科·学·探·索·发·现·之·旅

KEXUE

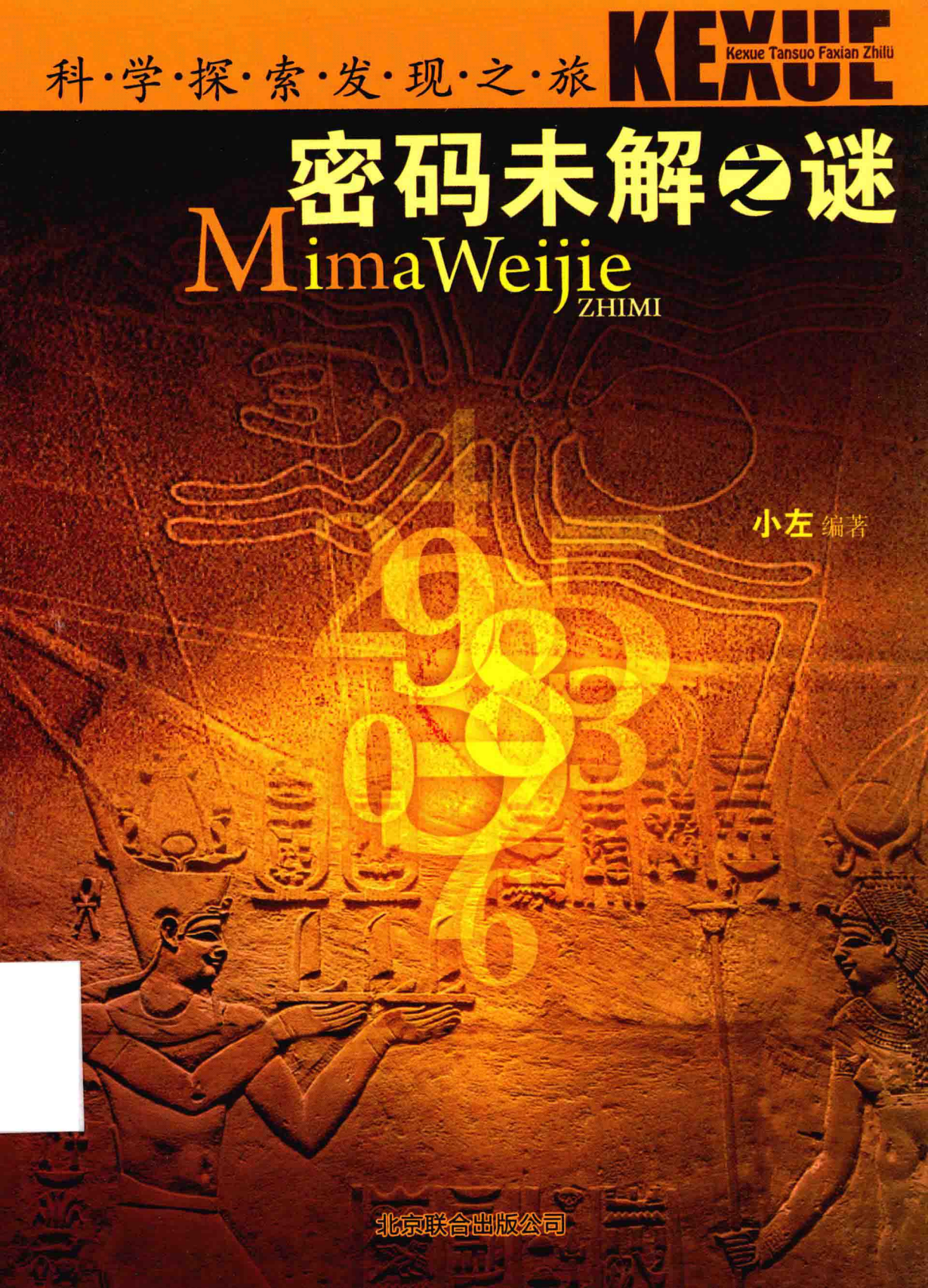
Kexue Tansuo Faxian Zhilü

密码未解之谜

MimaWeijie

ZHIMI

小左 编著



北京联合出版公司

科·学·探·索·发·现·之·旅

KEXUE

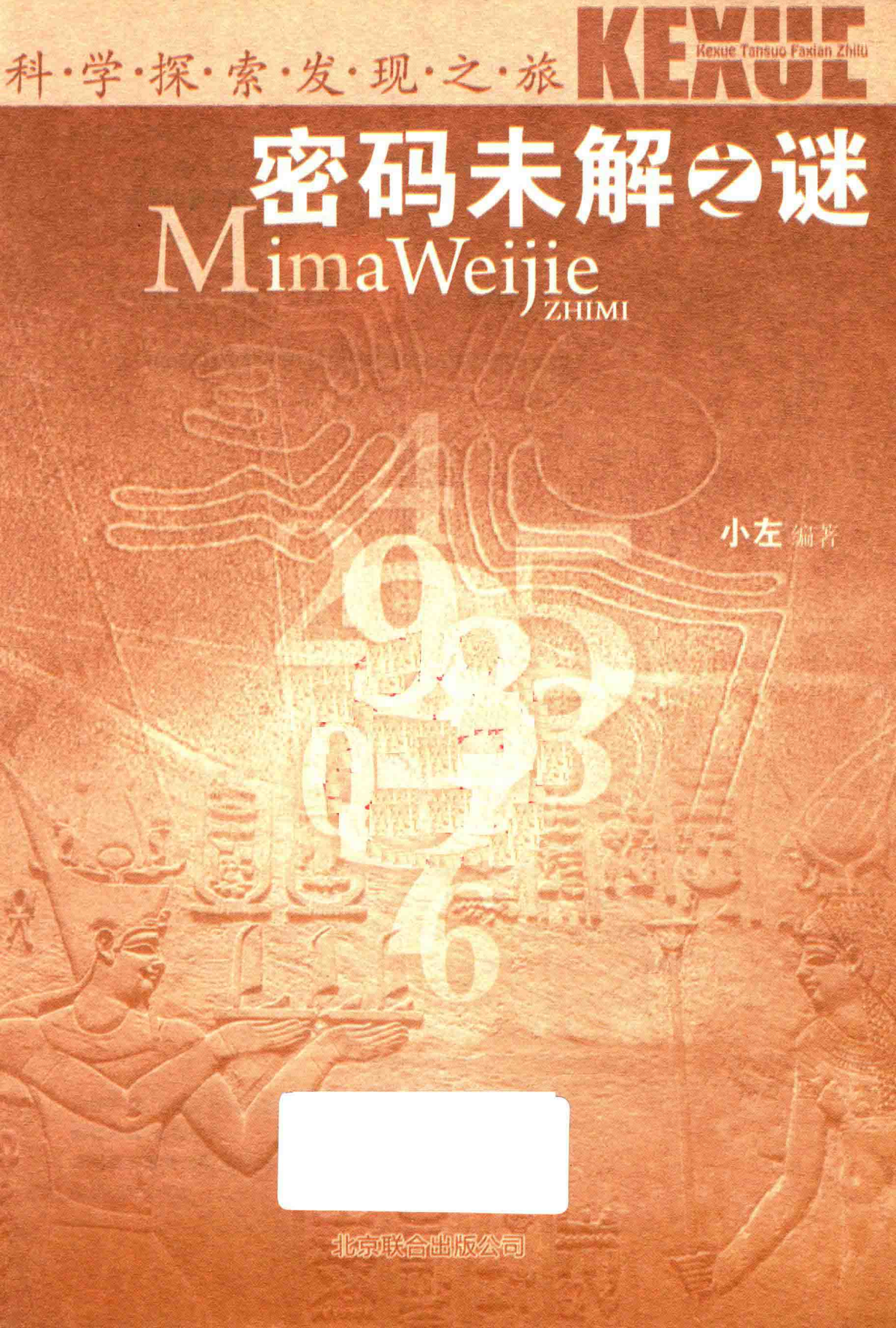
Kexue Tansuo Faxian Zhilü

密码未解之谜

MimaWeijie

ZHIMI

小左 编著



北京联合出版公司

图书在版编目(CIP)数据

密码未解之谜/小左编著. —北京:北京联合出版公司,2015.07
(科学探索发现之旅)
