破译英格玛密码

——马里安·乔耶夫斯基的密码人生

【译】千素芳

【著】莱斯泽克·格拉乌斯基（波兰）

Decoding Enigma

wydawnictwo adam marszałek

时代出版传媒股份有限公司
安徽科学技术出版社

破译英格玛密码

Decoding Enigma

——马里安·乔耶夫斯基的密码人生

【著】莱斯泽克·格拉乌斯基（波兰）
【译】于素芳

wydawnictwo adam marszałek
ARTTIME 时代出版
时代出版传媒股份有限公司
安徽科学技术出版社

[皖] 版贸登记号:1210867

图书在版编目(CIP)数据

破译英格玛密码/(波)格拉乌斯基著;于素芳译.
—合肥:安徽科学技术出版社,2013.6
ISBN 978-7-5337-5588-1

Ⅰ.①破… Ⅱ.①格…②于… Ⅲ.①密码-历史-普及读物 Ⅳ.TN918.1-091

中国版本图书馆CIP数据核字(2012)第256543号

Original Publisher: Adam Marszalek Publishing House

破译英格玛密码 (波)格拉乌斯基 著 于素芳 译

出 版 人:黄和平 选题策划:何迅文 责任编辑:王 宜
责任校对:盛 东 责任印制:梁东兵 封面设计:王 艳
出版发行:时代出版传媒股份有限公司 http://www.press-mart.com
安徽科学技术出版社 http://www.ahstp.net
(合肥市政务文化新区翡翠路1118号出版传媒广场,邮编:230071)
电话:(0551)63533330
印 制:合肥创新印务有限公司 电话:(0551)64456946
(如发现印装质量问题,影响阅读,请与印刷厂商联系调换)

开本:880×1230 1/32 印张:4.75 字数:136千
版次:2013年6月第1版 2013年6月第1次印刷

ISBN 978-7-5337-5588-1 定价:12.00元

译 者 序

这是一本有关密码学发展历史的著作。在书中，作者莱斯泽克·格拉乌斯基以主人公马里安·雷耶夫斯基破译英格玛密码(英格玛)的过程为主线，梳理了密码学发展的历史。书中详细讲解了从单表换位密码到多表换位密码，包括格栅密码、斯巴达天书、弗莱斯纳尔模板、德国简单换位密码和德国复式替换密码等的具体运算过程；从人工加密到用英格玛加密机等加密仪器进行加密，详细展示了密码学发展的过程，为密码学研究者及爱好者提供了翔实而具体的历史资料。

本书披露了第二次世界大战鲜为人知的历史内幕。三位波兰密码学家——马里安·雷耶夫斯基、耶日·鲁日茨基和亨里克·齐加尔斯基为破译德国英格玛 密码作出了巨大贡献。马里安·雷耶夫斯基发明了密码分析仪器“炸弹”，亨里克·齐加尔斯基创制出用于密码分析的钻孔表格。在皮瑞会议上，这两大发明连同波兰人仿制的英格玛加密机都拱手送给了英法盟国。波兰人使二战缩短了至少两年，拯救了数百万人的生命，使德国在战争一开始就注定了失败。但是这些二战的功臣并没有得到应有的承认与荣誉，皮瑞会议的直接参与者——法国的古斯塔夫·贝特朗将军在其著作《英格玛：1939—1945 年战争中最大的谜》中对他们只字未提。英国安德鲁王子虽曾向波兰人表示谢意——但这已是后话，而此前英国对波兰人破译英格玛密码一事一直是三缄其口；而布莱奇利庄园——它可是在波兰密码学家们拱手相送的资料基础上发展起来的，对波兰密码学家们更是防备有加。本书对这些历史真相进行了细致的披露。

这是一位有着伟大品格却又平凡的波兰密码学家——现代密码

学之父马里安·雷耶夫斯基不为世人所知的人生故事。他聪明好学，热衷于密码学分析，执著追求，终身不曾放弃。在二战残酷的历史大背景中，他曾遭遇国破家亡，受到盟国同行的压制、排挤，经受了巨大的精神煎熬，但却从未放弃过密码学研究。从二战的赫赫功臣到一名普普通通的公司小职员，他坚守自己的人生信仰，终身洁身自好，待人谦虚温和。当我们这些现代读者阅读雷耶夫斯基的故事时，他在残酷的现实面前所表现出的坚忍也许会激发我们很多的思考：究竟什么是人生的意义？人的一生中什么更重要，态度还是运气？面对压力，我们是扭曲变形还是勇往直前？相信你会从书中找到答案，感受到一种久违的生命力量。

