Verschlüsselte Botschaften

灯塔译丛

密码传奇

——从军事隐语到电子芯片

〔德〕鲁道夫·基彭哈恩 著
邓白桦 姚文俊 滕峻辉 译 卫茂平 校

上海译文出版社

灯塔译丛

Verschlüsselte Botschaften

密码传奇

——从军事隐语到电子芯片

〔德〕鲁道夫·基彭哈恩 著
邓白桦 姚文俊 滕峻辉 译
卫茂平 校

上海译文出版社

前　言

在青少年时代，我对密码的兴趣并不比其他喜欢神秘的男孩大。当然，我读过《跳舞小人》中歇洛克·福尔摩斯的故事，但我却不记得自己对密码有什么特别着迷的地方。即使在大学学习数学时，我也没意识到我的专业和加密、脱密这门艺术之间的联系有多么密切。直到在我70岁时，有位朋友给我讲起密码学的全新动态时，我才开始从事这方面的研究，而且我自己突然被一种来自这门学科的力量牢牢吸引住了。我了解了一些人的命运，密码学在这些人的生命中打下了烙印，之所以这么说，是因为他们将自己献身于编写和破译密码事业；之所以这么说，是因为密码保护了他们，或者相反，破译的密码使他们大难临头。

不知从什么时候起，我觉得有必要讲讲这种吸引力，于是便诞生了这本《密码传奇》。对这个题目研究得越多，我在情感上也就越深地卷入到第二次

世界大战的事件中去。因此，我书中有一部分是关于德国密码机“恩尼格玛”和那些成功地破译其密码的人。

然而，我并不是要写历史，更不是要写什么战争史。我感兴趣的是密码学本身。我之所以描写历史过程，是因为正是密码学在历史中卓然可见，科学与人类命运休戚相关。

如果得不到多方面的帮助，我不可能完成这本书。我和许多朋友，其中包括在查找资料时才结识的朋友进行过讨论，从中学到了不少东西。我感谢所有的人，特别是弗朗茨-莱奥·贝雷茨、约阿希姆·海因克、赖马尔·吕斯特、哈特穆特·佩措尔德、沃尔夫冈·斯孔多和赫尔穆特·施泰因韦德尔先生。此外，我还要感谢汉堡地方法院院长女士，感谢为我完成摄影工作的罗尔夫·施平德勒先生。但我特别想感谢的是我的朋友，数学家汉斯·路德维希·德弗雷斯，他不仅激励我进行该课题的研究，而且还和我一起逐页逐页地对全部文章进行修正，就像对待我以前的书稿一样。最后，我还要谢谢罗沃尔特出版社工作人员的真诚合作。

该书中所有的图表都是用 Corel Draw! 绘图程序的制作，其中有部分图片来自克利帕尔特图书馆。

鲁道夫·基彭哈恩

格丁根，1997 年 3 月 17 日

1

战争与和平中的密码

我比较熟悉各种形式的秘密文字，也写过一篇关于这个问题的粗浅论文，其中分析了160种不同的密码。

歇洛克·福尔摩斯

（《跳舞小人》）

“大桥先生，如果我被判处死刑的话，我作鬼也会回来找你。”逃犯对秘密警察署的检察官说，经过多次审讯两人之间已经形成了一种和谐的气氛。1941年10月那个星期六清晨，当人们闯入记者R·佐尔格东京的家中，把穿着睡衣、趿着拖鞋的他带到警察署去时，大桥检察官也在场。

从那以后，犯人有足够的时间来思索他的生活。在牢房刚开始的几个星期中，这失败的新体验把他推入绝望。后来，一种起初较微弱，之后逐渐增强的安慰感在他体内复苏，他的确成功地完成了任务，这种想法使他更能忍受不可知的未来

命运。在希特勒对苏联发起进攻之后，佐尔格向莫斯科第四局发出信息，日本不会从东边向苏联进攻。正是他的报告使得朱可夫元帅能够把军队、坦克和飞机从西伯利亚撤出来转移到莫斯科前方去对付德国人。难道不是他，R·佐尔格创造了世界历史吗？从审讯人的问话中他可以断定，日本人没能破译他加密的消息，他的报务员曾数千次地将这些消息发送到上海和海参崴的苏维埃电台。