ISBN 978-7-5502-2120-8

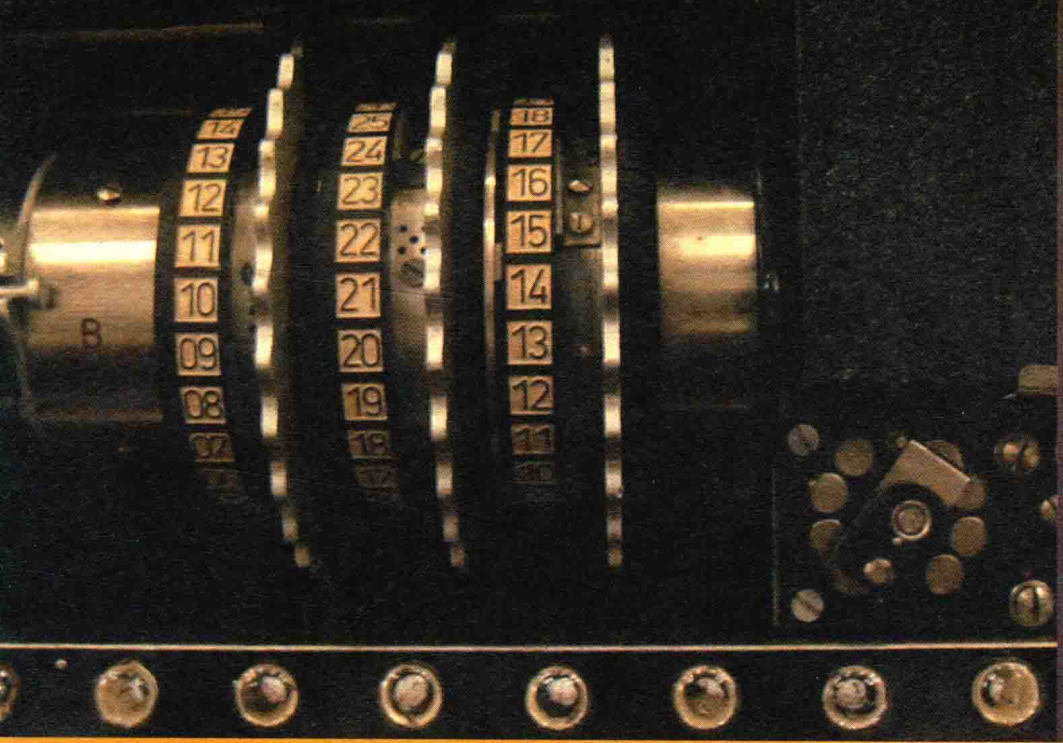
Ⅰ.①密… Ⅱ.①小… Ⅲ.①密码—普及读物 Ⅳ.①TN918.2-49

中国版本图书馆 CIP 数据核字(2013)第 250649 号

密码未解之谜

编　　著:小　左
责任编辑:李　征
封面设计:吕莉梅
版式设计:东方视点

北京联合出版公司出版
(北京市西城区德外大街 83 号楼 9 层　100088)
三河市明华印务有限公司　　新华书店经销
字数 160 千字　710 毫米×1000 毫米　1/16　8.5 印张
2015 年 07 月第 1 版　2015 年 07 月第 1 次印刷
ISBN 978-7-5502-2120-8
定价:29.60 元



