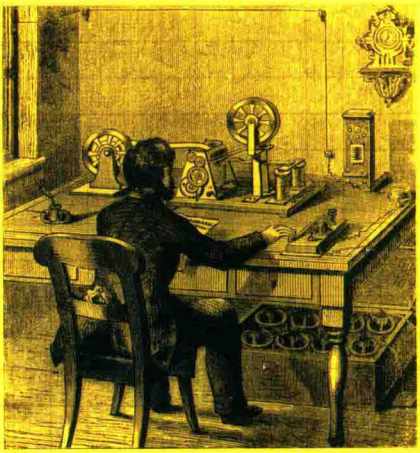
CODEBREAKER

THE HISTORY OF CODE AND CIPHERS,
FROM THE ANCIENT PHARAOHS TO QUANTUM CRYPTOGRAPHY

破译者

从古埃及法老到量子时代的密码史

〔英〕斯蒂芬·平科克 著 曲陆石 译

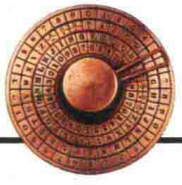


商務印書館
The Commercial Press

CODEBREAKER

the history of code and ciphers, from the ancient pharaohs to quantum cryptography

破译者



从古埃及法老到量子时代的密码史

〔英〕斯蒂芬·平科克 著

曲陆石 译

商務印書館 The Commercial Press

2017年 · 北京

图书在版编目（CIP）数据

破译者：从古埃及法老到量子时代的密码史 /（英）斯蒂芬·平科克著；曲陆石译. —北京：商务印书馆，2016
ISBN 978－7－100－12367－9

Ⅰ. ①破… Ⅱ. ①斯… ②曲… Ⅲ. ①密码—普及读物 Ⅳ. ①TN918.1-49

中国版本图书馆 CIP 数据核字（2016）第160029号

破 译 者
从古埃及法老到量子时代的密码史
〔英〕斯蒂芬·平科克 著
曲陆石 译

商 务 印 书 馆 出 版
（北京王府井大街36号 邮政编码 100710）
商 务 印 书 馆 发 行
山东临沂新华印刷物流
集团有限责任公司印刷
ISBN 978－7－100－12367－9

2017年5月第1版 开本 720×1000 1/16
2017年5月第1次印刷 印张 13½

定价：60.00元

Stephen Pincock

Codebreaker

The History of Codes and Ciphers, from the Ancient Pharaohs to Quantum Cryptography

涵芬楼文化 出品

简　介

当今世界，我们周围充斥着各种各样的加密技术。我们用手机拨打的每个电话，收看的每个有线电视频道，每次从自动取款机里提取现金，都依靠复杂的计算机加密技术来保证不被窃听或偷窥。但是，保密措施不为现代世界所独有。在过去的2000年甚至更早，在政治、血腥战场、暗杀活动和打击犯罪中，代码和密码扮演着至关重要甚至决定生死存亡的角色。战争的胜负、帝国的兴亡、个人的生死，皆受秘密信息的影响，就不算什么稀奇事儿了。密码专家专门将信息意义隐藏到代码或密码背后；机敏狡黠的破译专家，则致力于破解代码与密码，揭示隐藏在它们背后的意义。由于密码利害攸关，两者之间存在永无止息的战争，自然就不会令人意外了。

每次密码专家发明了新的代码或密码，破译专家便陷入一片黑暗中。此前容易破解的信息，突然费解起来。但是，这场战争从未结束。凭着顽强的毅力，或灵感一现，破译专家就会找出坚不可摧的密码中的隐患，不知疲倦地钻研，直至秘密信息再次展现在眼前。

进入破译行当的人才，不论男女都具有许多类似的特质，让他们从事困难且时常危险的工作。首先，他们常常显示出惊人的原创思维。历史上最好的破译专家之一，阿兰·图灵，他的工作扭转了第二次世界大战的局势，他也是他所在的时代最具原创性的思想者。

破译专家的成功也取决于志在必破的决心。没有什么能像秘密那样诱惑人心，而对于破译者来说，努力破解密码往往就是足够的动机。但是，就算他们也会受到其他激励因素的影响——爱国主义、复仇、贪婪，或是对知识的渴望。

破解代码和密码需要的不只是一时的兴趣。尽管早期尤里乌斯·恺撒钟爱的字符换位密码现在看起来简单到小孩子都能攻破，但当时恺撒的敌手却得孜孜以求才能破解编码信息。实际上，绝大多数破译者无法锲而不舍地坚持下去，才使密码破解不了。