报务员克劳森致电莫斯科

这个夏日，东京上空的空气令人窒息。马克斯·克劳森看着他前面桌上的纸条。过了一阵，文章才被破译。他读着——又是"奥托"发来的报告。上司从来没跟他说过，但是马克斯知道，"奥托"是小组中的一个日本同事，他的消息总是很重要。

1941 年 6 月 22 日后，德国军队越来越深入苏联境内。很久以前，马克斯就向莫斯科发电警告，其中甚至还包括德国进攻的准确日期，然而那里却没人作出反应。也许，苏联在不久以后不仅要对付德国，而且同时——虽然在 4 月份已订立不进犯条约——也必须防御日本？日本在这几天里进行了战争动员，新组建的部队会被调往南方，还是调往北方，对付苏联？

"奥托"的报告弄清了一切。日本无论如何也不会进攻俄国，因为中国的事件已经够它忙的了，只要与美国的谈判结果尚不明确，没有一个日本人愿意与俄国打仗[①]。如果日本确

① F·W·迪金，G·R·斯托里：《R·佐尔格：一个著名的双重角色的故事》，慕尼黑，1965 年，第 259 页。

实要进攻苏联的话，最早也应在明年，在这期间德国军队早已深入到俄国领土内部去了。看来希特勒在冬天来临之前想占领莫斯科。日本方面不会进攻的消息使苏联大大地松了一口气。报务员马克斯·克劳森开始了加密工作。

他虽然已熟知第一步，但这次还是用了一张纸，这张纸随后就会被销毁。第一步是将字母表中的字母与数字对应起来，为此他必须利用他的密钥词，即英语中“地铁”这个单词：SUBWAY。他按顺序写好这 6 个字母，然后在下面划了 4 条线，在这 4 条线中按顺序分别排入字母表中剩余的字母以及圆点和线符号(作为单词分开的标志)。这样，他就得到了图 1.1 上面这张表格。

因为他总是用英语发送信息，所以在这种语言中最经常出现的字母 a、s、i、n、t、o、e 和 r 对他来说就显得特别重要。“a sin to err”(犯错是一种罪过)这句话正是由这些字母组成的——这是一种帮助记忆的方法，对克劳森来说已没必要。这 8 个字母应分别分配给 0…7 这些数字，他将这数字填入表格，逐列逐列的，从左开始。一旦碰到“a、s、i、n、t、o、e、r 当中的一个字母，就按从 0 到 7 的顺序在下面写下其中一个数字。这样，他的表格就很像图 1.1 中间这一幅了。现在他在剩余的字母下按竖列顺序写下从 80 到 99 的数字，于是就得到图 1.1 下面这张表格。

现在，字母表中的每一个字母都有它对应的数字，利用它们，克劳森就能够将电文中的字母转换成一排数字。我们以一条简单的电文为例进行说明：按照德语“没有进攻”，即英语的“no attack”的顺序，产生了“729456658088”，这 12 个数字符号又可以被轻而易举地分解为与字母或字符相应的数字。如果字符前没有 8 或 9，字符将单个地与表格中的一个字母相

对应；如出现 8 或 9，则与下一个字符一起对应表格中的某个字母。在“729456658088”中，7、2、94 和 5 分别与字母（亦即符号）n，o，/和 a 对应，两个 6 对应双写是 t，80 是 c，88 代表字母 k。于是，“no attack”就被加了密，但这只不过是第一步，克劳森眼前得到的仅仅是暂时加密的电文而已。