这是一本介绍密码学知识的读物。原作语言深入浅出，亦庄亦谐，娓娓道来，融知识性于平实的语言中。让人不由感叹：密码学很神秘，但绝不艰深。翻译时，译者本着体现原作这种风格的思想，在忠实再现原作的基础上尽量用普通读者喜闻乐见的表达方式传译，以期译文读者能如原文读者一样感受到该书的魅力。

书中提到了很多密码学术语，对于这些术语的翻译，译者大量参阅国内密码学界的已有译著。有通用译法的则采用通用译法，如“Session key”就采用通用译法，译成“会话密钥”，而不是“季密钥”等；对于没有通用译法的，则根据术语本身词义结合语言环境进行翻译，如“Daily characteristics ”译成“每日特征词”等。对专有名词的翻译，有通用译法的则采用通用译法，没有通用译法的则采用音译法。

于素芳

前　言

让我来问问我们的同胞，在反对纳粹德国战争所取得的胜利中波兰人作出的最伟大贡献是什么？也许有人会说是波兰飞行员参加了不列颠之战，有人会说是波兰人攻占了蒙特卡西诺（Monte Cassino）要塞，还有人可能会说是陆军情报部门捕获了V-2实验火箭并把它移交给了英国。我们甚至还听说过把对德战争的胜利归功于波兰某著名电视剧中的4个坦克兵和一条狗，这4个人开着一辆苏联坦克把纳粹党徒从提拉古不纳（Trigubova）一直驱赶到布兰顿布鲁格（Brandenbrug）大门。而事实上，在世界反法西斯战争中波兰人的主要贡献根本不是这些。波兰人的贡献是至少把战争缩短了两年，拯救了数百万人的生命，并且使纳粹德国无法制造从而不可能在战争中使用原子弹。

在二战中，各军事行动中心和决策部门主要使用无线电下达命令、传递信息。比起直接送信的方法，如用信鸽送信，无线电的传输速度要快捷得多，但同时它又比较容易被截获，无论是在战时还是在和平时期，外交、商业和军事领域的通信在发送前都会加密，这样即便是被敌方截获，他们也无法读取。这也是为什么读取加密信息的技巧，或者说破解密码，在外交领域和情报部门之间的斗争中至关重要，从最早的文字出现以来情况莫不如此。早在两次世界大战期间，波兰密码学家们就开始尝试破解德国人用一种叫做“英格玛”的电汽加密机加密的密码。如果没有这些密码学家们的智慧和努力，或许大西洋战争和不列颠之战都不会取得胜利。

波兰密码处最早意识到了数学在破解复杂密码中的作用，并率先雇用接受过专门数学教育的数学家们从事解密工作。这些数学家

们在破解密码中取得了突破性进展：不仅复制出了密码机，而且破解了解密的关键一环，即所谓的信息密钥。如果我们的密码学家们没有破解出寻找信息密钥的方法，那么即便是我们有一台德国的密码机也无济于事。1932 年底，年轻的数学家马里安·雷耶夫斯基在费尽周折破解出信息密钥后，很快就仿制出了一台密码机。首先，他根据密码机的工作原理，用纸加笔的方法破译出了截获的密电，之后不久在华沙又仿制出了好几台德国英格玛加密机。当时，还没有人能破译出用军用英格玛加密机加密的密电，华沙造密码机是根据马里安·雷耶夫斯基提供的图纸制造的，尽管包括他在内，所有参与制造者都没有见过英格玛军用机原型，制造机器所用的图纸是根据密电分析绘制出来的。在 20 世纪 30 年代，也就是在二战爆发前夕，波兰密码学家们又制造出一种用英格玛处理的加密信息的破译机器。这两种机器连同制造图纸和使用说明，在二战爆发前几周他们都拱手送给了盟国。

从德军入侵波兰到占领法国全境，波兰、法国、西班牙和英国的密码学家们一直都在奋力工作，试图破译密钥从而读取德军密电。英国人在波兰密码学家们所取得成就的基础上，掌握了密码的破译方法，并最终认识到要破解这些现代密码，仅仅靠善于猜测纵横字谜，拥有高超的语言能力（指语言学方法）而对数理统计仅一知半解的情况已是远远不够了。于是英国人在离伦敦不远的布莱奇利庄园（Bletchley）建立起了自己的密码破译机构，开始雇用数学家从事密码分析工作。

