**Enigma破译过程（愿做展示）**

计21

2012011401

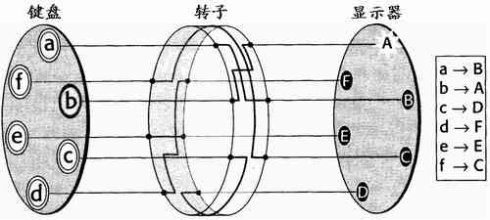
张梦豪

摘要：亚瑟·谢尔比乌斯 Enigma 键盘 转子 显示器 反射器 连接板 汉斯—提罗·施密特 绝密情报 雷杰夫斯基 “重复乃密码大敌” “炸弹” 布莱切利公园阿兰·图灵 候选单词 破译

正文：

Enigma是德国发明家亚瑟·谢尔比乌斯Arthur Scherbius发明的加密电子机械。它将被证明是有史以来最为可靠的加密系统之一，而对这种可靠性的盲目乐观，又使它的使用者遭到了灭顶之灾。

Enigma看起来是一个装满了复杂而精致的元件的盒子。不过要是我们把它打开来，就可以看到它可以被分解成相当简单的几部分。下面的图是它的最基本部分的示意图，我们可以看见它的三个部分：键盘、转子和显示器。



在上面ENIGMA的照片上，我们看见水平面板的下面部分就是键盘，一共有26个键，键盘排列接近我们现在使用的计算机键盘。为了使消息尽量地短和更难以破译，空格和标点符号都被省略。在示意图中我们只画了六个键。实物照片中，键盘上方就是显示器，它由标示了同样字母的26个小灯组成，当键盘上的某个键被按下时，和此字母被加密后的密文相对应的小灯就在显示器上亮起来。同样地，在示意图上我们只画了六个小灯。在显示器的上方是三个转子，它们的主要部分隐藏在面板之下，在示意图中我们暂时只画了一个转子。

键盘、转子和显示器由电线相连，转子本身也集成了6条线路（在实物中是26条），把键盘的信号对应到显示器不同的小灯上去。在示意图中我们可以看到，如果按下a键，那么灯B就会亮，这意味着a被加密成了B。同样地我们看到，b被加密成了A，c被加密成了D，d被加密成了F，e被加密成了E，f被加密成了C。于是如果我们在键盘上依次键入cafe（咖啡），显示器上就会依次显示DBCE。这是最简单的加密方法之一，把每一个字母都按一一对应的方法替换为另一个字母，这样的加密方式叫做“简单替换密码”。

所以如果转子的作用仅仅是把一个字母换成另一个字母，那就没有太大的意思了。但是大家可能已经猜出来了，所谓的“转子”，它会转动！这就是谢尔比乌斯关于Enigma的最重要的设计——当键盘上一个键被按下时，相应的密文在显示器上显示，然后转子的方向就自动地转动一个字母的位置（在示意图中就是转动1/6圈，而在实际中转动1/26圈）。

但是我们看到，如果连续键入6个字母（实物中26个字母），转子就会整整转一圈，回到原始的方向上，这时编码就和最初重复了。而在加密过程中，重复的现象是很危险的，这可以使试图破译密码的人看见规律性的东西。于是谢尔比乌斯在机器上又加了一个转子。当第一个转子转动整整一圈以后，它上面有一个齿拨动第二个转子，使得它的方向转动一个字母的位置。

我们看到用这样的方法，要6\*6=36（实物中为26\*26=676）个字母后才会重复原来的编码。而事实上ENIGMA里有三个转子（二战后期德国海军用ENIGMA甚至有四个转子），不重复的方向个数达到26\*26\*26=17576个。

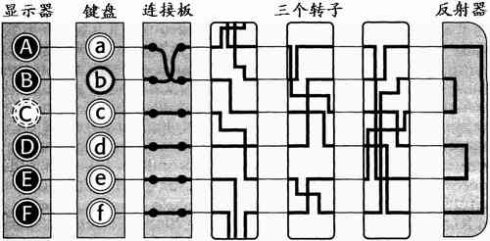
在此基础上谢尔比乌斯十分巧妙地在三个转子的一端加上了一个反射器，而把键盘和显示器中的相同字母用电线连在一起。反射器和转子一样，把某一个字母连在另一个字母上，但是它并不转动。乍一看这么一个固定的反射器好象没什么用处，它并不增加可以使用的编码数目，但是把它和解码联系起来就会看出这种设计的别具匠心了。

