

密码的故事

数字、欺骗与秘密编织的世界权谋史

[英] 阿尔·西米诺 著
杨义先 郑心哲 译

追溯数字的链条，探寻人类智慧的巅峰

湖南文艺出版社

密码是天外之音、无声之音、秘密之音

——麦家《暗算》

枪炮声中的静默大师，现实版本的《模仿游戏》

丘吉尔口中的“秘密武器”

艾伦·图灵、冯·诺伊曼、休·亚历山大……

谁控制了密码，谁就控制了世界。这就是等待着我们的未来。

——马克·古德曼

多亏了“超级机密”，我们才赢得战争。

——温斯顿·丘吉尔

难怪丘吉尔称这种努力为“英国的秘密武器”。这种武器比韦恩赫尔·冯·布朗为德国设计的嗡嗡响的炸弹和火箭更有效。许多人都认为，武器绝对能决定战争的胜负。然而“秘密武器”为盟军赢得了战争。

——彼得·希尔顿

古往今来的任何战争，自始至终都离不开情报战，否则是不可思议的。一方不断努力阅读另一方的主要军事情报，反之亦然。德国人肯定也阅读了我们的大量编码信息，但其阅读方式和内容，无论是在广度还是在深度方面，都达不到我们的程度。

——斯图尔特·米尔纳-巴里

总有一天不再是“他们通过我的电话监视我”，而是“我的手机监视我”。

——菲利浦·K. 迪克



获取更多图书信息



海南出版社微信公号

上架建议：畅销·历史·社科

ISBN 978-7-5443-9195-5



9 787544 391955 >

定价：58.00元

密码的故事

[英] 阿尔·西米诺 (Al Cimini) ◎著

杨义先 钮心忻◎译

海南出版社

·海口· 定价：25.00元

此为试读, 需要完整PDF请访问: www.ertongbook.com

The Story of Codebreaking, by Al Cimino

Copyright © Arcturus Holdings Limited

First published in 2017 by Arcturus Publishing Limited

All rights reserved.

Simplified Chinese rights arranged through CA-LINK International LLC (www.ca-link.cn)

版权所有 不得翻印

版权合同登记号：图字：30-2017-142 号

图书在版编目 (CIP) 数据

密码的故事 / (英) 阿尔·西米诺 (Al Cimino) 著；

杨义先，钮心忻译。——海口：海南出版社，2020.4

书名原文：The Story of Codebreaking

ISBN 978-7-5443-9195-5

I. ①密… II. ①阿…②杨…③钮… III. ①密码学

IV. ① TN918.1

中国版本图书馆 CIP 数据核字 (2020) 第 035100 号

密码的故事

MIMA DE GUSHI

作 者：[英] 阿尔·西米诺 (Al Cimino)

译 者：杨义先 钮心忻

监 制：冉子健

责任编辑：张 雪

执行编辑：邓博文

封面设计：@ 吾然设计工作室

责任印制：杨 程

印刷装订：三河市祥达印刷包装有限公司

读者服务：武 铠

出版发行：海南出版社

总社地址：海口市金盘开发区建设三横路 2 号 邮编：570216

北京地址：北京市朝阳区黄厂路 3 号院 7 号楼 102 室

电 话：0898-66830929 010-87336670

电子邮箱：hnbook@263.net

经 销：全国新华书店经销

出版日期：2020 年 4 月第 1 版 2020 年 4 月第 1 次印刷

开 本：880mm × 1230mm 1/32

印 张：9.25

字 数：180 千

书 号：ISBN 978-7-5443-9195-5

定 价：58.00 元

【版权所有 请勿翻印、转载，违者必究】

如有缺页、破损、倒装等印装质量问题，请寄回本社更换

编者序

多亏了“超级机密”，我们才赢得了战争。

——丘吉尔

密码是一张神秘的通行证，它使只有一线之隔的“公开世界”和“秘密世界”之间烟火缭绕，仿佛隔着千山万水。秘密的价值在于那些不知道秘密的人。在信息化的背景下，秘密就意味着权力。广义的密码并不是令人眼花缭乱的天书字符，也不是需要无线电加密的信息。密码之广泛与普遍，甚至只需要一段旁人不理解的共同经验就可以加密完成。

与文字一样，密码的发现与发明超越了地域、国家、语言，甚至不同文化的隔阂，成为人类某种或某些日常活动的基础。可以说，不同的语言、文化本身就是一种密码，我们去学习一门语言的努力，更像是对另一种文化的破译和解密，只不过这种破译和解密的方式太过普遍，以至于我们忽略了语言本身的加密功能。在悠长的时光中，“密码的故事”见证了人类的活动轨迹，忠实地记录了社会的发展规律，集聚了人类智慧的巅峰状态，极大程度