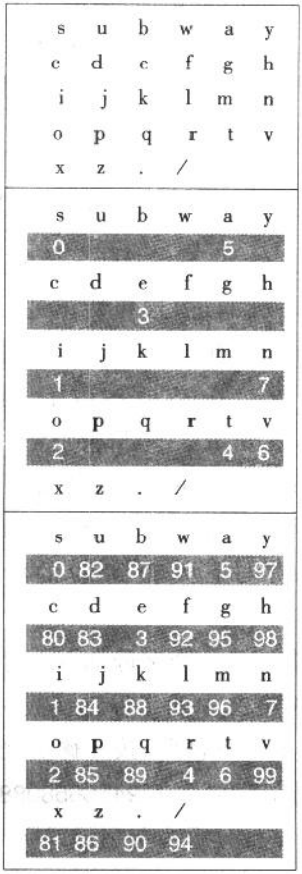


图 1.1：马克斯·克劳森用密钥词 SUBWAY 和 asintoer 这个提示词分三步制成一张密码表，利用这张表他可以将字母表中的字母转变成数字。

至此加密工作只完成了一小部分。每个新手都能发现，在用这种方式编写的长条消息中，数字“3”出现的频率最高，它与无论德语还是英语中都最常出现的字母 e 相符合。这样，每个窃码者都可以完成解码的第一步。所以，马克斯·克劳森现在才开始真正编写密码。他从书架上拿出 1935 年德意志统计年鉴，翻开充满数字的一页。他记下页码和表格中某个数字的行数和列数，他想从这个数字开始。这些是关于各个国家烟草生产的报告，其中有数字 4230，下面是 5166、7821、9421 等等。他必须从第一个数字的第三个数码开始，然后加入其他数字：30516678219421……这是莫斯科和他之间的一种老规定，而这一行数字才是真正的密钥。克劳森写下他暂时加密的电文，再在下面写上密钥：

729456658088
305166782194 . .

然后把它们相加，在这当中，如果和数超过 9，十位数就不进到前面一位，即不是 7 + 8 = 15 而是 7 + 8 = 5，计算过程见图 1.2 上，接下来他还得告诉接收人年鉴的页码以及行数和列数，以便对方可以从同一本书中查取密钥。就页码而言，两个数字就够了，因为如果给出 34，那么可以是 34、134 或 234，至于哪个是正确页码，接收人自己很容易就可以判断。就行数和列数来说，3 个数字也够了。236 指第 23 行第 6 列，所以 34236 总共 5 个数字就足够标识密钥的开头。克劳森将这 5 个数字放在他电文的开头，但把它们加密，方法是把密文开始的 5 个数字相加，同样再次排除十进位法，即将 34236 + 02451 = 36687。这样，他的电文就被分成若干组，每组 5 个数字：36687 02451 23301 72，然后向空中发送这些数字组。他知道，

接收人首先会把第一组数字减去第二组数字，不考虑十进位制：36687 – 02451 = 34236，这样他就获得了页码（34 或 134 或 234）以及行数和列数（23 和 6），即所有用来确定密钥的信息。现在他只需从接收到的电文中（排除用来找密钥的前 5 个数字）减去密钥；如图 1.2 下所示。

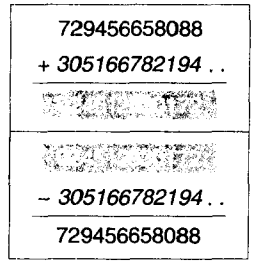


图 1.2 上：从一条数字化的，即已转变成数字符号的普通电文，通过密钥（斜体部分）变成一条数字化的秘密电文；下：从数字化的秘密电文到数字化的普通电文。

这样，他就得到了用这份表格加了密的电文，而且能轻而易举地将其译回普通电文，因为他手上也有图 1.1 下的那一份表格。

马克斯·克劳森每次都从不同的地方发送新信息。如果上一次是从自己的住所发送电波，那么下一次就从间谍组织中一位南斯拉夫同事的家里，偶尔在其他朋友那儿他也会架起电台，竖起天线。因此，虽然这些从东京向空中频繁传递的电波早已引起了日本秘密警察的注意，但他们却无法在这座人口密度极高的城市中测定和发现电台的方位。

为了不被测向车发现，在发报的过程当中克劳森也经常更换位置，他不时地将发报机从一个地方挪动到另一个地方，所以很有可能在这时撞上警察，但最后泄露间谍组织的却并

非电波，日本警察是在仔细调查日本共产党早期支持者的过程中，偶然发现的。

1941 年 10 月 14 日晚，R·佐尔格想和他的日本同事尾崎秀实，这个专门提供消息的“奥托”碰头，但这人却没有在约好的时间露面，接下来的几天里也无法用电话与他联系上。克劳森在 10 月 17 日深夜即 18 日凌晨被捕，警署的人在大清早也敲响了佐尔格的门。对他以及他同事的审讯持续了 3 年多，尾崎和佐尔格于 1944 年 10 月 7 日被绞死；而克劳森被判终身监禁，他妻子也被处以服刑 3 年的惩罚。在日本投降以后，这两人都被盟军释放并逃往苏联，之后很长一段时间内再也没有听到有关他们的消息。

