

大奖
15000美元
挑战智力极限

密码故事

人类智力的另类较量

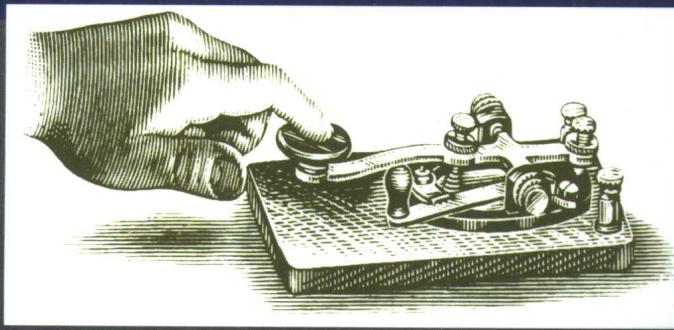
读懂本书，并将所附10道
密码按其规则破译，即可获得
15000美元巨奖。

THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY

〔英〕西蒙·辛格 著

朱小篷 林金钟 译

THE
CODE
BOOK



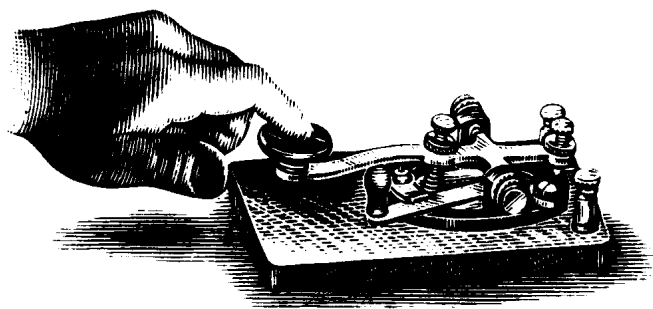
海南出版社

密码故事

人类智力的另类较量

〔英〕西蒙·辛格 著

朱小篷 林金钟 译



海南出版社

图书在版编目(CIP)数据

密码故事/(英)辛格(Singh, S.)著;朱小蓬译.

——海口:海南出版社,2001.9

书名原文:THE CODE BOOK

ISBN 7-5443-0218-0

I. 密… II. ①辛… ②朱… III. 密码-基本知识 IV. TN918.1

中国版本图书馆 CIP 数据核字(2001)第 062684 号

Copyright: 1999 by SIMON SINGH

This Edition Arranged With

CONVILLE & WALSH LIMITED

Through Big Apple Tuttle - Mori Agency, Inc., and

Beijing International Rights Agency

Simplified Chinese Edition Copyright:

2001 HAINAN PUBLISHING HOUSE

All Rights Reserved.

版权合同登记号:图字 30-2001-69 号

密码故事

(英)西蒙·辛格 著

朱小蓬 林金钟 译

责任编辑 野夫 莫竹岑

※

海南出版社出版发行

(570216 海口市金盘开发区建设三横路 2 号)

全国新华书店经销

北京市通州运河印刷厂印刷

2001 年 10 月第 1 版 2001 年 10 月第 1 次印刷

开本:850×1168 毫米 1/32 印张:11.75

字数:218 千字

书号:ISBN 7-5443-0218-0/N·1

定价:20.00 元

前 言

几千年来,无论是国王、女王还是将军,在管理国家或指挥军队中一直离不开一个高效的通讯系统。同时他们都明白,假如他们的信息落入对手的手中,也就等于将珍贵的机密泄露给了敌国。至关重要的情报被敌军掌握,那将会导致什么后果?正是由于这种情报可能被敌方截获的威胁推动了密码或代码术的发展:一种伪装信息的技术,使得只有联络好的信息接收者才能够读懂它。

对密码的需求必然推动了国家建立密码编码机构,他们负责发明使用新的密码来保障通讯的安全。同时,敌方密码破解者正试图破解这些密码,窃取信息。密码破解者通常是语言学上的炼丹者,他们能神奇地把一堆无意义的符号魔术般地变成有意义的单词。几个世纪以来,密码编码者和密码破解者之间的斗争事实就形成了密码的历史。这是一场智力上的接力赛,并且对历史的发展方向往往有着戏剧性的影响。

写这本书有两个主要的目的:第一是讲述密码的演化过程。用演化这个词是恰到好处的,因为密码的发展可以被看成一种演化竞争。一个密码产生之后,便会经常遭受密码破解者的攻击。当密码破解者发展了一种新的武器能够揭示这个密码的弱点,那么这个密码就不再有用。它或者永远消失或者进化为一种更新更