速度在密码破译中也至关重要。许多编码和密码是可破解的——但那得一个人有足够的时间研究它们才行。RSA 加密演算是一个经典例子。它依赖的是这么一种奇怪的现象：把两个质数相乘只花一点时间，但要计算一个给定数字是哪两个质数相乘得到的，却得花掉一辈子，哪怕是用计算机计算。

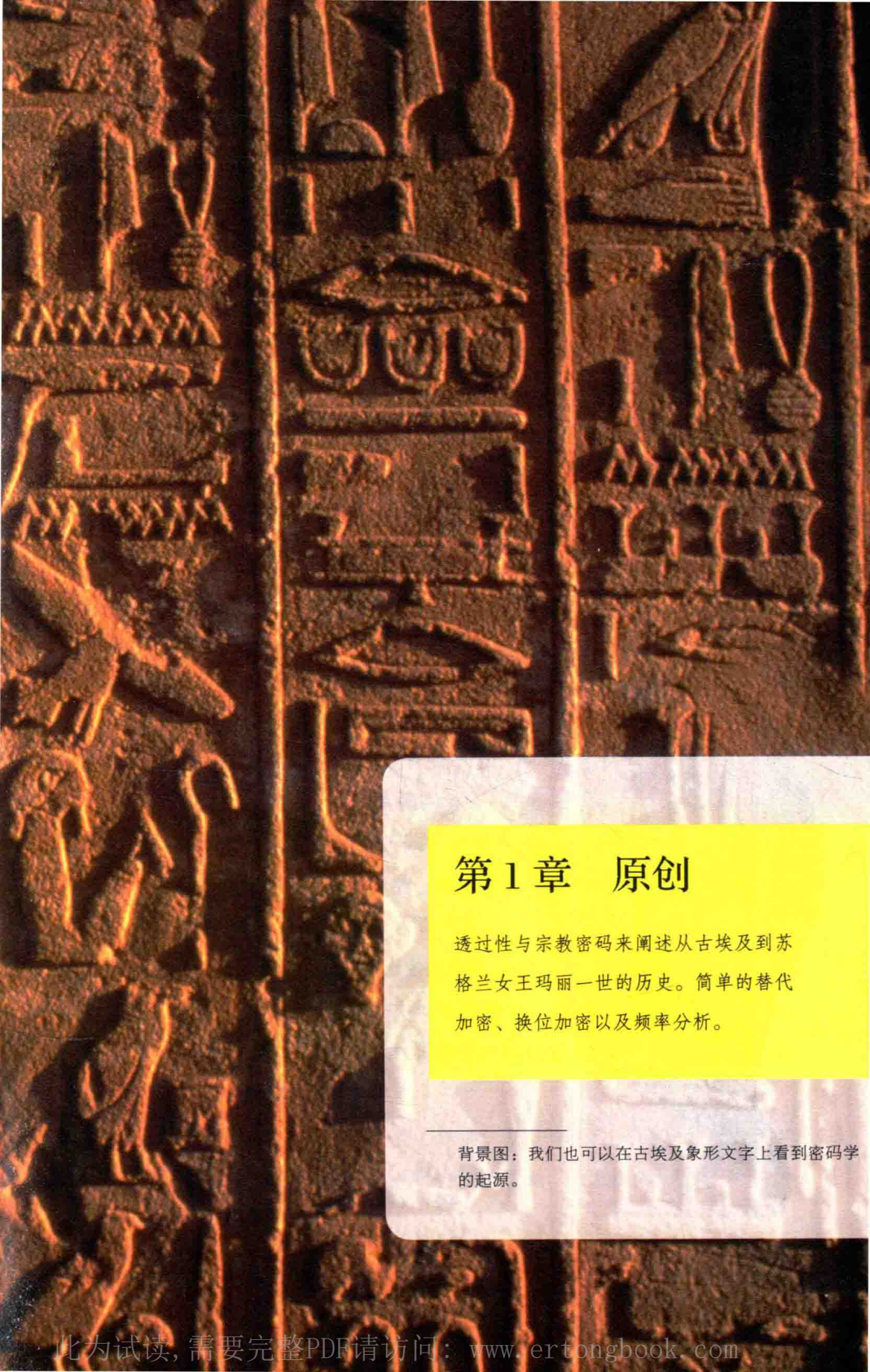
破译者也需要远见。他们经常在官方或刑事保密的掩护下工作，他们工作的敏感性质常常需要他们独自工作。没有对最终目标的预见，破译者们就白费力气。