直到将近 20 年后的 1964 年 10 月，东柏林的一家报纸[①]刊登了一篇题为《马克斯·克劳森还活着》的报道，称莫斯科《消息报》的柏林通讯社在德国同志的帮助下，发现了克劳森夫妇，他们在民主德国首都过着简朴和隐居的生活，于是各种新闻媒体开始对此大肆宣扬。这对夫妇在一次疗养度假之后于 1964 年前往当时的苏占区，并化名为“克里斯蒂安森”定居下来，后来迁往柏林，东柏林报界将此二人誉为正直的共产党人和民主德国市民。直到此时民主德国的媒体才发现，马克斯·克劳森曾由于他“模范的建设意志”成为焦点人物，《新德意志报》从档案中发掘出一条已尘封 9 年的关于先进工作者“马克斯·克里斯蒂安森”的新闻，他那时是克珀尼克游艇厂的政治指导员，照片上的他正用尖头十字镐清除废墟。当时报纸还不知道这张照片上的人和谁有关呢。

据说当时他对自己的功绩秘而不宣，只是由于其谦逊的

① 1964 年 10 月 29 日《新德意志报》。

性格所致。然而1964年沉默突然被打破，克劳森接受采访并详细谈论了他在日本与佐尔格从事的工作。克劳森——克里斯蒂安森突然又重新露面。关于先进工作者马克斯·克里斯蒂安森过去的报道显然直到1964年才被公开。因为每次就佐尔格周围间谍组织工作进行的深入的历史研究，都不可避免地涉及斯大林所犯的错误，即斯大林最后将佐尔格关于希特勒进攻苏联的警告当成了耳边风。但1964年已取消禁令，德国统一社会党中央委员会成员、民主德国国家广播委员会主席、老共产党员格哈特·艾斯勒可以光明正大地回忆他和佐尔格曾见过一面，老党员赫尔曼·西布勒也重新记起他和直到现在仍被人闭口不谈的R·佐尔格见面的情景。而格拉工具机器厂的劳动英雄埃伦弗里德·纳瓦拉则让他的生产小组在佐尔格生日之际举行一场劳动竞赛。81岁的马克斯·克劳森于1979年9月15日与世长辞，在此之前他早已被授予卡尔·马克思勋章、苏联红旗勋章以及其他高级荣誉称号。

日本人始终未能破译R·佐尔格忠诚的发报员发出的加密电文，因为编密方法早被精心设计了一番，而且关键是利用一本无关紧要的书，而这本统计年鉴可能在抄家时未被注意到。

小蜡板的秘密

发报员马克斯·克劳森致电莫斯科的方式令外行人无法读懂，而对于今天的编码人员来说却十分原始，他可以让电脑将一封发给一位澳大利亚同事的信加密，并通过网络寄出。但相对于初步尝试信息加密的人而言，克劳森已采用了一种相当不错的方法。

早在几千年以前，人们就已经开始交换秘密消息。世界历史上的许多事件周围都萦绕着有关秘密消息的传话，例如公元前480年著名的温泉关战役。

今天，在欧罗巴75大道上从塞萨洛尼基朝雅典驱车前行，经过奥林匹斯山后，便抵临拉米亚海湾，在那儿，高速公路沿海岸延伸。丘陵上的纪念碑使人回想起那场战役，在这次战役中斯巴达国王莱奥尼达斯抵抗由波斯国王薛西斯率领的优势兵力，但却徒劳无功。其实战争爆发之前莱奥尼达斯就在等待着波斯军队的到来，因为他已通过一封密信得知了这一消息。

正如希腊历史学家希罗多德所报道的一样，一个被流放波斯的希腊人送了一块小蜡板回国，一块与当时人们用于书写毫无二致的涂有蜡层的小木板。这人先除去蜡层，在木板上写下关于波斯人将大举入侵的消息，然后又重新抹上蜡并把它送给了莱奥尼达斯。由于这样一来这封信无法读出，于是得以畅通无阻地抵达希腊，不过如果不是莱奥尼达斯的妻子戈尔戈无意中发现了蜡层下面的字迹，这则消息肯定会被一直隐藏下去。莱奥尼达斯就是这样接到警报的。