FOREWORD 前言

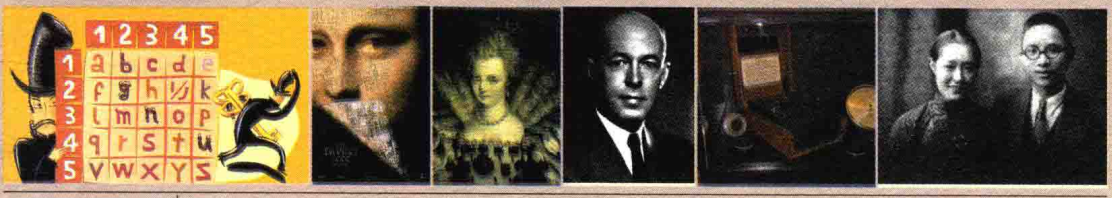
在人类的历史长河中，密码一直是那朵不被人注意，但却散发着迷人魅力的小浪花。今天，我们已经无从知晓是谁发明了第一个密码。我们知道的是，从它诞生之日开始，人类就陷入了无休无止的加密——解密——再加密的无限循环中。这是人类智力的另类较量，也是历史之书的诡异版本。

密码及密码学，从来都不仅仅只是数学家的研究范畴。从凯撒大帝在《高卢战记》里的秘密情报，到玛丽女王软禁岁月中的暗中谋反；从英吉利海峡上空的密电较量，到太平洋战场的硫磺岛反击之战，密码在波诡云谲的历史变幻中一直充当着急先锋与终结者的致命角色。谜一样的密码，密码般的谜，一扇扇紧锁的历史真相的大门，必须要借助密码这把黄金钥匙才能打开。