本书阐述的是密码的创造与破解如何影响历史潮流。这就难怪密码会深深地影响我们的想象力，而《达·芬奇密码》之类解密小说的成功，以及电视、电影中常见破译者的身影，也就不足为奇了。

真实世界并不像小说场景，密码学（尤其是密码分析）的真正历史，如果有什么不同凡响的话，就是比惊悚小说家能虚构出的任何东西都奇怪。在以下篇幅中，你将发现破译者有何出类拔萃之处。你将遇到一些最神秘的人物，并了解破译者必备的基本技能。

但这并不是全部。通过本书，我们为你提供机会，亲自使用这些重要工具。根据你在每一章中学到的内容，我们精心制作了 7 个精巧的密码，希望你能破解它们。破解它们不会太容易——你需要独创性的思维、好运气、毅力以及远见博识。

目 录



第1章　原创

透过性与宗教密码来阐述从古埃及到苏格兰女王玛丽一世的历史。简单的替代加密、换位加密以及频率分析。

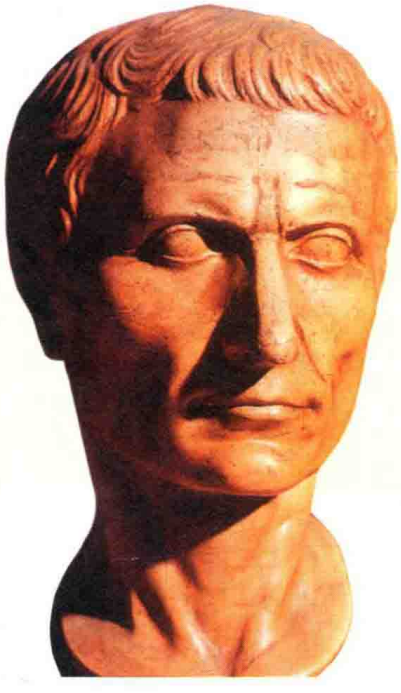
背景图：我们也可以在古埃及象形文字上看到密码学的起源。

很难想象存在一个没有秘密的人类社会——没有诡计、阴谋、政治暗算、战争、商业利益，或者风流韵事的世界。因此，隐藏信息和秘密书写的历史，上溯到世界最古老的文明那里，也不应该让人意外。

密码学的起源可以追溯到近四千年前的古埃及，那时把历史刻入巨大纪事碑的记录者们，开始微妙地改变他们所刻的象形文字的用法和目的。

这些发明，目的多半不为隐藏文辞的意思；反而可能是抄写员想难住或者娱乐来往过客，也可能是想增加经文的奥秘与神奇。但是，他们这么做，开启了在此后的一千年中演化出来的真正的密码学。

在研发密写方法上，不独埃及人一家。例如，在美索不达米亚，密写技术为其他行业所用。在距今日的巴格达 18 英里（30 公里）、位于底格里斯河河畔的塞琉西亚遗址发现的小型泥板，就证实了这一点。这块巴掌大的泥板大约制作于公元前 1500 年，上面以



盖乌斯·尤里乌斯·恺撒，著名的罗马军事家和政治领袖，发明了早期的恺撒密码并加以应用。

加密的方式记载着制作陶釉的配方。用楔形符号中最不常见的音节——最不常见的辅音和元音——用以保护有价值的商业秘密免于外泄。

巴比伦人、亚述人和古希腊人也各自发展出他们自己的方法，用来隐藏信息含意。不过到了古罗马时期，第一位名字永久地与加密法连在一起的重要历史人物出现了，他就是尤里乌斯·恺撒。

恺撒的密写术

作为古罗马最著名的统治者，恺撒名垂青史。作为将领，他以胆识过人著称；作为政治家，他卓见才华服众；而就性格而言，他集奢华的时尚意识、放纵的性欲与赌徒的冒险精神于一身。他睿智、大胆、无情——所有这些，都是成功的密码专家所具备的优秀特质。

在他的战争回忆录《高卢战记》中，恺撒描述了他如何巧妙地掩饰重大战报信息的意义，以防被敌人截获。

在罗马人对抗当地（我们今天称为法国、比利时和瑞士）军队的战役中，恺撒的军官西塞罗被包围，几乎要投降。恺撒想让他知道援军将至，但又不惊动敌军，为此他派了一名信使，带着一封用希腊字母写的拉丁语的信。他告诉信使，如果他无法进入西塞罗的军营，就把信绑在长矛上，然后把长矛投进城防里。