强的密码。同样这个新密码也只能存活到密码破解者发现它的弱点为止,就这样发展下去。这与生物上的抗逆性相似。例如对于一株感染菌,这种细菌先在人体里繁衍生殖,但是一旦医生发现了某种针对它弱点的抗生素,它就无法遁形。这种细菌不得不演化直到能够抵抗抗生素为止。如果成功,它将又一次存活下去,也就是这样,细菌在抗生素的一轮轮攻击下不断地演化。

在密码编码者和密码破译者之间硝烟不断的战争中,一系列令人称谓的科学突破也应之而生。密码编码者一直努力构建一种至强的密码来保障通讯安全,而密码破解者则一直努力发明更有效的方法来攻击它们。在他们解密和保密的斗争中,双方都吸收了各种原理和技术,从数学到语言学,从信息论到量子论,范围很广。反过来,密码编码者和密码破解者又丰富了这些理论,他们的工作促进了技术发展,最值一提的是现代计算机的发明。

历史的道路上到处点缀着密码的踪迹。他们决定着战争的结果,甚至带给国王和女王毁灭性的后果。因此,我完全可以根据某些政治谋略的故事以及生与死的传说,来描述密码演化发展中的一些转折点。然而,密码的历史是丰富的,所以我不得不略过许多迷人的故事,这也表示我的说明不是完全的。对于你所喜爱的故事或你喜欢的密码破解者,如果你想了解得更多你可查阅相关读物,它能帮助一些读者更加详细地了解密码学。

在讨论完密码的演化以及它对历史的影响后,这本书的第二个目的是说明在今天密码是怎样的比以前更加重要。随着信息变成不断增值的商品,加上通讯革命改变着这个社会,给信息加密的过程在日常生活中将扮演一个越来越重要的角色。如今我们的电话要通过卫星,我们的电子邮件要通过不同的电脑,这两种通讯形式都很容易被拦截,这样就暴露了我们的隐私。同样的,越来越多的企业通过互联网运作,为了保护公司和他们的客户,防卫措施必须要放在重要的位置。加密是保护我们隐私和保证数字市场

成功的惟一方法。秘密通讯的技术或者叫密码编码术为信息时代提供了锁和钥匙。

10年来,警察和情报部门使用无线监听来搜集对付恐怖分子和犯罪集团的证据,但是近来密码术的发展直接影响到无线监听的效果。随着人类进入21世纪,人们急需密码编码的广泛使用来保护个人隐私。有同样要求的是商业公司,他们需要强大的密码编码术使得他们能在互联网时代保证业务的安全。可是同时一系列政策法规却限制密码编码术的使用。问题在于哪一个更重要——我们的隐私还是有效的政权?或者有没有一个折中的办法。

现在密码编码术对人类的有着巨大的影响,尤其值得一提的是军事密码编码术具有举足轻重的地位。有人说第一次世界大战是化学家的战争,因为芥子气和氯气第一次被用来作为战争武器;第二次世界大战是物理学家的战争,因为原子弹被派上了战场。同样我们可以说,如果有第三次世界大战的话,那将是数学家的战争,因为数学家将控制战争中下一个重要的武器——信息。现在由数学家负责发明新密码来保护军事信息。相应的,数学家也会站在破解这些密码的前沿。

在讲述密码的演化和对历史的影响时,我偏离了一下话题。在第五章我描述几种不同的古代文章的破译,包括B类楔形文字和埃及象形文。技术上,密码是与通讯相关,有意设计来保护己方的秘密,而古文明留下的笔迹并不是想用来保密的,问题仅仅是我们不能解释它。然而复原远古文章内容技术与密码破解术是非常相近的。约翰·查德威克曾写过一本书,描述了如何揭示一篇古地中海文章的原意。我对那些破译我们祖先留下的文字的人们所取得的智力成就感到震惊,他们使我们知道了我们祖先的文明、宗教和日常生活。