本书以人类历史和文化为主线，撷取有趣悬疑的未解之谜，向读者系统介绍密码的产生、发展及具体应用的相关知识。以轻松简洁的文字，珍稀罕见的图片，首次曝光的历史资料，让读者在趣味阅读中了解密码学，重新认识那些被人为掩藏和故意篡改的历史文化之谜。

CONTENTS 目录

密码历史之谜 1



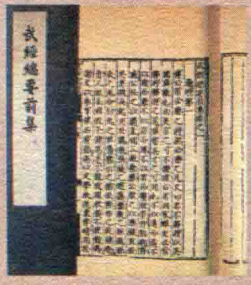
密码战争之谜 31

密码趣味之谜

67

密码文化之谜

93



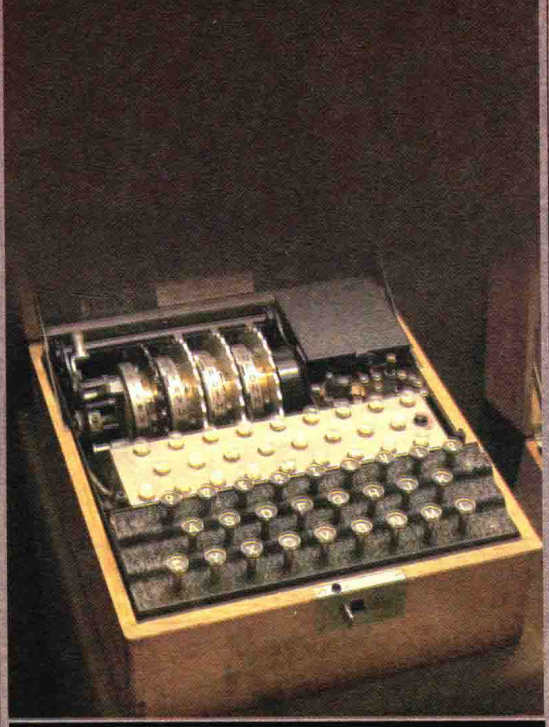
CONTENTS 目录

密码科技之谜

115

PFEESESN
RETMMFHA
IRWEOOIG
MEENNRMA
ENETSHAS
DCNSIIAA
IEERBRNK
FBLELODI

ADFGX
Abtalp
Ddhozk
Fqfvsn
Ggjcux
Xmrewy



密码历史之谜

- 密码的起源之谜
- 世界上最早的密码之谜
- 埃特巴什码与圣殿骑士之谜
- 玛丽女王死于密码被破之谜
- 密码天才赫伯特·奥利弗·亚德利生涯之谜

密码的起源之谜

观点：密码的历史几乎与文字一样悠久，公元前3000年前古埃及就出现了具有密码功能的符号。由于密码的隐蔽性，它不可避免地被首先应用在部族内部斗争与军事战争上。早期的密码虽然简单，但是其设计的巧妙与使用的出人意料，还是令现在的人惊叹赞许。

古埃及象形文字图

密码何时在人类文化中出现，目前没有一个确切的说法。但是，密码的历史十分悠久，这是不争的事实。应该说，人类文明刚刚形成的时候，就有人开始使用密码了。在人类文明几个著名的发源地，都能找到使用密码的事例。

考古发现，公元前2000年，古埃及的某些贵族就有在坟墓中树碑的习惯，这些墓碑上有些神秘的文字，已经具备了密码的特征。考古学家说，墓碑上的象形文字不同于已知的普通埃及象形文字，而是由一位当时的书法家经过变形处理之后写的，但是具体的使用方法已经失传。人们推测，这种做法是为了给坟墓增加神秘气氛，提高墓主的声望。到了公元前1500年左右，还是在古埃及，人们发现了一名陶工留下的信息，他试图用一种简单的密码掩藏自己给陶罐上釉的配方技巧。

《圣经》

希伯来也是较早使用密码的古老的文明之一。公元前 21 世纪，希伯亚民族发源于两河流域的美索不达米亚的吾珥（Ur）。这批游牧民族后来为了寻找牧场而迁移，他们来到迦南的巴勒斯坦之后，被称为希伯来，即迦南语“越河者”之意。希伯来民族在长期的发展过程中，曾经开发出了三种加密法，称为“atbah”、“atbash”和“albam”。这也就是著名的小说《达·芬奇密码》中出现的那种密码体系。中世纪时有许多修士坚信，在《圣经》的古代写本中，就隐藏着大量的密码，那里有众多的神秘信息。甚至还有人从中读出了肯尼迪遇刺与卫星上天等预测，事后被证明大多是生硬的附会及东拼西凑而已。

