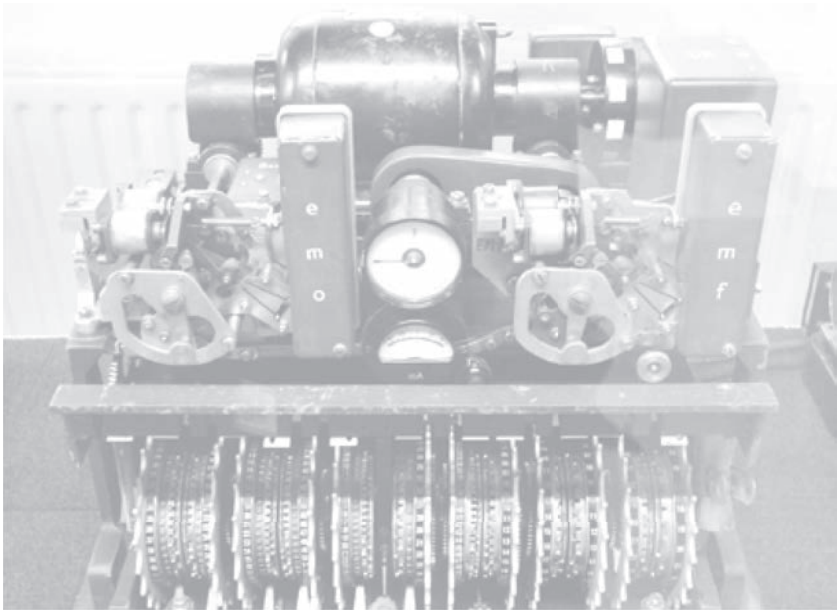
神圣的秘密服务

Mark Ronan

译者：李样明、薛燕汝

Mark Ronan，伊利诺伊大学芝加哥分校的数学名誉教授，伦敦大学学院的数学名誉教授。他曾就读和任教于多地：德国的不伦瑞克大学和柏林自由大学；从 1989 年到 1992 年在英国的伯明翰大学任梅森数学教授；在美国的伊利诺伊大学芝加哥分校，他教授的课程包括从美索不达米亚时代开始的古代文学、历法史和数学。除了研究工作，他还在芝加哥歌剧院表演过多部歌剧，参与芭蕾舞剧《胡桃夹子》的演出。

007 系列故事的作者 Ian Fleming，是第二次世界大战时期英国海军情报局和“政府密码学校”（Government Code and Cypher School, GC&CS）的联络官。政府密码学校是英国政府的一个秘密机构，如果德军知道它的作用



↑ 在布莱切利庄园中陈列的Lorenz电传打字加密机（第二次世界大战中德军最高统帅部专用的秘密通信设备）

和地址的话，早就将其炸得粉碎。其“雇员”（如果可以这样称呼的话）为象棋大师、数学家、古典学者、纵横字谜爱好者，还有其他各种各样的怪人；原先的办公大楼住满了，于是他们住进一些临时棚屋里进行工作。他们分散在一个大庄园（译注：布莱切利庄园，作为第二次世界大战期间政府密码学校的所在地，1992 年起对外开放）里不同的地方，而且彼此之间不认识（也没有必要）。因此在战后 46 年重聚的时候，他们都很惊讶地看到别人之前也在那里工作过。没人和外人谈论过，一个字也没有，一点儿都没有。当一个妇女发现自己的丈夫也被邀请来参加重聚，她还询问自己的丈夫究竟是怎样得到这个邀请的。她曾经在那里工作过但从没向他提及 —— 她丈夫也一样。

现在我们都知道，那是在布莱切利庄园 —— 就在米尔顿 · 凯恩斯—白金汉郡的外面。在那里可以参观到缴获来的 Enigma 密码机，上面带有接线板和 3 个加密的转子。海军和反间谍机关的密码机则带有 4 个转子。而德军最高指挥部使用的 Lorenz 机器上有 12 个转子。破解 Enigma 密码的方法最初是波兰人获得的，但必须不断地了解其最新的设置参数，而这需要大费脑筋。德国陆军和空军都是使用相同的标准 Enigma 密码机，但最优先的是要掌握德国海军密码机的设置参数。于是 Fleming 想了个点子：让一架缴获的德国飞机坠落于英吉利海峡，英国特种部队战士藏身于飞机中；当德国潜艇赶来救飞机时，就可以制服潜艇人员并获得艇上密码机在这个星期的设置参数。这个主意从未被采纳，但是确实采取了其他一些办法。1942 年末，当英国食物供应减少到大概只能维持 6 个星期的储量时，三个男人 —— 其中一个仅有 16 岁，进入北大西洋的一艘 U 型潜水艇中，搞到了德国海军密码机的每月密钥设置参数。在这次行动中，16 岁的男子活下来了，而其他两个都牺牲了。