迫于需要,我在书中介绍了密码编码学中多种技术词汇。虽然我一般是按照它们的定义,但难免有时候我会使用一个技术上

并不准确的词汇,这也许对非专业人员来说更加容易接受。

在结束引言之前,我必须提及一个问题,这是每一个密码学方面的作家都要面对的,那就是加密科学很大程度上是一门秘密的科学。书中提到的许多英雄在他们的一生中都没有因他们的工作而得到认可,因为当他们的发明仍具有外交和军事价值时,他们的贡献是不能公开赞颂的。在本书完成过程中,我有幸与英国通讯总部(GCHQ)的专家进行了交谈,他们向我揭示了70年代研究过程的详细细节,这些现在已解密了。其结果是,世界上三位最伟大的密码编码师现在能够得到他们应有的荣誉。然而,这次披露却使我认识到还有许多我以及其他科学作家所不知的事情在进行。像英国通讯总部和美国国家安全局这样的组织在继续进行密码编码的研究,这意味着他们的突破仍需保密,他们本人也只能默默无闻。

尽管涉及到政府机密,我还是用本书最后一章来讨论密码的未来。这一章将试图发现我们是否能够预测在密码编码者和密码破解者之间革命性的斗争中谁胜谁负。密码编码者能够设计出一种真正无法破解的密码,成功满足他们绝对安全的需要吗?或者密码破解者能建造一台能够解密任何信息的机器吗?由于我们知道一些最伟大的头脑仍在秘密实验室工作,他们有足够的科研资金,因此我在最后一章的某些论断显然可能是不准确的。例如我提到虽然量子计算机具有破解今天所有密码的潜在可能,它应该还处在非常原始的阶段,但是可能已有人建造了一台。惟一可以指出我错误的人甚至没有理由来暴露自己的身份。

内容简介

自从人类开始会用笔书写，他们就开始用密码通讯了。密码并不仅仅与电报、军事或爱情相关，它已进入人类生活的很多层面：信用卡、保险柜、电脑等等。密码无处不在，同时又随时可能被破译。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，又是数学的神秘之美的比拼。在《密码故事》中，西蒙·辛格讲述了关于间谍、阴谋和聪明才智的精彩故事，从而揭示了密码学引人入胜的历史。

作者的叙述结合了可读性与耐人寻味的专业分析，十分新颖独特。



作者简介

西蒙·辛格在剑桥大学得到了物理学博士学位，曾在BBC做制片人。执导的纪录片《费马大定理》荣获了BAFTA(英国电影和电视艺术学院)大奖。同时他撰写了与纪录片同名的畅销书。

责任编辑：野 夫

莫竹芩

选题策划：任建成

封面设计：水 平

目 录

前言/1

第一章 玛丽女王的密码/1

密文的演化/4

阿拉伯密码破译师/14

破译一条密文/20

西方的文艺复兴/26

巴宾顿计划/32

第二章 不可破译的密码/45

从维热纳尔密码的冷落到铁面人/52

密室/59

巴比奇破解维热纳尔密码/63

从激情栏到埋藏的宝藏/78

第三章 加密的机械化/100

密码编码学上的圣杯/114

密码机的发展:从密码盘到恩格玛密码机/124

第四章 破解恩格玛/142

从不咯咯叫的鹅/160

截获密码簿/182

神秘的密码破译者/186

第五章 语言上的隔阂/191

破译失落的语言和古代的文字/202

B类楔形文字之谜/217

连接的音节/225

琐碎的枝节/231

第六章 艾丽丝和鲍勃的公开密钥/244

上帝青睐愚人/253

公共密钥密码术的诞生/269

质数猜想/273

公开密钥密码学的另一个历史/280

第七章 相当好的隐私/293

为大众加密吗？/303

齐默尔曼的复原/312

第八章 量子的飞跃/315

密码破译术的未来/316

量子密码术/330

附录 向密码挑战/349

第

一 玛丽女王的密码

章

1586年8月15日,星期六的早晨,玛丽女王被带到福斯灵海城堡的法庭上,那里已坐满了人。虽然几年的监狱生活加上风湿病的困扰已使她身心憔悴,但她仍保持着一份威严和镇定,显出不容置疑的皇家风范。在随身医师的陪同下,她沿着又长又窄的议会,经过法官、官员和观众席,来到正中的王座前。玛丽试图把王座想像成以一种尊敬的姿态对着她,但她却错了。这个空着的王位就象征着她的敌人而且是检举人——伊丽莎白女王。玛丽轻轻地走过王座,走向屋子的另一边——被告席:一个深红色的绒毛椅子。

苏格兰玛丽女王正因叛国罪被接受审判。她被指控密谋刺杀伊丽莎白女王并取而代之成为英国新女王。伊丽莎白的首席大臣弗朗西丝·沃尔辛厄姆已经逮捕了其他同谋者,逼供并处决了他们。现在,他正设法想证明玛丽是这次计划的核心人物,因而同样有罪,同样该受死刑。