希腊也有过很早使用密码的历史记载。这是一种非常有趣的传递情报的手段。有一个希腊城邦想要给对方送出一份非常重要的情报，为了保密和掩人耳目，他们把一个奴隶剃成光头，然后在头皮上写下情报内容，等头发长好后，这名奴隶就可以带着这份情报出发。到达目的地后，对方只要再剃去他的头发，就可以读到完整的信息。这种办法看上去很麻烦，但确实非常安全，因为再严密的搜查，也不可能发现头发下的秘密。希腊的密码与众不同，它属于夹带加密法，是把密文以隐藏的方式传递。但问题是，这种密码没有什么时效性，毕竟不是每次都可以等送情报的头发长到可以隐藏情报时，才能够出发将情报传送到它应该被送到的地方。

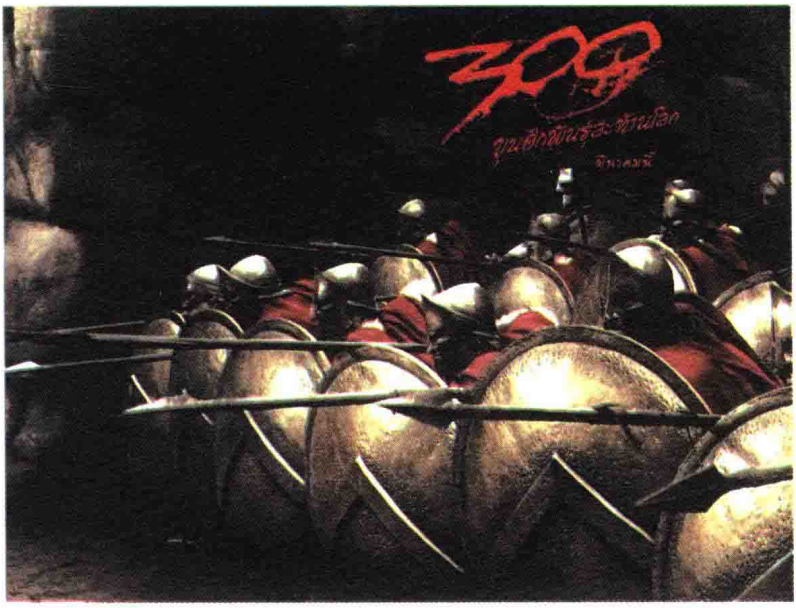
中国是著名的文明古国，历史上也不乏使用密码的记载。公元前 11 世纪的周武王时代，就已经使用了一种“阴符”系统，用不同的长度来表示战争的结果。《资治通鉴》卷二百零一载：唐高宗乾封二年（667），唐朝大军征讨高句丽，运粮使郭待封率

著名科技史专家李约瑟

海军舰队从海上进攻平壤，主帅李勣命冯师本运送粮秣武器在后接应。不想补给船只在海上遇险，未能及时送达前线。郭待封军中乏粮，作书向李勣告急，但他担心书信会落入高丽人之手，从而暴露军中虚实，于是将告急书信写成“离合诗”。

英国科学家李约瑟是公认的研究中华文化的外国人，他曾经称《武经总要》为“军事百科全书”。

《武经总要》是中国北宋时期的军事家、政治家曾公亮编纂的一本书，该书辑录着一种真正意义上的军事通讯密码表，大概也是世界上保存至今最早的军用密码表。当时常规军事通讯存在着严重缺陷，曾公亮创造出了一种“优雅的诗歌密码”。这种密码先在一本密码本中收集当时军中必用的 40 个军事短语，给它们分别编上相应的代码数字。如：1. 请弓；2. 请箭；3. 请刀……一直到最后：40. 战小胜。大将率兵出征时，先带上一个密码本，同时与指挥部事先约定，利用某一首五言诗作为解码密钥。这些事先约定的诗的字数正好是 40，每一个字均对应着 40 个军事短语的某一个。如果前线发生某种情况，需要向指挥部请示或报告时，就在一封普通的公文中有意写进诗中相应的一个字，并在该字上盖章，以示关键所在。指挥部接到公文后，根据这个字到约定的诗中检索一番，便可了解前线发回的意图。指挥部回复时，如果同意，就重新使用这个字，也夹杂在普通的公文中，盖章发回；如果不同意，则什么也不写，依然原样盖章发回。这种诗歌密码，不仅敌人看不出任何异常，就连送信人也一头雾水，确实属于一种可靠的密码通讯。