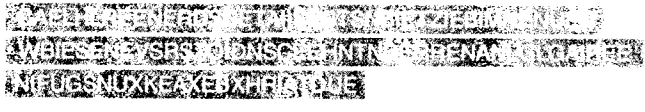
然而，如同历史上屡见不鲜的事例一样，这封密信并没有对战争的结局产生什么决定性的影响。一个希腊的叛徒带着波斯人通过一条隐蔽的小路，越过山岭，偷袭莱奥尼达斯位于温泉关的驻地，于是莱奥尼达斯的军队被左右夹击，最后全军覆没。

根据希罗多德的记载，当时没人能从外面看出小蜡板里隐藏着至关重要的消息，估计蜡板上可能刻有一篇无关紧要的文章，使人根本无法注意那则真正的消息。

致桑道夫伯爵的密信

1867 年,的里雅斯特是奥地利帝国的一座城市,哈布斯堡王朝准备在它的北面建立王朝最大的港口,然而那年春天出现了种种不太利于该计划实施的迹象。几个月前,奥地利在克尼格雷茨战役中败给了普鲁士,而自从拉约什·科苏特领导的起义被奥地利人镇压下去之后,匈牙利的自由运动就从未平息过。

儒勒·凡尔纳的小说《马蒂亚斯·桑道夫》就是以这种紧张的气氛为背景的:匈牙利伯爵桑道夫暂时住在的里雅斯特,由信鸽给他捎去关于家乡独立斗争运动的加密消息。有一次,一封信件落入敌手,大意是人们已准备就绪,只等他一声令下便起义反抗奥地利,信文如下:



奥地利间谍中当然无人能破译这封信,直到一个混蛋从伯爵的书桌里窃取密钥之后,他们才得以解开它。

密钥是一个由横竖 6 格组成的正方框。从 36 个正方格里剪去 9 格,于是形成一个编码板,如图 1.3 所示。接收人为解开密码,将秘密信文写成 3 个正方形,每个由 36 个字母组成,如图 1.4 上所示。现在他把编码板放在秘密信文字母组成的正方形上,通过剪掉的空格读出:allesistb(图 1.4 下左),然后沿顺时针方向将编码板旋转 90 度(图 1.4 下右),并读出:ereitbeim。再转 90 度:erstenzei,又一次转动编码板:chendassi。这样,第一个方

框的工作就完成了，与其他几个方框一起得出原文：

allesistbereitbeimerstenzeichendassieunsvontriestsendenwerdener hebensichallefuerdieunabhangigkeitungarnsxxx

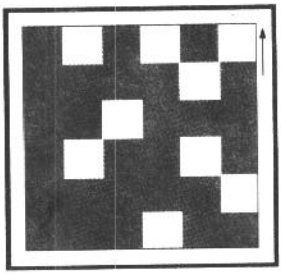


图 1.3：这是儒勒·凡尔纳在他的小说《马蒂亚斯·桑道夫》中所描绘的编码板，把它放在一张空白纸上，在框中剪去的（图中为白色）格里填入需要加密的消息的前 9 个字母，之后沿顺时针方向将编码板旋转 90 度，并在空格里填入接下来的 9 个字母。依此类推，直到编码板已转过 4 个方位为止，填入的字母在纸上构成一个长宽各为 6 格的正方形，按行读出，便得到了编好的信文。如消息更长，则又开始一个新的正方形；如方框不能填满，则任意选择字母补充信文，直到 36 个空格都被填满为止。

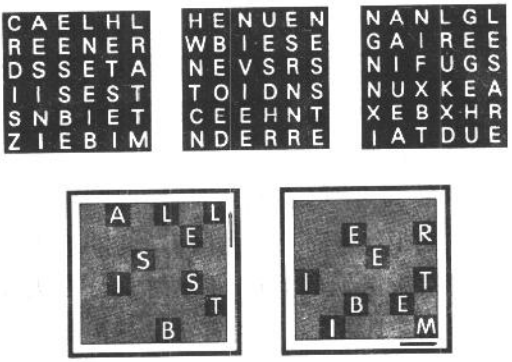


图 1.4：如何破译第 10 页上的加密信文。秘密信文被写成 3 个正方形，如上。将图 1.3 的编码板按照最初的形式放在第一个正方形上，如左下，右下为顺时针旋转 90 度后的情形，在这两种状态下，原文的前 18 个字母被重现出来。