沃尔辛厄姆知道在他能够处决玛丽之前,他必需使伊丽莎白女王信服玛丽确实有罪。虽然伊丽莎白鄙视玛丽,但她也有众多原因不愿看到玛丽被处以极刑。首先,玛丽是苏格兰的女王,许多人怀疑英国法庭是否有权处决一个国外政权的首领?其次,处决



图 1: 苏格兰的玛丽女王

了玛丽或许就形成一个使其不安的先例。如果本国政权有权杀死一个女王,那么叛军就会没有什么保留地杀死另一个女王,这可能就是伊丽莎白。再说,伊丽莎白和玛丽本是表亲,她们的血缘关系更加使得伊丽莎白难以定她死罪。一句话,只有沃尔辛厄姆能够

彻底地证明玛丽曾是刺杀计划中的一份子，伊丽莎白才能认同玛丽的死刑。

同谋者是一群年轻的贵族天主教徒，他们志在废黜新教徒伊丽莎白，而让同样是天主教徒的玛丽取代她。其实在法庭上已很明显地表露出玛丽是这些同谋者的幕后主使人，但玛丽是否真正批准过这个谋划却无从得知。事实上，玛丽确实签署过这个计划。摆在沃尔辛厄姆面前的一个挑战就是证明玛丽和其策划者之间这种触手可及的联系。

在她被审判的这天早上，玛丽身穿色调悲哀的黑色丝绒衣，独自一人坐在被告席上。对于叛国罪，被告人不允许有辩护律师，也不允许传叫证人。而对玛丽，甚至不允许其部下帮助她一同准备该案件。然而她的处境也不是毫无希望，因为她曾经也留有一手，就是确保每次和同谋者之间的通信都是用密码写成。密码把她的话变成看似没意义的一系列符号。玛丽相信即使沃尔辛厄姆拿到这些信，他也只能对信中字母的意思感到毫无头绪。如果信中的内容成为一个谜，那么这些信就不能作为对其不利的证据。然而，所有这些都建立在一个假定之上，就是这些密码不能被破解。

不幸的是，沃尔辛厄姆不仅仅是位首席大臣，他还是英国的间谍首脑。他已经截获了玛丽给策划者写的信。他也非常清楚谁能够解开这些密码。托马斯·菲利普斯是该国一流的密码破译专家。几年来，他一直在破解那些密谋推翻伊丽莎白女王的贵族之间传递的信息，从而为指控他们提供所需的证据。如果他能解开玛丽和共谋者之间的信，那么她的死刑将是不可避免的。而另一方面，如果玛丽的密码足够安全而掩盖了她的秘密，那么她或许还有一线生机。一条密码即决定着生死存亡，这在历史上已不是第一次。

密文的演化

最早对密文作出一些说明的人可追溯到希罗多德，罗马著名的政治家和哲学家西塞罗称他为“历史之父”，希罗多德以编年史的形式记载了公元前五世纪希腊和波斯之间的冲突，并认为这些冲突是自由和奴役之间的对抗，是保卫独立的希腊国和压迫统治他们的波斯人之间的对抗。根据希罗多德的记载，正是由一种叫密文的技术才使希腊免遭被波斯暴君也是王中之王薛西斯一世征服的厄运。

薛西斯开始选择在波斯波利斯上建一座城堡作为其王国的新首都，不久以后，希腊和波斯之间长期的矛盾达到了顶点。当时，波斯帝国上下及其众多邻国都送来了贡品和礼物，但雅典和斯巴达却一概不献。于是薛西斯决定要报复希腊对他的傲慢，开始调动了一支军队，声称“我们要把波斯的领土扩大到天界，那么在我们自己的领土上空就永远会悬挂着太阳”。他花了五年的时间秘密组成了一支有史以来最强大的军队，到了公元前480年，他已经做好了准备，发动一场出其不意的进攻。

然而，波斯的军备建设都被一个名叫德马拉图斯的希腊人看在眼里。这位希腊人曾经被他的祖国驱逐出境，现在住在波斯的苏萨。但尽管已被流放，他仍然对希腊保持着一份忠诚，因此他决定给斯巴达带去消息以告诫他们薛西斯的侵犯企图。可问题是怎样才能够送出信息而不被波斯士兵截住？希罗多德写道：