当一个键被按下时，信号不是直接从键盘传到显示器（要是这样就没有加密了），而是首先通过三个转子连成的一条线路，然后经过反射器再回到三个转子，通过另一条线路再到达显示器上，在这种设计下，反射器虽然没有象转子那样增加可能的不重复的方向，但是它可以使译码的过程和编码的过程完全一样。

于是转子的初始方向决定了整个密文的加密方式。如果通讯当中有敌人监听，他会收到完整的密文，但是由于不知道三个转子的初始方向，他就不得不一个个方向地试验来找到这个密匙。问题在于17576个初始方向这个数目并不是太大。如果试图破译密文的人把转子调整到某一方向，然后键入密文开始的一段，看看输出是否象是有意义的信息。如果不象，那就再试转子的下一个初始方向……如果试一个方向大约要一分钟，而他二十四小时日夜工作，那么在大约两星期里就可以找遍转子所有可能的初始方向。如果对手用许多台机器同时破译，那么所需要的时间就会大大缩短。这种保密程度是不太足够的。

当然谢尔比乌斯还可以再多加转子，但是我们看见每加一个转子初始方向的可能性只是乘以了26。尤其是，增加转子会增加ENIGMA的体积和成本。谢尔比乌斯希望他的加密机器是便于携带的（事实上它最终的尺寸是34cm\*28cm\*15cm），而不是一个具有十几个转子的庞然大物。首先他把三个转子做得可以拆卸下来互相交换，这样一来初始方向的可能性变成了原来的六倍。假设三个转子的编号为1、2、3，那么它们可以被放成123-132-213-231-312-321六种不同位置，当然现在收发消息的双方除了要预先约定转子自身的初始方向，还要约定好这六种排列中的使用一种。

下一步谢尔比乌斯在键盘和第一转子之间增加了一个连接板。这块连接板允许使用者用一根连线把某个字母和另一个字母连接起来，这样这个字母的信号在进入转子之前就会转变为另一个字母的信号。这种连线最多可以有六根（后期的ENIGMA具有更多的连线），这样就可以使６对字母的信号互换，其他没有插上连线的字母保持不变。在上面ENIGMA的实物图里，我们看见这个连接板处于键盘的下方。当然连接板上的连线状况也是收发信息的双方需要预先约定的。



只要约定好上面所说的密匙，收发双方利用ENIGMA就可以十分容易地进行加密和解密。但是如果不知道密匙，在这巨大的可能性面前，一一尝试来试图找出密匙是完全没有可能的。我们看见连接板对可能性的增加贡献最大，那么为什么谢尔比乌斯要那么麻烦地设计转子之类的东西呢？原因在于连接板本身其实就是一个简单替换密码系统，在整个加密过程中，连接是固定的，所以单使用它是十分容易用频率分析法来破译的。转子系统虽然提供的可能性不多，但是在加密过程中它们不停地转动，使整个系统变成了复式替换系统，频率分析法对它再也无能为力，与此同时，连接板却使得可能性数目大大增加，使得暴力破译法（即一个一个尝试所有可能性的方法）望而却步。

在自1925年接下来的十年中，德国军队大约装备了三万台ENIGMA。谢尔比乌斯的发明使德国具有了最可靠的加密系统。在第二次世界大战开始时，德军通讯的保密性在当时世界上无与伦比。似乎可以这样说，ENIGMA在纳粹德国二战初期的胜利中起到的作用是决定性的，但是我们也会看到，它在后来希特勒的灭亡中扮演了重要的角色。

汉斯—提罗·施密特(Hans-Thilo  Schimdt) 于1888年出生在柏林一个中产阶级家庭里，一次大战时当过兵打过仗。根据凡尔赛条约，战败后的德国进行了裁军，施密特就在被裁之列。退了伍后他开了个小肥皂厂，心想下海从商赚点钱。结果战后的经济萧条和通货膨胀让他破了产。此时他不名一文，却还有一个家要养。他只好去请求春分得意的大哥，当时是德国通讯部门的头头，给他在政府机构中谋求的一个职位。施密特把一家留在巴伐利亚，因为在那里生活费用相对较低，勉强可以度日。就这样他一个人孤零零地搬到了柏林，拿着可怜的薪水，对大哥又羡又妒，对抛弃他的社会深恶痛绝。