上推进了人类科技与文明的进步，改变了社会的面貌。

正如这一系列书籍想要表达的思想——无论是《颜色的故事》，还是《密码的故事》，实质上都在讲述“人类的故事”。

密码虽然由人类所创造，但“密码是反科学，反人性的。反科学也是科学，所以研制和破译密码都需要智慧、知识、技术、经验、天才。但同时更需要一颗‘恶毒的心’——不管是研制还是破译密码，因为它是反人性的。密码，说到底，玩的是欺骗，是躲藏，是暗算。兵不厌诈，密码是兵器，是兵器中的暗器，是人间最大的诈”（麦家《暗算》）。在波谲云诡的人类斗争史上，密码将这些天才的数学家、发明家甚至是游戏高手联系到一起，协力改变了历史的进程。

在这本书中，你将会看到：斯巴达人是如何传送秘书，在温泉关重创波斯，为希腊于萨拉米斯战役中战胜波斯奠定基础的；伊丽莎白一世是如何破解玛丽女王的密码，从而粉碎其政变的阴谋，巩固英格兰新教国家宗教的地位的；艾伦·图灵是如何在第二次世界大战中提出现代计算机的逻辑理论，并指导盟军在战争中力挽狂澜赢得战争，同时开创出一个崭新的信息时代的。

毫不夸张地说，现代社会建立在这些人类争斗的故事之中。

然而，《密码的故事》又超脱了“故事”。就在一两个世纪之前，密码还更多地让人联想到浮华宫廷中不足为外人道的窃窃私语，又或者是王公贵族用以纵横捭阖的私密信件。20世纪的两次世界大战以及地缘政治将世界大国联系到一起，今天密码学俨然

成为现代社会的活动基础，其理论知识却愈发艰深晦涩，不为常人所通晓。

对高度信息化的现代社会来说，这种非对称的知识无疑是极度危险的。而这，也是近几十年来兴起的赛博文化所表达的忧思。

随着数字技术的发展，互联网已成为人们生活、工作的重要组成部分，同时也将我们所有信息数据保存到了网络空间中。然而，数字不仅为我们的生活带来便捷，也为我们的个人自由与隐私带来隐患。事实上，在大数据时代，我们的每一笔金融交易、每一次通信、每一封电子邮件和每一通电话都受到编码保护，却又可能是被跟踪的对象。黑客能够通过密码技术来直接盗取或者骗取我们的财产；而大型组织更能通过数据来收集每一个人的喜好、线上活动规律，甚至推断出我们的消费习惯与隐私，以至于掌握我们的一举一动从而达到控制我们未来行动的目的。在这种数据洪流中，个人显得尤为孱弱。

这正是作者为读者提出的先见性警告。在人类数千年的文明历史中，密码以不同的形式作为“矛”与“盾”在我们无法洞见的阴暗处激烈碰撞，悄无声息地改变着历史的进程。但密码却没有像今天这样，对民众拥有如此巨大而又细微的影响力。在这种影响力面前，我们对密码的了解显得如此肤浅，而想要了解它，我们就不能忽视这一段由数字、欺骗与秘密编织的世界权谋史。

这一段权谋史的主角，最早出场于约公元前 1900 年的古埃及，并在无数个人类的关键节点中发挥作用，引领着那些永不言

弃的领袖们侃然前行，编写了一部部有关密码的英雄史诗。直至今今天，它已渗透进我们生活中的每一方面，一以贯之地在舞台后面操控新时代的走向。

《密码的故事》将带领您探索这一串串神秘编码的前世今生，见证这段由智慧、努力、勇气，以及少许运气编织的传奇。

前言

PREFACE

密码攻防

“可以肯定，人类设计的任何密码，都是可破译的。”

埃德加·爱伦·坡



神秘莫测的埃及象形文字，终于被人类借助罗塞塔石碑（Rosetta Stone）给破解了。通常，越罕见的符号，表达的意思就越神秘。



犹太教神秘主义体系的卡巴拉圣典中，也藏有信息。

纵观历史，人类总是想为自己的知识加密，因为知识就是力量，掌握了别人的知识，便能使自己更强大。在古代，那些掌握了炼金术的众神控制着世界文明。人们相信，在律法和《圣经》中隐藏了某些信息，甚至在犹太教神秘主义体系的卡巴拉圣典中，也藏有信息。

战争利器

加密和解密，向来就是战争工具。不论是公开战争（比如在战场上保护消息），还是隐蔽战争中间谍的暗中较量，密码专家们都在进行着一种特殊的战斗，即用自己的加密信息指挥军队，或努力窃取敌方的信息。通常，若对手太强，那就只能依靠智取来挫败敌方计划。

为了用密文与下属通信，尤利乌斯·恺撒（Julius Caesar）发

明了一种加密方法。该方法在几百年后的现代密码学中，仍然扮演着关键角色。在欧洲还处于黑暗的中世纪时，阿拉伯世界就开发出了多种新型的加密和破译方法，其中最著名的就是频率分析。在文艺复兴时期的意大利，欧洲密码破译终于进入辉煌时代，这主要得益于各国家之间互相窥探信息的激烈竞争。