斯巴达勇士的军阵

真正得到大部分人公认的最早的密码是斯巴达人发明的（也有说法是斯巴达人从希腊人那里学习到的）。公元前8至公元前6世纪，希腊半岛上出现了200多个奴隶制国家，它们以一个城市为中心，包括周围的若干城镇，这被称为“城邦”。在这些城邦之中，有两个最为强大：一个是由欧洲北部南下定居的推崇武力的斯巴达；另一个是发端于地中海沿岸

奇迷机的设计就借鉴了“斯巴达密码棒”的原理

的强调民主的雅典。

公元前 12 世纪，一批多利亚人来到斯巴达地区，200 年后，他们由原有的五个村落渐渐发展成一个城市，称为“斯巴达城”。斯巴达人推行武力扩张的立国信条，凭借自己强大的武装，斯巴达成功地成为希腊半岛上最强大的城邦，并将周围的其他城邦征服，成立了以自己为首的城邦联盟。

公元前 431 年，斯巴达和雅典以及双方的盟友发生了战争。战争持续了几十年，这段时间中斯巴达人借助波斯的力量构建了一只强大的海军。在长期的战争中，斯巴达人使用一种叫“Skytale”（中文译为“天书”）的密码。斯巴达人把一个带状物，比如纸带、羊皮带或是皮革类的东西，呈螺旋形紧紧地缠在一根权杖或木棍上，之后再沿着棍子的纵轴书写文字，在这条带状物解开后，上面的文字将杂乱无章，收信人只需用一根同样直径的棍子（这两根同样直径的棍子可以是在出征前把一根棍子锯断后得到，之后将领和“情报部门”各拿一半。）重复这个过程，就可以看到明文，这还是人类历史上最早的加密器械。

玛丽女王画像

公元 9 世纪，阿拉伯的密码学家阿尔·金迪提出解密的频度分析方法，通过分析计算密文字符出现的频率破译密码。正是利用频度分析法，英国的菲利普斯成功破解苏格兰女王玛丽的密码信，信中策划暗杀英国女王伊丽莎白，这次解密将玛丽送上了断头台。

在 14 世纪，密码得到了更加广泛的运用，主要被炼金术士和科学家们用来隐藏他们的发明。到 15 世纪的时候，欧洲的密码术简直

离合诗

离合诗，是指用拆字法写成的诗，最早见于史载的离合诗出现于南北朝时期。一般认为离合诗属文人的一种文字游戏，实际上，这也就是密码的一种类型。著名诗人皮日休曾经写过一首《晚秋吟》：东皋烟雨归耕日，免去玄冠手刈禾。火满酒炉诗在口，今人无计奈侬何。

第一句的最末一字“日”与第二句的首字“免”，合“晚”字。第二句的最末一字“禾”与第三句的首字“火”，合“秋”字。第三句的最末一字“口”与第四句的首字“今”，合“吟”字。三字组成诗题“晚秋吟”。

已经成为一种产业。文艺复兴时期科学、艺术和宗教的复苏、繁荣刺激了密码术的发展，而使用秘密通信最重要的动机还是政治阴谋，尤其是在意大利。到19世纪，出现了无线电密码通信，逐步运用到军事、政治、经济等领域。第一次世界大战时，密码通信已经十分普遍。到20世纪70年代，密码普及于民用，可谓渗透到社会的方方面面。到了今天，密码更是成为人们须臾不可离的必备。