因为被发现后危险会很大，因而只有一种方法他能尝试送出这条信息：就是利用已上蜡的一副可折叠的刻写板，先将蜡刮去，再将薛西斯的阴谋刻写在木板的背

面,然后再涂上蜡盖住消息。这样刻写板看上去没写任何字,一路上就不会被士兵怀疑。当这条信息到达目的地后,没有人能够猜出其中的秘密,就我所知,是克莱奥梅尼的女儿戈尔戈,也就是齐奥达斯的妻子,占卦并告诉其他人如果他们把蜡刮去,他们就会发现在木板的背面写有东西。有人这么做了,于是这条信息被揭开,而后传到其他希腊人手中。

由于得到了警告,一直没有防备的希腊人开始武装自己。以前国家银矿的收入通常被民众分享了,现在转给了海军用来建造了二百艘战船。

薛西斯已经失去了战争的一个关键因素——趁人不备。公元前480年9月23日,当波斯舰队向雅典附近的萨拉米斯海湾开进时,希腊人已经恭候多时了。虽然薛西斯相信他已经包围了希腊海军,但是希腊人正是有意地诱使波斯船队进入海湾。希腊人知道他们的舰船又小又少,在开放海域很易被摧毁。但在海湾领域内,他们却可以运用策略打败波斯。随着风向的改变,波斯人发现他们正被风吹进海湾,钻进了希腊人的陷阱。领军出战的波斯公主三面被围,意图退回到海域。却仅有她自己冲了出来。接着,波斯军大乱,更多的船只撞在一起,希腊人发起了全面猛攻。仅一天,强大的波斯军队被挫败了。

德马拉图斯的这种秘密通讯的策略就在于简单地将信息隐藏起来。希罗多德也讲了另一个例子,在这个例子里信息的隐藏程度足以保证其安全传送。他以年事记的形式讲述了希斯塔亚乌斯的故事:希斯塔亚乌斯想鼓励米勒图斯的阿里斯塔哥拉斯反叛波斯国王,为了秘密地传达他的指示,希斯塔亚乌斯剃光了他的一个信使的头发,将信息写在其头皮上,再等信使的头发重新长起来,很明显这段历史时期发生的还不是什么紧急事件。这个信使显然

不用携带任何异物,能够自由穿行,不会有麻烦。一旦到达目的地,他就剃光头发,指给联络人看。

通过把信息隐藏起来的这种秘密通信称为 Steganography(隐文术),由希腊词 Steganos(意为“覆盖”)和 Graphein(意为“写”)派生而来。从希罗多德以后 2000 多年,各种形式的隐文术被使用。例如,中国古代将信息写在小块丝绸上,塞进一个小球里,再用蜡给封上,然后让信使吞下这个蜡球。16 世纪,意大利科学家乔瓦尼·波塔描述了如何将信息埋藏在一个煮熟的鸡蛋里:他把少许明矾和一点醋混在一起制成一种墨水,再用这种墨水将信息写在鸡蛋壳表面。墨水溶液就会经蛋壳上的微孔渗透进去,在已凝固的鸡蛋白表面留下印迹,这样只能剥去蛋壳后才能读取。隐文术也包括用隐形墨水来写信息,早在公元一世纪普林尼就解释了体液如何用作隐形墨水。用这种液体写的字干后即变得透明,但轻轻地加热就能把液体烤焦,从而字迹就以棕色显现出来。许多有机流体都有这样的性质,因为它们富含碳因而很易被烤焦。事实上,即使是现代间谍也很少知道在标准配备的隐形墨水用完之后还可以用自己的尿来临时代替。

隐文术的长久使用表明它确实起到了一定保密作用,但它也有一个根本的弱点。如果信使被搜查,信息被发现,那么秘密通信的内容也立即暴露无遗。一旦信息被截获,所有的安全性也就随之荡然无存。一个严格的士兵会例行地搜查每一个过境人,包括刮一刮所有上蜡的刻写板,给所有空白纸张加加热,剥开煮熟的鸡蛋,剃光人们的头等等。难免会有发现隐藏信息的时刻。

因此,在隐文术发展的同时,还有另一种方法也在演化,那就是 Cryptography(密码术),从希腊词 Kryptos(意为隐藏)派生而来。密码术的目的不是隐藏信息本身,而是要隐藏它的意思,也就是一种加密的过程。为了使信息无法被外人理解,将信息按照事先在发送者和接收者之间规定好的某种特别规则打乱。那么接收