为了让秘密信文填满 3 个正方形。信的结尾补充了 3 个增加的字母 x。

玛丽亚·斯图亚特是如何被出卖的

大约在 1586 年，菲利普二世成为西班牙国王，他从父亲卡尔五世手中接过了一个世界王国，一个包括西班牙、西西里岛和意大利南部的王国，拥有哈布斯堡家族的所有财产以及西班牙遍及全球的殖民地。因此卡尔五世可以骄傲地宣称："在我的王国里太阳不会落下！"当 1527 年他的儿子菲利普出生时，即路德把他的论纲贴在维滕堡宫殿教堂的大门上之后的第十年，新教开始在欧洲各国传播开来。连苏黎世教士乌尔利希·茨温利也反对罗马教皇的教义。继而是瑞士法语区的 J·加尔文，经他改革的教派传播到法国、荷兰、英格兰和苏格兰。菲利普二世让他奥地利的同父异母兄弟，唐·胡安管辖当时仍属于西班牙的荷兰，此人曾于 1571 年在勒班陀战役中与意大利人一道战胜了土耳其人，捍卫了天主教。被派往荷兰后，他仍把抵制福音新教的异端邪说，保护天主教教义当作自己在该处最重要的使命。

在英国，早在 30 年代，亨利八世就和罗马教皇闹翻了，这是因为罗马教皇拒绝宣布英格兰国王亨利八世与卡尔五世的姑妈卡塔琳娜结束婚姻的消息，也不赞成接下来他与一名宫廷妇女的亲事。在此之后，亨利宣布自己为英格兰教派的带头人，并强迫教士承认他的权威地位，以代替罗马教皇。于是在当时便形成了支持加尔文教义的英国圣公会。改革主要是在亨利的女儿伊丽莎白一世的统治下进行的，就这样，英格兰发展成为最强大的新教势力。

在苏格兰，加尔文教义也找到了支持者，在一次起义中，天主教女王玛丽亚·斯图亚特被驱逐出境，她在亲戚伊丽莎白的国家里寻求庇护，然而这两人之间的关系却异常紧张。国内的天主教徒认为，按照法律玛丽亚才是英格兰真正的女王，这招致她后来被伊丽莎白软禁了长达20年。

据说玛丽亚·斯图亚特是个魅力十足的女人，但这显然并不是唯一的原因，唐·胡安企图率领军队登上英格兰，迎娶玛丽亚，帮她坐上伊丽莎白的位子，与她共同治理这个国家。他还在信中告诉其他人他的这一想法，当然是以加密的形式，然而这种方式对他却毫无帮助，显然他没有考虑到英格兰的特务机构这一因素。

伊丽莎白一世在位时，英格兰国内的阴谋造反运动甚嚣尘上，以至于不得不建立秘密警察以维护国家制度。该机构的建立由伊丽莎白的大臣弗朗西斯·沃尔辛厄姆负责。当他几年前在意大利旅游时，就已强烈地感受到编写密码的重要性，而这在当地已有着悠久的历史。他创建了一个机构，单单在欧洲大陆上就安插了53个密探。这一举措的作用，不久就显露出来了。那时，荷兰一位深谙密码的贵族接到一封悄悄递来的密码信，一个月后他破译了该信。信是唐·胡安发出的，在信中他公开表露占领英格兰的梦想。沃尔辛厄姆的一个亲信在荷兰获悉该信内容后向大臣报告了此事。大臣认为，眼下正是十万火急的紧要关头，应对玛丽亚·斯图亚特严加看管。碰巧就在此时，他偶然收到一个名叫吉尔伯特·吉福德的囚犯的申请书，请求替他效劳。待此人刑满之后，沃尔辛厄姆接纳了他并委之以监视玛丽亚·斯图亚特周围动静的任务。于是，吉福德就作为信差混入了玛丽亚的人当中。

1586年，当玛丽亚在英格兰被软禁了20年之后，她的一