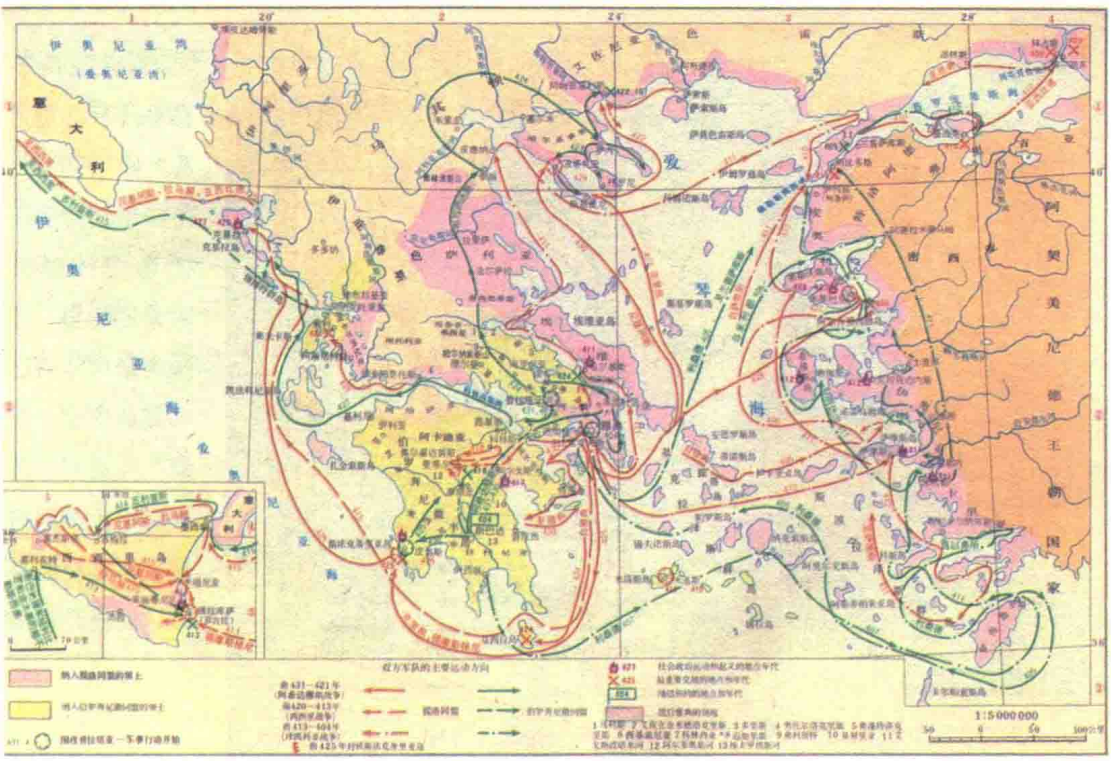
世界上最早的密码之谜

观点：世界上出现的第一种符合密码学意义上的密码是棋盘密码，也即波利比奥斯方表。它是以希腊历史学家、军事家、数学家波利比奥斯 (Polybius) 的名字命名的。这种密码是个划时代的发明，是密码学上的丰碑，它的最大特征就是用 1–5 个数字的组合替代全部字母。可以说，之后出现的许多密码都与其有起源关系。

图为编码所用的可以代替人工的奇迷机

我们都知道，密码之所以会产生、发展及得到应用，根本原因在于人们想要传递一些只有我们希望或者允许的接受者才能接受并理解的信息。一套成体系的密码系统，必须要有以下特征和条件：被隐藏的真实信息称为明文（Plaintext），明文通过加密法（Cipher）变为密文（Ciphertext），这个过程被称为加密（Encryption），通过一个密钥（Key）控制。密文在阅读时需要解密（Decryption），这也需要密钥，这个过程由密码员（Cryptographer）完成。通常使用的加密方法有编码法（Code）和加密法（Cipher），编码法是指用字，短语和数字来替代明文，生成的密文称为码文（Codetext），编码法不需要密钥或是算法，但是需要一个编码簿（Codebook），编码簿内是所有明文与密文的对照表；而加密法则是使用算法和密钥。