在战时，布莱奇利庄园的雇员从最初几十人猛增到 10 000 人。由于破译了用英格玛 加密的报告和命令，并通过无线电及时传递给了盟国，才使得盟国生擒德军潜艇“海狼号”。美国有一支商船先是开往英国，后又转道苏联，途中就曾遭到过该潜艇的袭击。

德国大力筹备空军，做好了入侵不列颠岛的准备（即“海狮行动”），以期一举摧毁英国防护。德国空军元帅赫尔曼·戈林（Hermann Goering）原计划于 1940 年 8 月 8 日发动进攻。他并不知道自己通过无线电传输给 3 个舰队的作战命令，即要求他们实施“鹰击行动”

的密电已被英国信号情报部门截获，而且很快就被布莱奇利庄园的密码学家们破解。英国绝密情报部门又在第一时间把破译的密电转呈给英国首相丘吉尔和空军元帅道丁(Dowding)。绝密信息专家们就在斯坦莫尔(Stanmore)的地下防空洞里工作，绝密情报部门和布莱奇利庄园之间用电传打印机相互传递信息。8月15日，德国人终于盼来了晴好天气，他们随即发动了对英国的进攻。戈林用无线电发布了作战命令，而在同一时间英国信号情报部门就截获了这些密电，再经由布莱奇利庄园转交给绝密情报部门。负责英国防卫的元帅道丁立刻指示英国皇家空军飞往最需要的战场——他当然知道哪些地方最需要支援，这多亏了来自绝密情报部门破译的密电信息。道丁不会坐视德军挑衅英国皇家空军，更不会让皇家空军像戈林希望的那样直接卷入战争。不列颠空战于9月中旬结束，德军在9月15日投下了最后一颗炸弹。由于英国人截获了德军信息，德军此举对英国来说是意料之中的事。因此德军损失惨重，不得不放弃以"闪电战"入侵英国的作战计划。通过被破译的希特勒命令，丘吉尔甚至提前就知道德军取消了闪电行动。

德国人发现用英格玛 加密的信息已经被敌方破解了吗？战后历史研究表明，对此他们毫不知晓。原因在于所有知情的军事指挥者们从未透露他们和盟军共享过破译的德国密电。

丘吉尔为了让德国相信英格玛加密机坚不可摧，竟然故意让纳粹党徒炸毁英国的一座大城市。德国人相当自信，认为其他国家的密码学家们无论怎样努力，都无法破解自己的密码，要知道仅仅破译一条用英格玛加密的密电就需要几十亿次的尝试。不过，德国人并没有因此止步，而是不断改进原先的加密方法、密钥和传输方法。在20世纪20年代末，德国首先在海军中引进机器加密法，然后在全军和情报部门推广，而就在此时他们有一个纰漏被波兰密码学家们发现了。原来德国人在发送明文时还随同发送经过两次加密处理的会话密钥(Session key，用日密钥连续加密两次)。还有英格玛报务员所犯的其他错误同样也帮助波兰密码学家们更容易地破解出英格玛加密机的构造。因此，当德国启用更安全的传递密钥的方法时已为

时太晚。马里安·雷耶夫斯基破译加密的会话密钥时，借用了密码替代中的字母循环理论，最终找到了破解日密钥的方法，复制出了英格玛机器，尽管他从来没见过这种加密机原型。所有这些成就，马里安·雷耶夫斯基都是在1932年末至1933年初取得的。尽管后来德国人进一步改进了加密方法，使破解工作更加艰难，但是都难不倒布莱奇利庄园的英国密码学家们。他们胸有成竹地知道该怎么做，因为他们可以凭借自己国家里一个不起眼的密码分析中心所首创的密码分析法。以前，他们可是对这个小小的密码分析中心嗤之以鼻的。

如果你认为波兰数学家们——即密码学家们工作的环境安逸、静谧的话，那你可就大错特错了。二战伊始，他们就一直在不断地搬迁，在躲躲藏藏中工作和生活，甚至还多次穿越国界。他们被迫与家人分离，心里充满牵挂，为家人的安全担忧，而且还要在陌生的国度里顶着巨大的压力不停地工作。