接下来的事情可想而知。如果把自己可以轻松搞到的绝密情报出卖给外国情报机构，一方面可以赚取不少自己紧缺的钱，一方面可以以此报复这个抛弃了他的国家。1931年11月8日，施密特化名为艾斯克Asche)和法国情报人员在比利时接头，在旅馆里他向法国情报人员提供了两份珍贵的有关ENIGMA操作和转子内部线路的资料，得到一万马克。靠这两份资料，盟国就完全可以复制出一台军用的ENIGMA机。

在十年前法国和波兰签订过一个军事合作协议。波兰方面一直坚持要取得所有关于ENIGMA的情报。既然看来自己拿着也没什么用，法国人就把从施密特那里买来的情报交给了波兰人。和法国人不同，破译ENIGMA对波兰来说至关重要，就算死马也要当作活马医。现在他们总算能迈出最初的一步了。

在施密特提供的关于ENIGMA的情报中，不仅有关于ENIGMA构造和转子内部连线的描述，还有德国人使用ENIGMA进行编码的具体规定。每个月每台ENIGMA机的操作员都会收到一本当月的新密钥，上面有此月每天使用的密钥。比如说，第一天的密钥可以是这个样子：

连接板的连接：A/L-P/R-T/D-B/W-K/F-O/Y

转子的顺序：2,3,1  
转子的初始方向：Q-C-W

当操作员要发送某条消息时，他首先从密钥本中查到以上信息。然后按照上面的规定，首先用连线把连接板上的A字母和L字母，P字母和R字母……连接起来；然后把2号转子放在ENIGMA的第一个转子位置上，把3号转子放在第二个位置上，把1号转子放在第三个位置上；最后，他调整转子的方向（从照片上可以看到每个转子的边上都刻着一圈字母用来显示转子所处的方向），使得三个转子上的字母Q、C和W分别朝上。在接收信息的另一方，操作员也进行同样的准备（他也有一本同样的密钥本），就可以进行收信解码的工作了。

调整好ENIGMA，现在操作员可以开始对明文加密了。但是我们看到每天只有一个密钥，如果这一天的几百封电报都以这个密钥加密发送的话，暗中截听信号的敌方就会取得大量的以同一密钥加密的信息，这对保密工作来说不是个好兆头。我们记得在简单替换密码的情况下，如果密码分析专家能得到大量的密文，就可以使用统计方法将其破解。

尽管不知道对ENIGMA是否可以采用类似的统计方法，德国人还是留了个心眼。他们决定在按当日密钥调整好ENIGMA机后并不直接加密要发送的明文。相反地，首先发送的是一个新的密钥。连接板的连线顺序和转子的顺序并不改变，和当日通用的密钥相同；想反地，转子的初始方向将被改变。操作员首先按照上面所说的方法按当日密钥调整好NIGMA，然后随机地选择三个字母，比如说PGH。他把PGH在键盘上连打两遍，加密为比如说KIVBJE（注意到两次PGH被加密为不同的形式，第一次KIV，第二次BJE，这正是ENIGMA的特点，它是一种复式替换密码）。然后他把KIVBJE记在电文的最前面。接着他重新调整三个转子的初始方向到PGH，然后才正式对明文加密。

用这种方法每一条电文都有属于自己的三个表示转子初始方向的密钥。把密钥输入两遍是为了防止偶然的发报或者接收错误，起着纠错的作用。收报一方在按当日密钥调整好ENIGMA机后，先输入密文的头六个字母KIVBJE，解密得到PGHPGH，于是确认没有错误。然后把三个转子的初始方向调整到PGH，接着就可以正式解密其余的密文了。

如果不使用对每条电文都不同的密钥，那么每天很可能总共会有几千条电文也就是几百万个字母的消息以同一个密钥加密。而采用每条电文都有自己的密钥这个方法后，当日密钥所加密的就是很少的几万个字母，而且这些字母都是随机选取，和有意义的电文性质不同，不可能用统计方法破译。