“正如我告诉他的那样，高卢人没管长矛的事儿，”恺撒回忆道，“碰巧，长矛牢牢插在塔楼上，我军两天不曾注意到。到了第三天，一名士兵发现了，取下来，呈给西塞罗。西塞罗读懂了，然后在军前朗读了这封信，将这个最鼓舞士气的消息带给全军。”

恺撒利用密写，古人皆知。一百多年后，历史学家苏维托尼乌斯·特兰克维鲁斯描述恺撒的生平写到，恺撒每有秘密要说，“他就用密码来写”。

密码和代码的定义特质

苏维托尼乌斯对“密码”这个词的用法值得注意，因为尽管我们趋向于把“密码”与“代码”用作可以互相替换的词，但这二者之间其实有重大区别。

大致说来，区别如下：**密码**是一种系统，意在隐藏信息的意思，手段是用其他符号替换信息中的每个字母；而**代码**更注重文字意义而非字母，往往根据代码本中的对照表，来替换整个词语或整个短语。

代码与密码之间的另一个区别，与其内在的灵活性有关。代码是固定的，依赖在代码本里的词语和短语的配对，来隐藏信息的意思。

例如，一个代码或许规定：“5487”这组数代替“攻击”这个词。这就意味着，每次“攻击”被写进信息，代码版本都将包含**代码组**“5487”。即使代码本里包含好几个代替“攻击”的可选方案，变化的方式也有限。

与此相比，密码在本性上更灵活。像“攻击”这么一个词的加密方式可能取决于它在信息中的位置，以及密码系统规则所规定的许多其他可变因素。这意味着，信息中的同一个字母、同一个词语或短语，在同一条信息中的不同位置，也可以用完全不同的方式加密。

对于任何密码系统来说，用于加密信息的一般规则，谓之**算法**。其**密钥**规定了在任何具体情况下进行加密的精确细节。

哈利卡纳苏的希罗多德，公元前 5 世纪的学者和历史学家，在他的历史著作中提到隐写术的早期实例。

隐写

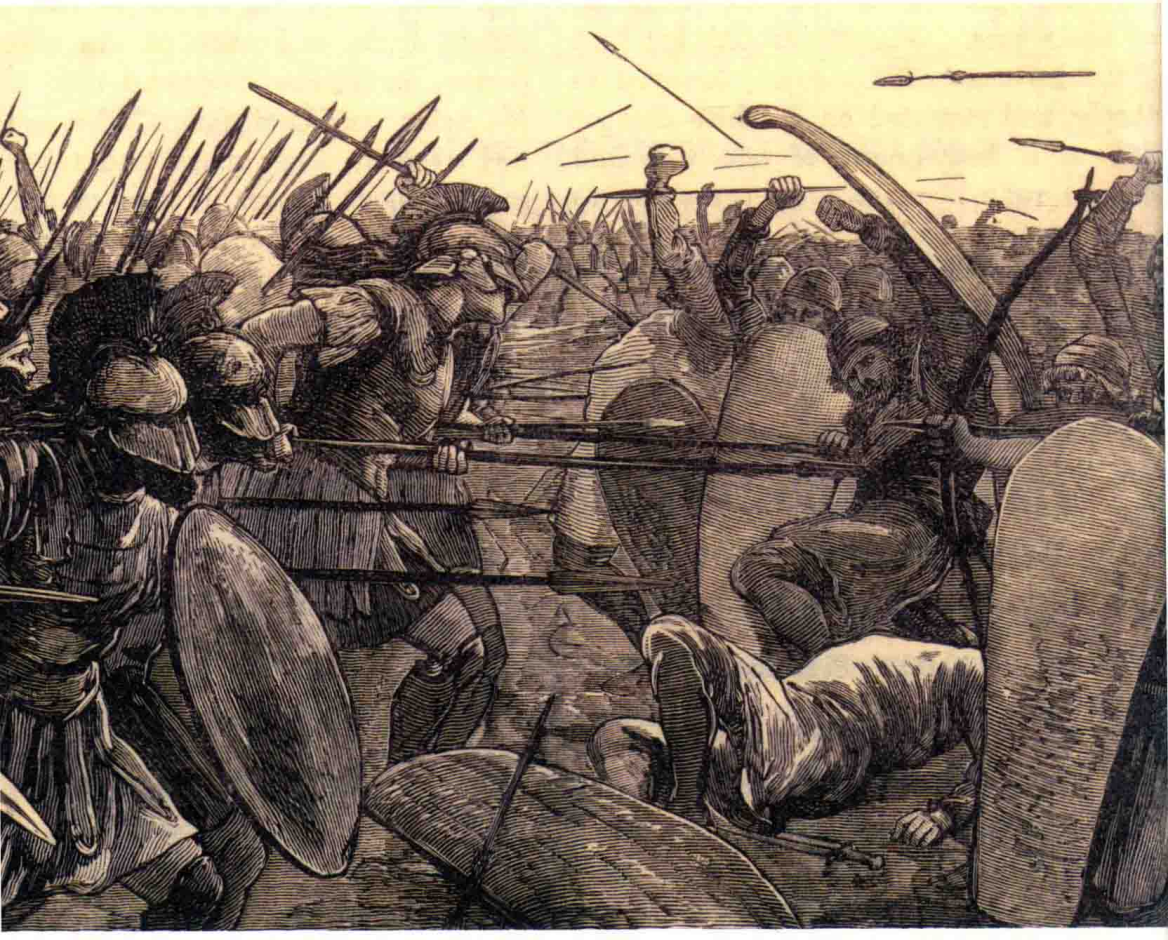
古希腊人擅长密码术，同时也用另一种形式的密写方法，即隐写术。密码术旨在隐藏信息的意思，而隐写术却会全然隐藏存在信息这一事实。

