人们去掉书版上的蜜蜡，那样就可以看到刻在木板上的文字。人们按照她的说法去做，果然书版上的文字显露无遗。当斯巴达人了解到书版上的信息之后，又迅速告知了希腊其他城邦。

这是发生在公元前 480 年的一个故事，当利奥尼达斯了解了书版上的内容之后，就前往塞莫皮莱山谷等候波斯国王薛西斯的讨伐大军，这里正是波斯征讨希腊的必经之路。利奥尼达斯在此与波斯苦战两天两夜，最后命令主力军队撤退，自己率领 300 名卫兵血拼到最后，战死沙场。希腊人民深受鼓舞，“斯巴达人是不可战胜的”这一说法也自此流传开来。



▲ 埃及的象形文字——阿门神殿的柱子上镌刻着新王国时期的象形文字

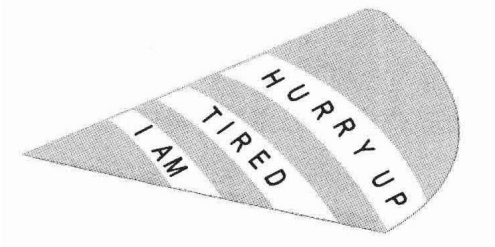
另外，歌果也可以称得上是世界上破译密码的第一人。为什么这样说呢？虽然歌果只是发现了隐藏在蜜蜡下面的秘密，但所谓密码，不仅仅指语言方式的改变，所有隐藏原有信息的现象都可以称为密码。

最早的密码工具

世界上最早的密码工具出现在公元前 400 年左右，被用于古希腊军队将领之间的秘密通信。那时，每当需要从城邦国家向其他地方派遣将领的时候，都会制作两条长和粗相同的锥形木棒。一条留在本部，另一条交由被派遣的将领保管。

这种被称为 Scytak 的工具的具体用法，就是将记载了情报信息的羊皮

纸螺旋式缠绕在锥形木棒上，从而显示出它的真实内容。羊皮纸又细又长，像磁带一样，如果是一条这样单独的羊皮纸，你根本无法理解上面显示的文字信息，但如果将羊皮纸螺旋式缠绕在形状相同的木棒上，就可以呈现出它要表达的具体内容。换句话说，你无法理解羊皮纸上纵向排列的文字信息，但如果将它们横向缠绕在木棒上，文字意思就可以一目了然。由于这种木棒被称为 Scytak，因此这种密码方式被称为 Scytak 密码，它也许就是通过改变单词顺序来隐藏真实意义的转字密码的始祖。



▲ Scytak——卷成圆筒形即可阅读密文

Scytak 在公元前 450 年左右还被用作打入敌人内部的间谍人员的密报工具。那时斯巴达与波斯结为同盟国，正与雅典展开激战。斯巴达的雷桑德将军觉察到波斯正对自己虎视眈眈。但没有确切的证据，如果判断失误贸然对波斯发起攻击就会失掉这个宝贵的同盟国。

最终雷桑德将军向波斯派出了自己的间谍，那位谍报人员在掌握了具体情况之后就利用 Scytak 制成密报，藏在一个奴隶的腰带里传递给了将军。雷桑德将军在拿到密报后，立刻将它缠绕在木棒上，文字内容显示出来了："波斯杀害了将军最好的朋友，正伺机对将军发起进攻。"至此一切都真相大白了。

雷桑德将军立刻对波斯发起进攻。其实波斯是为了一雪 30 年的前耻，假意与斯巴达交好，而这次又是因为疏于对军事机密的管理，再次饱尝了战败的苦果。斯巴达正是凭借密码工具 Scytak 再次获得了胜利。

除此之外，希腊城邦国家还通过"点"的数量使文字信息密码化，或者是在书或其他文件的文字上、下方打上点，传达密码信息。直到第二次世界大战爆发后，德国间谍又将这种"点密码"重新整理并加以使用。

直到 14 世纪末，欧洲各国在外交通信上使用了一种密码工具——密码盘。这种密码工具由可以旋转的两个同心圆组成，每个同心圆上都刻有 26

此为试读，需要完整PDF请访问：www.ertongbook.com