乍一看来这种方法无懈可击。可是波兰人铁了心，必须在这厚厚的护甲上撕出一个口子来。

此以前，密码分析人员通常是语言天才，精通对语言方面特征的分析。但是既然ENIGMA是一种机械加密装置，波兰总参二局密码处就考虑到，是否一个具有科学头脑的人更适合于它的破译工作呢？  
　　1929年1月，波兹南大学数学系主任兹德齐斯罗·克里格罗夫斯基(Zdzislaw Krygowski)教授开列了一张系里最优秀的数学家的名单，在这张名单上，有以后被称为密码研究“波兰三杰”的马里安·雷杰夫斯基(Marian Rejewski)，杰尔兹·罗佐基(Jerzy  Rozycki)和亨里克·佐加尔斯基(Henryk Zygalski)。波兹南大学并非当时波兰最有名的大学，但是它地处波兰南部，那里直到1918年还是德国领土，所以所有这些数学家都能讲流利的德语。

在三位被密码局招聘的数学家中，雷杰夫斯基的表现最为出色。当年他是个架着一副近视眼镜，脸上略带羞色的二十三岁小伙子。他的在大学里学的专业是统计学，打算以后去干保险业行当，也许在此之前他从未想到会在密码分析方面大展身手。在经过短期的密码分析训练后，他把所有的精力都投入到破解ENIGMA的工作中去。  
　　雷杰夫斯基深知“重复乃密码大敌”。在ENIGMA密码中，最明显的重复莫过于每条电文最开始的那六个字母——它由三个字母的密钥重复两次加密而成。德国人没有想到这里会是看似固若金汤的ENIGMA防线的弱点。

德方每封密文最开始的六个字母，是此信密钥的三个字母重复两遍，由当日密钥加密而成。比如说这封信的密钥是ULJ（这是开始加密明文时由操作员临时随机选取的），那么操作员首先用当日通用的密钥加密ULJULJ，得到六个字母的加密后序列，比如说PEFNWZ，然后再用ULJ来作为密钥加密正文，最后把PEFNWZ放在加密后的正文前，一起用电报发给收信方。  
　　雷杰夫斯基每天都会收到一大堆截获的德国电报，所以一天中可以得到许多这样的六个字母串，它们都由同一个当日密钥加密而成。

对于每封电报来说，它的第一个字母和第四个字母都是由同一个字母加密而来，同样地第二和第五个字母以及第三和第六个字母也是分别由同一个字母加密而来。

从L和R是由同一个字母加密而来这点，雷杰夫斯基就有了判断转子的初始位置的一条线索。当转子处于这个初始位置时，字母L和R在某种意义下具有紧密的联系。每天截获的大量电文能够给出许多这样的紧密联系，从而使雷杰夫斯基最终能够判断出转子的初始位置。

波兰人按照汉斯-提罗·施密特提供的情报复制出了ENIGMA样机。到了1934年，他们有了十几台波兰造ENIGMA。雷杰夫斯基和他的同事们每天都在ENIGMA前工作，一个接一个地试验转子的不同位置和初始方向，然后产生相应的字母对应表并构造相应的字母循环圈，并把它们记录下来。

当对所有105456种转子位置和初始方向都编好记录以后，破译ENIGMA生成的密文就比较容易了。首先要取得足够的当日电文来构造字母对应表并且写出字母循环圈；然后根据循环圈的数目和它们的长度从记录表中检索出相对应的转子位置和初始方向：这就是当日的密钥（连接板的情况还未知）。循环圈的个数和长度可以看作是这个密钥的“指纹”——通过建立密钥“指纹”档案，雷杰夫斯基就能及时地把当天的密钥找出来。通过分离转子的状态和连接板的状态，雷杰夫斯基大大简化了破译ENIGMA的工作。建立这样一个档案花了整整一年时间，工作相当艰苦，有时工作人员的手指都被磨出血来。

在雷杰夫斯基和他的同事的努力下，波兰情报部门在后来的几年里成功地掌握了大量德国方面的情报。据估计，在1933年1月到1939年9月这六年多的时间里，波兰方面一共破译了近十万条德方的消息，其中最重要的有德国在包括苏台德地区兵力重新部署的情报，这对波兰的安全是极大的威胁。对ENIGMA的破解即便在总参二局领导层内部也属最高机密，军官们会收到标有“维奇尔”(Wicher，破译ENIGMA行动的代号)的情报，他们被告知这些情报绝对可靠，但来源绝密。1934年，纳粹德国元帅赫尔曼·戈林访问华沙，他怎么也没有怀疑波兰人已经掌握了他的机密。当他和德国高级官员向位处波兰密码处附近的无名战士墓献花圈时，雷杰夫斯基正透过办公室的窗子望着他们，心中为自己能知道他们最机密的通讯而狂喜不已。