被尊称为历史之父的希罗多德在他的《历史》中讲了好几个隐写术的例子。其中一段，他提到了一个叫哈尔帕哥斯的贵族，此公向米底亚国王复仇，因为国王此前设计让他吃了自己的儿子。哈尔帕哥斯把一条给潜在同盟者的信息藏在了一只死兔子里，然后派一名假扮成猎人的信使把信送去。这条信息送到了，联盟形成。最终，米底亚国王被推翻了。

普鲁塔克（46–127 年），希腊历史学家、传记作家和散文家，他详细说明了密码棒的使用方法。

古希腊人还把信息藏在蜡板的蜡层下面，以免被他人窥破。另外一个更骇人的办法，是把信息刺到奴隶的光头上。假设他在这段时间里没有死于败血症，一旦这位倒霉的信使头发长回来了，他将被派去把信亲自交给某个人。在目的地，信使的脑袋将被预期的收信人剃光；这个收信人就可以阅读这条信息。

用剃头的奴隶送密信，显然有不利之处。其过程极其缓慢尤为人诟病。尽管如此，隐写术还是流传到现代，且一直深受间谍们青睐。事实上，有大



密码棒所传递的加密信息是否让斯巴达人取得胜利？斯巴达的保萨尼亚斯带领军队击败两倍于己的波斯军队。

量不同的加密法，也同样有大量隐写法。隐写法范围广泛，从自古以来隐形墨水的使用，到现代科技手段（把资料秘密隐匿进数字图像或者音乐文件中），都可以算是隐写术的范畴。

古希腊人似乎是隐写术专家。例如，历史学家波利比乌斯发明了一个到现代仍在用的隐写系统。

古希腊人可能通过火把传递信号——例如，左手两个火把，右手一个火把，表示字母b（见第 8 页

“密码分析”）——此谓之“棋盘”法，后来成为发展更加复杂的密码的基础。

可能早在公元前 7 世纪，好战的斯巴达人就以用装置传递秘密信息而闻名。该装置叫密码棒，用的是一种换位密码。

希腊历史学家普鲁塔克讲了密码棒如何运作：

> 当“统治者”派出海军指挥官或将军时，他们制作两个长度、厚度和尺寸都一模一样的圆木棒。然后，统治者自己留一个，把另一个交给派出的将领。他们把这些木棒称为密码棒。如此一来，每当他们想发送重要的秘密信息时，他们就做一狀似皮带的狭长羊皮卷，把它缠到密码棒上，中间不留空隙，将羊皮纸密实地卷在密码棒上。之后便在卷在密码棒上的羊皮卷上写下信息；写完信息之后，他们取下羊皮卷，送给指挥官。当指挥官接到羊皮卷时无法从这些毫无关联、次序混乱的文字中读出任何意思，除非他拿出自己的那个密码棒，将羊皮纸卷上去。