三位波兰数学家中的耶日·鲁日茨基(Jerzy Różycki)死于客轮沉没，另一位亨里克·齐加尔斯基(Henryk Zygalski)战争结束后再也没有回波兰，而本书主人公马里安·雷耶夫斯基却回到了祖国。卡洛尔·格维多·兰杰(Karol Gwido Langer)中校、玛克斯米廉(Maksymilian)少校，以及工程师安东尼·帕鲁斯(Antoni Palluth)、爱德华·弗克孜依恩斯基(Edward Fokczyński)和卡齐米日·加察(Kazimierz Gaca)在穿越法(国)西(班牙)边境时被德国人抓获。德国人并不知道他们是波兰反情报部门的军官和工程师，因此把他们全都关进了集中营。安东尼·帕鲁斯和爱德华·弗克孜依恩斯基被关进了位于萨克森豪森-奥兰尼恩堡(Sachsenhausen—Oranienburg)的集中营。在盟军飞机轰炸集中营时，两人不幸身亡。

令人惊讶的是，直到20世纪70年代末，只有极少数与二战盟军反情报部门有渊源的人知道破解英格玛加密机以及破译德国密电的事。波兰人则认为他们必须保持沉默，因为他们在刚加入反情报部门时曾宣誓要保守秘密。在二战的最后阶段，英国人缴获了德国的英格玛加密机，战后全部廉价卖给了新兴的后殖民国家。至于英国人为什么不愿透露自己是怎样知道破解密码方法的，原因已无须

多言。

英国的弗雷德里克·W. 温特伯(Frederick W. Winterbotham)和法国情报部门官员古斯塔夫·贝特朗(Gustave Bertrand)率先打破了围绕英格玛密码的缄默。古斯塔夫·贝特朗曾被德军抓获,但侥幸存活下来。在20世纪30年代,弗雷德里克·W. 温特伯曾是英国情报部门的间谍,向英国提供了大量的有关德国空军的信息。当意识到可能会暴露身份而被捕时,他离开德国来到了英国,建立起一家解密机构,并组织撰写了一部描写密码情报部门工作的著作《超级机密》,1974年《超级机密》一书出版(由伦敦 Futura 出版社出版)。在书中,除了其他内容之外,他还报露了怎样破解用英格玛加密的德军密电。古斯塔夫·贝特朗创作了一个剧本《英格玛 超级机密备忘录》,之后还出版了著作《英格玛:1939—1945年战争中最大的谜》(1973年在巴黎出版)。波兰陆军退伍士兵约瑟夫·噶林斯基(Jozef Garlinski)博士出版了著作《截获密电——英格玛 战争的秘密》(1979年在伦敦出版)。就这样,破解英格玛 密码的历史终于浮出水面。马里安·雷耶夫斯基当时住在波兰,认识到时候已到,可以不再受誓约的束缚,于是开始披露自己破解英格玛密码的经历以及同事耶日·鲁日茨基和亨里克·齐加尔斯基所作的贡献。1979年,在少校瓦迪斯洛瓦·格扎斯祖克(Wladyslaw Kozaczuk)博士出版的专著《在英格玛密码界》里,马里安·雷耶夫斯基写的一篇文章《破解英格玛密码中排列理论的应用》出现在该书附录中。

英格玛秘密至此真相大白,接下来我们主要讲述波兰人在对纳粹斗争中所起的作用,讲述当然不会利用电影、书籍以及网络的资料。上面提到过的弗雷德里克·W. 温特伯尤其具有想象力。他曾虚构出一个具有非凡记忆力的波兰工人,声称自己曾在德国英格玛密码工厂工作过。根据温德博瑟姆的说法,该波兰工人记住了转子(rotor)内部的连线情况和英格玛密钥(key)的构成,然后又告诉了波兰情报部门。而对于这种荒唐的编造,许多电影和出版物竟然津津乐道,争相引用,但事实最终证明该说法纯属虚构。首先,从来没有过什么英格玛密码工厂。加密机是在德国反情报部门阿勃维尔

(Abwehra)的秘密车间组装的,而个别零件像测量仪等部件则是订单生产的,交给为数不多且彼此相隔甚远的工厂制造。其次,即便有英格玛复制品,如果密码学家们没有足够的专业知识和工具重建密钥的话,同样也解读不了用该加密机加密的密电。