当德国人对ENIGMA转子连线作出一点改动以后，花了一年功夫建立起来的密钥“指纹”档案就变得毫无用处了。但是雷杰夫斯基和罗佐基有了一个更好的主意。他们在ENIGMA的基础上设计了一台能自动验证所有26\*26\*26=17576个转子方向的机器，为了同时试验三个转子的所有可能位置的排列，就需要6台同样的机器（这样就可以试遍所有的17576\*6=105456种转子位置和初始方向）。所有这6台ENIGMA和为使它们协作的其他器材组成了一整个大约一米高的机器，能在两小时内找出当日密钥。罗佐基把它取名为“炸弹”(La Bomba)，可能是因为它运转起来震耳欲聋的声响；不过也有人传说，制造这样一台机器的主意是雷杰夫斯基一次在饭店里吃叫做“炸弹”的冰淇淋时想到的。无论如何，“炸弹”实现了密码分析机械化，它是对ENIGMA机械加密的一种很自然的回应手段。

波兰密码局的破译能力在1938年的十二月达到了极限，德国人加强了ENIGMA的加密能力。每台ENIGMA机增加了两个可供选择的转子。原来三个转子不同的排列方式有6种，现在从五个转子中选取三个装入机器中的方式达到了5\*4\*3=60种。这就意味着要达到原来的效率，“炸弹”中必须有60台机器同时运转，而不是原来的6台。建造这样一台“炸弹”的价格是密码处总预算的十五倍！在1939年一月，连接板上的连线又由六根增加到十根，这样就只剩6个字母不会被交换。密钥的总数达到了一万五千九百亿亿个，是原来的一万五千九百倍。

虽然波兰数学家们成功地推断出了第四和第五个转子中的连线状态，雷杰夫斯基也证明了ENIGMA并非象德国人或盟国密码分析专家想象的那样坚不可破，但是他的方法终于也不适用了。这时兰杰少校应该从他的抽屉里拿出施密特提供的密码本来——但是正是德国人增加转子个数的时候，施密特停止了和法国情报部门的接头。七年中施密特不断地提供给波兰人能靠自己的力量破译的密钥，现在波兰人急需这些密钥，他们却再也搞不到了。

波兰被入侵前夕，波兰决定把直到现在还对盟国保密的关于ENIGMA的破译方法告诉盟国同行，以便在波兰遭到入侵后，拥有更大人力物力财力的盟国还可以继续对雷杰夫斯基的方法进行研究。8月19日，在横渡英吉利海峡的渡船上有两位看似平常的旅客：英国作家沙夏·居特里(Sacha Guitry)和他的太太女演员依弗娜·普林坦普斯(Yvonne Printemps)。但是在他们的旅行箱里却藏着当时英国最高的机密：一台波兰制造的ENIGMA。为了避开无所不在的德国间谍的耳目，ENIGMA就这样来到了英国，在那里等待它的将是它的彻底灭亡。

英国数学家和其他密码分析人员很快就掌握了波兰人进攻ENIGMA的技巧和方法。布莱切利公园拥有比波兰密码处多得多的人员和资金，所以足以对付由于德国人对ENIGMA的改动而增加到原来十倍的破译工作量。和在波兰密码处的情景一样，布莱切利公园的男女们日夜紧张工作，为的就是找到德国人当天的密钥。一到午夜，转子和连线板的设置就会变动，一切又要重新开始。

在掌握了波兰人对付ENIGMA的手段后，英国密码分析专家也开始摸索出自己独特的方法。在正式用“炸弹”开始系统搜索当日密钥以前，他们总要试一遍“投机取巧”的门道。根据德军通讯的规定，每一条电文都要随机选择三个不同的字母组合，但是在激战之时，德军指挥官经常顾不上“随机”，往往在键盘上敲上三个相邻的字母了事，比方说DFG或者VBN，有时甚至重复使用某三个字母的组合来当密钥。英国密码分析专家把这样的密钥叫“西尔丝”(cillies)，即三字母组合CIL的读音，大概来源于哪位倒霉德国军官的女友的名字。