在英国，密码破译导致了苏格兰玛丽（Mary）女王被绞死；而且在“火药阴谋”中，密码破译也扮演了重要角色。在同期的法国宗教战争中，密码破译还导致了胡格诺派（Huguenot）的拉罗谢尔（La Rochelle）失守。后来，路易十四甚至研发出“伟大密码”，并把它作为国家工具。很快，在欧洲主要国家的首都，都建造了自己的“黑室”，专供密码学家在这里拦截、破译别人的密码信息。



托马斯·菲利普斯(Thomas Phelippes)受雇于弗朗西斯·沃尔辛厄姆(Francis Walsingham)爵士，从事反情报工作，以此保护伊丽莎白女王。菲利普斯破译了苏格兰玛丽女王的密码，揭露了她的“火药阴谋”(图中最上面的那行字)，并导致她被判死刑。

机械密码

在北美，美国第三任总统托马斯·杰斐逊（Thomas Jefferson）发明了一种机械加密系统。该系统在形式上，完全不同于美国内战期间开发出来的其他加密系统。同样在 19 世纪，像英国著名物理学家查尔斯·惠斯通（Charles Wheatstone）和数学家查尔斯·巴贝奇（Charles Babbage）等伟大的科学家和计算机先驱，也在密码编码和破译方面花费了大量的时间和精力。大家一致认为，巴贝奇的密码破译系统在克里米亚战争期间曾被使用过。同时，密码破译方法还被用来帮助人们破解已被遗忘的自然语言，比如埃及的象形文字和早期希腊语的“线性文字 B”（Linear B）。

英国截获并破译了齐默尔曼（Zimmermann）电报，披露了德国的作战计划，并将美国拉入第一次世界大战。之后，在 20 世纪 20 年代，美国政府曾经拒绝进行密码破译，认为这是缺乏教养的行为。于是，在第二次世界大战中，在毫无防备的情况下，美国再次受到战争袭击：本来截获了一条加密信息，若及时破译的话，便可预知日本偷袭珍珠港的情报，可惜却破译晚了。之后，美国密码学家努力破译了日本海军的密码，使自己在中途岛战役中占尽了上风，最终取得了太平洋战争的胜利。

恩尼格玛

德国之所以加入第二次世界大战，是因为他们相信自己拥有一种牢不可破的密码——恩尼格玛（Enigma）。但是，德国人没有想到的是，早在战争爆发前，就有三位优秀的波兰密码破译专家已经破译了恩尼格玛密码。波兰人将破译成果和早期破译设备交



在战争年代，通讯最为重要。这是第二次世界大战时期的一些老式装备，其中，最前面那个带键盘的是“恩尼格玛密码机”，它现在被保存在卢森堡迪基希（Diekirch）的国家军事历史博物馆里。

给了英国人，后者把它们用于整个第二次世界大战，并取得了良好效果，特别是在不列颠战役和阿拉曼（El Alamein）战役中，密码破译发挥了重要作用。尤其是在阿拉曼战役中，英国在北非与德国军队对阵时，全靠这些密码破译的成果，力挽狂澜，扭转了战争局势。

在英国位于布莱切利园（Bletchley Park）的密码破译中心，艾伦·图灵（Alan Turing）基于波兰密码专家的密码机，进一步改进了破译方法，使得更复杂的海军的恩尼格玛密码也能被破译。这就重创了曾经扬言要饿死英国士兵的德国潜水艇，并逼迫其投降。随后，布莱切利园的密码破译中心又成功破译了德军最高指

挥部的洛伦兹（Lorenz）密码。这要归功于邮局工程师汤米·弗劳尔斯（Tommy Flowers），他借助首台可编程的数字计算机，解决了该密码破译中的难题。

间谍与谍战

冷战期间，密码编码与破译，是间谍的主要工作。当后来的“007”系列电影中的詹姆斯·邦德用“一次一密”的方法将加密消息藏在公园石头底下时，现实中的研究人员也在努力用计算机程序加密信息，以避免黑客破译出政府和军队的顶级通信密码。

在计算机时代，密码编码和破译已成为商业命脉。海量的金融交易都在网上进行，必须确保它们的安全，使人们的财产不被窃取。一些庞大的政府机构，比如美国国家安全局（National



首台可编程计算机“巨人”（Colossus）及其操作者——英国前皇家海军女子服务队。从左到右分别是：艾琳·狄克逊（Irene Dixon），洛娜·科凯因（Lorna Cockayne），雪莉·惠尔登（Shirley Wheeldon），乔安娜·乔利（Joanna Chorley）和玛格丽特·莫蒂默（Margaret Mortimer）。当时共有 12 台这样的“巨人”计算机。布莱切利园的这些机器，破译了德军最高指挥部的洛伦兹密码。如今，在布莱切利园的国家计算机博物馆里，还可看到“巨人”的复制品。

Security Agency, 以下简称为“国家安全局”或“NSA”)和英国政府通信总部 (Government Communications Headquarters, 简称“GCHQ”), 也在通过拦截和过滤电子邮件, 努力寻找那些使用加密通信的恐怖分子和犯罪分子; 反过来, 网民们也在努力保护个人的隐私, 避免它们被政府窥探和窃取。甚至像量子物理这样高深的东西, 也被用于密码编码和破译者之间的持续较量。