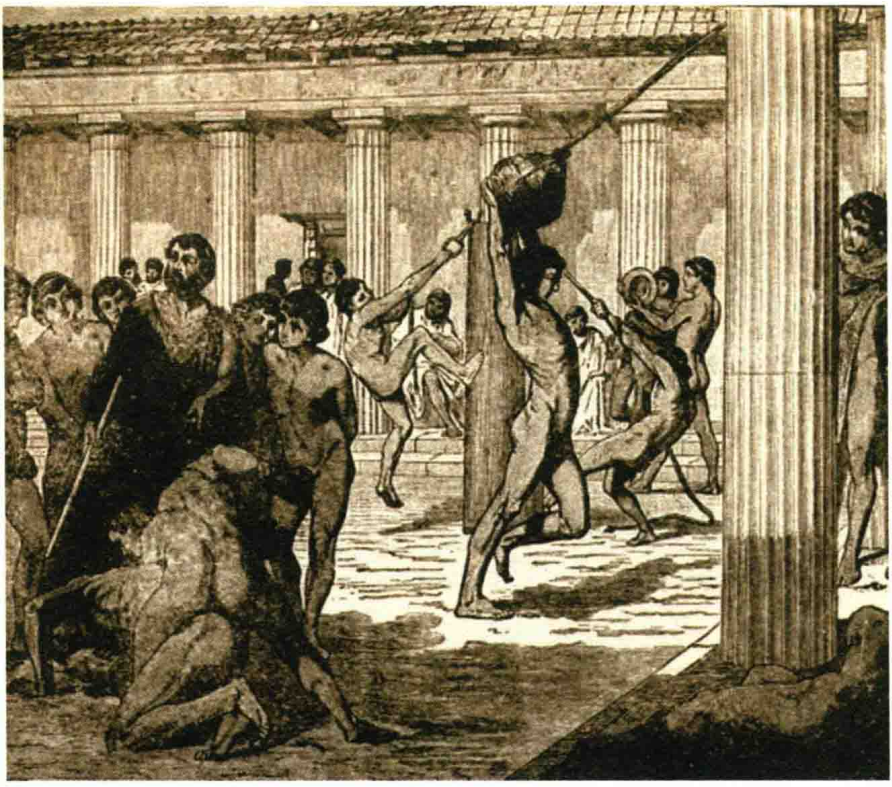
密码在传递过程中，必定面临着被外人截获的风险，这也正是密码编制的原因。当密码落到外人手中时，可能有人凭借耐心和智慧，在没有密钥的情况下得到明文，这种方法称为破解（Break）。如何才能确保密码不被外人破解，保证情报的安全呢？如果如上文所述，像希腊或者古埃及那种简单的掩饰方法，必定不可能做到万无一失。这就要求人们必须



伯罗奔尼撒战争地图

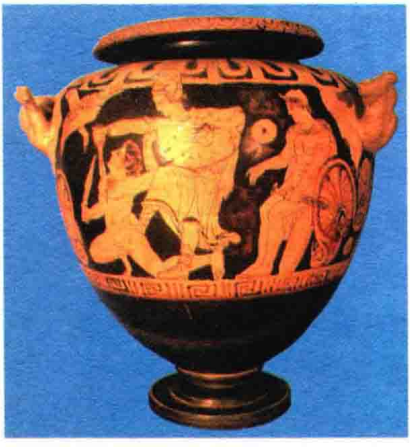
设计一套绝对安全或者足够复杂的密码。

就像今天的最新科技往往首先使用在军事领域内一样，最早的成体系的密码也是出现在两国交战之中。公元前 405 年，雅典和斯巴达之间的伯罗奔尼撒战争已进入尾声。得到了波斯帝国支持的斯巴达军队控制了海上交通，逐渐占据了优势地位。就在斯巴达准备对雅典发动最后一击的时候，原来站在斯巴达一边的波斯帝国突然改变态度，停止了对其援助。波斯帝国这样做，本意是使雅典和斯巴达在持续的战争中两败俱伤，以便从中渔利。在这种情况下，斯巴达急需摸清波斯帝国的具体行动计划，以便采取新的战略方针。正在这时，一名从波斯帝国回雅典送信的雅典信使被斯巴达军队捕获。如获至宝的斯巴达士兵仔细搜查了这名信使，可除了搜出一条布满杂乱无章的希腊字母的普通腰带外，其他任何有价值的东西都



正在训练的斯巴达少年

描绘战争的具有伊比利亚文化风格的陶罐



没有。那么，这名信使把情报藏在了什么地方呢？

事情传到斯巴达军队统帅莱桑德那里，他决定亲自审问这名雅典信使。莱桑德注意到了那条腰带，虽然只有一些杂乱的字母，但他觉得情报就隐藏在这其中。他与助手反复琢磨研究，把腰带上的这些天书似的文字用各种方法重新排列组合，却什么也读不出来。灰心丧气的莱桑德几乎失去了信心，当他无意中把腰带呈螺旋形缠绕在手中的剑鞘上时，奇迹出现了。原来腰带上那些杂乱无章的字母，竟组成了一段文字。原来，这果真是雅典间谍送回的一份情报，上面显示，波斯军队会在斯巴达军队发起最后攻击时，突然对斯巴达进行袭击。莱桑德根据这份情报，马上改变作战计划。他指挥斯巴达军队，首先突然攻击毫无防备的波斯军队，一举将它击溃。解除后顾之忧之后，斯巴达军队又回师征伐雅典，取得了伯罗奔尼撒战争的最后胜利。

雅典间谍送回的这份令斯巴达人百思不得其解的腰带情报，就是世界上最早的密码情报。具体方法是，通