“西尔丝”并非ENIGMA本身的弱点，而是ENIGMA使用者的弱点。另一种更为严重的人为使用错误是密钥本编制者对密钥使用过分严格的规定。为了强调密钥的不可预见性，他们规定每天在三个放置转子的位置上，不得有和昨天放在此位置上相同的转子。比如说每台ENIGMA机一共配备编号为1、2、3、4、5的五个转子，而前一天所使用的转子顺序为134，那么第二天可以使用例如215这样的转子顺序，但是214这样的顺序是不允许的，因为和前一天相比较，在第三个位置上都是4号转子。看起来这样交叉使用转子是个好主意，避免了象上面所说的重复使用某个密钥的过失，但是如果过分强调这一点，却会使英国密码分析专家的工作量减小一半，因为在开始分析当日密钥前，他们就可以把所有至少有一个转子处在前一日位置上的那些转子的排列排除在外了。德军密钥编制的另一条规定是，在连接板上不允许把两个相邻的字母连接起来。直觉似乎告诉人们不该使用这样简单的字母交换，但是这样的规则搞得太严格过了头，也就反而会帮对手的忙，对手根本就不用考虑这样的可能性了。  
　　在整个战争过程中，ENIGMA机被不断改善，所以这样的“投机取巧”也变得十分重要，密码分析专家可以通过对密钥的猜测来推断出密码机新的变动，从而相应地改善“炸弹”的设计，使用新的策略。

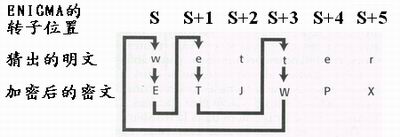
在布莱切利公园有一大群为破译ENIGMA作出了卓越贡献的人们。但是如果只能选择性地讲述一个人的功绩，那么这个人无论如何应该是阿兰·图灵(Alan Turing)。

1939年9月4日，就在首相张伯伦向德国宣战的第二天，图灵离开了剑桥，来到离布莱切利公园五公里的雪纳利布鲁克恩德(Shenley Brook End)居住。他每天骑自行车到布莱切利公园上班。因为患有对花粉过敏的鼻炎，图灵就常常戴个防毒面具骑车上班，招摇过市。  
　　在布莱切利公园里，每天他花一部分时间和其他人一样在小木屋里进行破译密码的工作，而另一些时间他就呆在被称为“智慧水箱”(Think Tank)，原来用来放水果的储藏室里。在那里密码分析专家思考在未来日子里有可能碰到的难题以及它们的解决方法。  
　　直到当时，对ENIGMA的破译都采用雷杰夫斯基的方法，即利用每条密文最开始重复的密钥。如果此电文的密钥为YGB，那么电文开头就是六个由YGBYGB加密而成的字母，德国人以此来预防可能的传送错误。但是这是ENIGMA使用中的一个重大弱点，德国人很可能会发觉这一点并取消这种重复，这样就会使英国密码分析专家的破译手段变得毫无用处。图灵的任务就是要找到另一种不必利用重复密钥的破译方法。

在分析了以前大量德国电文后，图灵发现许多电报有相当固定的格式，他可以根据电文发出的时间、发信人、收信人这些无关于电文内容的信息来推断出一部分电文的内容。比方说，德国人每天的天气预报总在早上六点左右发出，要是在六点零五分截获了一份德国电报，它里面八成有Wetter这个词，也就是德文中的“天气”。根据在此之前德国人天气预报电文的死板格式，图灵甚至能相当准确地知道这个词具体在密文的哪个位置。这就使得图灵想到了用“候选单词”这一方法来破译ENIGMA电文，在英语中，图灵把这些“候选单词”叫做Cribs。

如果在一篇密文中，图灵知道Wetter这个词被加密成了ETJWPX，那么剩下的任务就是要找到将Wetter加密成ETJWPX的初始设置。如果采用一个一个试过去的暴力破解法，那就会碰到1590亿种组合这个大问题。但是雷杰夫斯基的天才思想告诉图灵，必须把转子方向变化造成的问题和连接板交换字母造成的问题分开来考虑。如果他能够象雷杰夫斯基那样发现在Cribs中某些不随连接板上连线方式变化的特性，他就可以最多只用尝试1054560次（60种转子放置方法乘以17576种转子初始方向）便可找到正确的转子设置。