毕竟,布莱奇利庄园的英国人不是白手起家,他们可以依据1939年7月24—26日皮瑞会谈时波兰人提供给他们的资料和信息,然而有些人竟然想把这一史实从史册中抹去。

安杰伊·斯基比亚克

作者的话

本书写给那些想了解波兰数学家、现代密码学之父马里安·雷耶夫斯基的生活与工作情况的人们。他运用排列理论复制出了德国英格玛密码机，并找到了破译用该机加密信息的方法，这种方法早在二战爆发之前就已经影响到了二战未来的发展趋向。关于破译英格玛密码对整个战争的影响，历史学家和军事理论家们仍然兴趣颇浓，争论不已。

* * *

本书与其他出版物的不同在于书中大量引用了马里安·雷耶夫斯基的原话，这些话语出现在其回忆录、批注、文章和为他人著述所做的附录文章当中。很显然这些资料需要进一步详细地解释，为了让专门从事密码学的数学专家之外的读者也能看懂，引文略有改动。

我参考并借用了所能找到的历史著作、报刊文章、由马里安·雷耶夫斯基女儿杰尼娜·雷耶夫斯基所提供的资料和从全国纪念研究所搜集来的资料。

* * *

感谢所有帮助完成本书的人们。尤其要感谢杰尼娜·丝路丝扎克女士——马里安·雷耶夫斯基的女儿，感谢她与我分享对其父亲的回忆。我在书中大量引用这些内容，目的是向读者展示真实的马里安·雷耶夫斯基和他所生活工作的那个年代和环境。我还要感谢丝路丝扎克女士，感谢她允许出版其父亲文章中的章节和刊登她的家庭影集中的照片。

感谢安杰伊·斯基比亚克(Andrzej Szybiak)博士，感谢他第一个通读了该书草稿，给予我非常有见地的建议并给该书写了前言。

我还要感谢他允许我使用由他翻译的未经正式出版的戴维·卡恩著作的部分章节。

感谢耶日·尤布那维卡(Jerzy Urbanovicz)教授、维托尔德·兹穆斯基(Witold Rzymowski)教授、亚采·马利茨基(Jacek Malicki)博士、维克托·巴特(Wiktor Bartol)博士和卡罗尔·戈斯基(Karol Górski),感谢他们审读了本书草稿,并不吝赐教,他们的建议在很大程度上影响了本书的成形。

感谢安杰依·沃基诺斯基(Andrzej Wojnowski)博士,感谢他帮助我撰写本书并把阿尔贝蒂的短文从意大利语译成波兰语。

感谢维托尔德·莫兹卡娃(Witold Mozgawa)博士和亚采·维尔特(Jacek Welter)博士,感谢他们帮助我整理马里安·雷耶夫斯基的有关文献和资料。

感谢我的女儿卡布里拉·格拉乌斯基(Gabriela Gralewska),感谢她帮助我合成电脑图像并帮我整理索引。

莱斯泽克·格拉乌斯基

目　录

引　言

序　曲

1927年底，也可能是1928年初，华沙海关收到一份来自第三帝国的急件。据海关申报单上填写的内容，该急件里装的是一台无线电设备。德国公司代表强烈要求不经海关审查直接将该急件寄返第三帝国，声称该急件邮错了。他们的再三要求引起了华沙海关官员的怀疑，海关官员立刻把此事上报波兰总参密码处，该机构对无线电设备领域中各种新奇的玩意儿颇感兴趣。当时正是星期日下午，密码处特派员有足够的时间把整个事件调查得一清二楚。邮件被小心翼翼地打开了，里面装的并不是什么无线电设备，而是一台密码机。一番精心检验之后，盒子又被封上了。

我们很容易就能猜出这台设备就是一台英格玛加密机，不过明显是一台商务用机，因为当时军用型机还没有投入使用。尽管这一事件并没有产生什么实质性的效果，但它却标志着密码处接触英格玛加密机的开始。之后，密码处所做的第一件事就是通过正常的商业交易，购得一台商用英格玛加密机。1928年7月5日，当德国用该加密机加密的信息电波第一次出现在波兰加密机上时，就被波兰无线电监测站的报务员截获了。密码处对德情报部门的波兰密码学家们受命破译该条信息。可惜的是，这项工作很快就不了了之。关于这件事，在密密麻麻写满了字的长达几页的报告中只是捎带提了一下，当然还提到了一台商用英格玛加密机。

波兰人用的商用英格玛加密机，市场上就能买到，结果证明该商用机无法用来破译截获的军事密电。用来对军事信息加密的机器与商用机截然不同，波兰人几次尝试复制军用英格玛加密机，但都以失