八号棚屋是数学家 Alan Turing 工作室，他在这里破解德国海军密码。这个聪明的、富有创造性的思想家设计了一种电气—机械解密装置来替换原先波兰人使用的那个。他的工作使得盟军在大西洋每月的损失从 50 万吨减少到 5 万吨。有一些数学家是没有多少性需求的人，喜欢在偏僻安静的英国教区牧师的住宅和剑桥大学里工作，但是 Turing 是一个身体健康、性能力强的男人，他时常跑步到 40 英里外的伦敦参加重要会议（译注：Turing 是一位优秀的马拉松运动员）。战后，他荣获英帝国勋章。但是稍后因为他的性取向被起诉 —— 他是一个同性恋者。1954 年，年仅 41 岁的他自杀了。直到去年九月（译注：指 2009 年 9 月 11 日），英国首相才对 Turing 遭受指控表示了歉意，称他的遭遇为“可怕的”。确实如此。

虽然破解德国海军密码是一件很棘手的事，但破解德国最高指挥部的密码（称为金枪鱼，是由带 12 个转子的 Lorenz 电传加密打字机产生的）则几乎是不可能的；特别地，布莱切利庄园从未缴获过 Lorenz 机器 —— 他们战

后才获得一部。但在 1941 年 8 月 30 日，他们幸运地有了一个突破。一个德国密电员在雅典传输了 4500 字符的电文到维也纳。但是电文接收得不是很准确，因此密电员请求重新传输 —— 但是该请求没有加密。这就提醒了布莱切利庄园的密码专家，当德国密电员在雅典第二次传送电文时，他用了缩写词但是同样的设置参数，它们泄露了非常珍贵的信息。一个名叫 Bill Tutte 的数学家随后破解了 Lorenz 机器的结构，在北伦敦的多丽斯山上的邮局的研究中心开始设计一个大型的取名为巨人的计算机来破译从德国最高指挥部得到的电文。这项了不起的智力伟业甚至使破解 Enigma 密码机的成就相形见绌，但是这要与时间赛跑。到 1944 年 6 月 1 日，巨人 2 号在布莱切利庄园开始运作，及时赶上了诺曼底登陆。破译的德军最高指挥部的密码显示，希特勒已经被误导相信了错误的登陆地点，而且德国军队被安排在错误的位置上了。

在 20 世纪 50 年代初，政府密码学校改名为在切尔滕纳姆的政府通信总部（GCHQ），原先住在布莱切利庄园棚屋里的工作人员，现在也住进了一栋叫做“甜甜圈”的现代化大楼中。1970 年，在政府通信总部工作的 James Ellis 证明了，存在一种现在所有的破解方法都对它无可奈何的密码 —— 称为公钥密码体系。1973 年，也在政府通信总部工作的 Clifford Cocks 在被告知 Ellis 的想法的半个小时后，就想出了一个实现该密码的数学方法。当然这是完全保密的，但是在 1987 年，3 个人 —— Ron Rivest, Adi Shamir, Leonard Adleman —— 重新发现它，现在被称为 RSA 算法。下面就是 Ellis 的想法。

取一个大数 N—— 比如，600 位数，它远远大于宇宙中微粒的数目。将你的秘密信息转变为一连串的数字，然后将之分裂成一些片断，每一片断小于 N。通过做一系列的简单的数学变换将信息编译成加密的信息，但是在每一步骤中只取被 N 除后的余数。敌人可以截取加密的信息，知道大数 N 和精确的操作顺序，但是依然不知所措。解密相当于分解大数 N，但甚至是拥有最好的办法也需要花比宇宙年龄更长的时间。创造大数 N 很简单：你可取 2 个 300 位的素数的乘积。你 —— 或你的电脑 —— 知道因式分解，但是没有其他人会知道。

因此，并不奇怪，政府通信总部也雇佣数学家，包括大学的专业学者，虽然他们不仅不能够谈论他们所做的事情，甚至回到家后也不能思考关于工作的事情。正如布莱切利历史所示，英国人擅长保密。但是我有一丝怀疑：它有非常好的现代大厦并运用最新的数学，但世上有不少奇人 —— 如黑客能够从伦敦北部的阁楼里侵入美国的五角大楼获取机密；Oliver Sacks 则在他的书《错把太太当帽子的男人》里，描述了两个孤独症患者，他们俩是一对具有计算天赋的兄弟，能够立即判断出大的素数。还有，存在量子计算机，它在理论上能立刻做因子分解。但是还没有人能建造一台任何尺寸的量子计

算机 —— 或许它们已经被造出来了？

我希望政府通信总部仍然拥有一些棚屋，有古怪的人在里面工作，尽管我们极有可能在另一个 50 年里无法得到有关他们的消息。

编者按：本文译自 Mark Ronan, On Her Majesty's Secret Service, September 2010，STANDPOINT (http://www.standpointmag.co.uk/node/3314/full).