图灵找到了这样的特性。这是一种和雷杰夫斯基发现的循环字母圈类似的东西，只不过这回和重复的密钥没有关系，却是基于候选单词。假设图灵已经正确地猜到wetter被加密成了ETJWPX，这里就存在着一个字母循环圈：



图灵并不清楚在密文中出现这个候选单词时的转子状态，但是假设他猜对了这个候选单词，把这个候选单词起始时转子的方向记为S，那么在此时ENIGMA把w加密成了E；然后转子转到下一个方向，就是S+1，ENIGMA把e加密成T；在方向S+2上一个不属于这个循环的字母被加密了，这个我们暂且不去管它；接下来在方向S+3，ENIGMA把t加密为W。

这看起来好像还是让人摸不着头脑，但是图灵想的办法很巧妙，因为在这个字母循环圈里有3个字母，所以他想像如果用3台ENIGMA同时加密这个候选单词，会发生些什么事。三台ENIGMA的初始设置除了转子方向外完全一样，第一台ENIGMA机的转子初始方向被定为原来的S，而第二台ENIGMA机的转子初始方向却是S+1，第三台的转子初始方向是S+3。当然一开始图灵根本就不知道这个S具体是什么（要是知道的话密码也就破译出来了），所以只能一个一个方向地试。大家可能会问，那为什么需要3台ENIGMA呢？只要在第一台上我们发现了一个把wetter加密成ETJWPX的转子方向，不就找到了密码吗？

这就要考虑连接板的问题。上面我们说过，如果只用一台ENIGMA来试所有的密码，我们要试的就不仅仅是所有的转子方向，而且还要考虑所有的连接板上的连线方向，那个数目是1590亿种。图灵的绝妙主意就是用3台ENIGMA把连接板上连线的效应抵消掉！这样他就只要考虑1054560种转子方向就可以了。

图灵把三台ENIGMA的显示器按下图的方式连接起来，也就是说把第一台ENIGMA显示器上的E和第二台ENIGMA显示器上的e连起来，又把第二台上的T和第三台上的t连起来，最后把第三台上的W和第一台上的w连起来（注意ENIGMA上字母没有大小写之分，这里我们只是用大小写来区别密文和明文）。下面的解释听起来稍微有一点复杂，最好对照着上面的图来读。假设连接板上有关的交换字母的连线是下面这样的（三台ENIGMA机上的都一样）

E←→L1

T←→L2

W←→L3

当然这里的L1、L2和L3都还是未知的。

现在假设字母w被输入第一台ENIGMA，它先通过连接板变成了L3，然后通过三个转子经过反射器，再通过三个转子返回连接板；因为我们根据候选单词知道w此时会被加密成E，所以没有经过接线板前它一定是和E对应的L1；L1经过接线板变成E后，直接成了第二台ENIGMA的输入。提醒一下，第二台ENIGMA的转子方向是S+1，所以根据候选单词知道e此时会被加密成T，我们来看看具体是怎么回事。从第一台ENIGMA来的e通过连接板变成了L1，再通过转子和反射器回来变成了连接板上和字母T对应的L2；通过连接板后变成了T，然后这个T又变成第三台ENIGMA机上的输入t。第三台ENIGMA机的转子方向是S+3，这个传送过来的t会被加密成E，具体的情况和上面第一第二台上的类似。我们发现现在三台ENIGMA机的线路组成了一个闭合回路，如果在里面加上一个灯泡，它就会亮起来。这个闭合回路事实上就是那个字母循环圈的形象化。

稍微思考一下就可以看到，无论连接板上的连线实际如何（也就是说无论L1、L2和L3实际上是什么），只要转子方向凑对了，这个闭合回路就会形成（当然如果有闭合回路形成不等于这个方向就一定是正确的，但是这样的情况很少，用手工就可以把正确的方向从中选出）。就这样，连接板上的连线效应被消除了。找到了转子的初始方向S，当然还要找到连接板上的连线，才能最终找到完整的密钥，但是这就相当简单了，这只是一个简单替换密码。如果在一台普通的ENIGMA上不接连线板，调整好找到的转子方向，键入密文ETJWPX，出来的明文成了tewwer，我们马上就知道w和t被交换了。键入密文的其他部分可以猜出其他字母的交换状况。

把候选单词，字母循环圈和用线路连接起来的多台ENIGMA机构成了密码分析的强大武器。而只有图灵，这个数学虚拟机器的发明人，才能有这样的想像力。图灵对ENIGMA的破译方法完全是纯数学和理论性的，他为此写了一篇著名的论文，在http://frode.home.cern.ch/frode/crypto/Turing/你可以读到这篇论文的一部分。但是他的理论研究已经完全可以让工程师来实际造出这样一台机器了。

1940年3月14日第一台“炸弹”运抵布莱切利公园。可是它运行得太慢，有时要一个星期才找得到一个密钥。工程师们花了很大的努力来改善“炸弹”的设计，然后开始制造新的“炸弹”，这又花了四个月时间。但是在5月10日，最令英国密码分析专家担心的事情发生了，德国人改变了密码传递规则，他们的密钥不再重复，这使得布莱切利公园破译的电文量急剧下降。幸运的是，改进以后的“炸弹”在8月8日到达，而且这次它运行得很好。在接下来的八个月里，十五台新“炸弹”在布莱切利公园里轰然作响。一般上一台“炸弹”可以在一小时里找到一个密钥。

但是并非有了“炸弹”就万事大吉了。在让它运行之前还有许多困难要克服。比如说使用“炸弹”前先要找到一个候选单词。但是密码分析人员不能保证他猜的词一定在电报的明文中；就算猜对了，要把候选单词所在的位置正确地找出来也不是一件容易的事情，很有可能他猜到了电文中的一整句话，但是把这句话的位置搞错了，那“炸弹”也就白白运行了。密码分析人员找到了一些技巧，比如说，他知道下面“wetterbullsechs”一定在电文明文中，但是具体位置却只知道个大概。于是他猜想密文和明文的对应是：

候选单词：wetterbullsechs

密文：IPRENLWKMJJSXCPLEJWQ

在介绍ENIGMA的构造时我们知道，由于反射器的作用，一个字母从来也不会被加密成它本身。所以上面的候选单词所对应的位置一定是不对的，因为第二个字母e被对应到E上了。解决方法可以是慢慢地移动候选单词，看看是否每个字母都对应一个和自己不同的字母。比如把上面例子中的候选单词向左移动一位，变成

候选单词： wetterbullsechs

密文：IPRENLWKMJJSXCPLEJWQ

现在就符合要求了，所以此时才可以让“炸弹”去试试它的威力。

在前面的记述中读者似乎会有这样一种感觉，所有的ENIGMA机都是一样的，而密码分析人员在找到破译的方法以后每天按部就班地进行破译工作。但事实上，德军内部有好几个不同的通讯网络，比如说，在北非的德军就有自己的一套通讯网，他们的密码本和在欧洲的德军网络不同，德国空军也有自己的通讯网络。某些通讯网络的保密性要强于其他的，而德国海军通讯网的保密性是最强的，它使用的ENIGMA机是经过强化特制的，它有八个转子可供选择，这样转子的初始位置数就几乎是五个转子情况的六倍，于是布莱切利公园破译它所需要花费的时间也几乎是普通情况的六倍。另外海军用的ENIGMA机的反射器是可以转动的，于是密钥的可能性就是原来的二十六倍。有一些海军型ENIGMA机甚至有四个转子。德国海军为了加强通讯保密性，甚至取消使用固定的信件格式，这样就使图灵的“候选单词”法极难被使用。另外它的每条电文的密钥也以一种不同于平常的方式传送。

德国空军和陆军的ENIGMA密文都能比较顺利地被破译，但是德国海军的这些保密措施使得英国密码分析人员在破译电文时遇到极大的困难才取得了成功。

在二次大战盟军的胜利中，对布莱切利公园是否起了决定性的作用这点，历史学家自然有大量争议，但是毫无疑问的是，布莱切利公园的密码分析专家大大地加快了战争的进程。这在大西洋战役的历史中尤其明显。如果没有破译，德军就能在大西洋上保持一支强大的潜艇群和反应能力，相反地盟军必须付出巨大的人命和财力的代价来建造新的船只和保持运输能力。历史学家估计盟军的登陆计划会被推延到次年，而哈里·辛斯利则认为，在此情况下，战争很可能要到1948年，而不是在1945年，才能结束。如果是这样，希特勒将能够更大规模地使用V1和V2飞弹对整个英国南部进行轰炸。