二战密码战

THE CIPHER BATTLE

“风语者”的窃窃私语，“月光”计划下的超级机密，中途岛的“AF”代号之谜……

破译终极密码，截取超级情报，让战争胜败惊天逆转！

荣耀二战

GLORY OF WORLD WAR Ⅱ

庄严

编著

哈尔滨出版社

HARBIN PUBLISHING HOUSE

庄严 编著

二战密码战

The Cipher Battle

荣耀二战
GLORY OF WORLD WAR II

哈尔滨出版社
HARBIN PUBLISHING HOUSE

图书在版编目（CIP）数据

二战密码战 / 庄严编著. —哈尔滨：哈尔滨出版社，2015.5
（荣耀二战）
ISBN 978-7-5484-1743-9

Ⅰ. ①二… Ⅱ. ①庄… Ⅲ. ①第二次世界大战-情报活动-通俗读物 Ⅳ. ①D526-49②K152-49

中国版本图书馆 CIP 数据核字（2015）第 031423 号

书　　名：二战密码战
作　　者：庄　严　编著
责任编辑：李金秋　韩金华
责任审校：李　战
装帧设计：先知传媒·郝强

出版发行：哈尔滨出版社（Harbin Publishing House）
社　　址：哈尔滨市松北区世坤路 738 号 9 号楼　　邮编：150028
经　　销：全国新华书店
印　　刷：辽宁星海彩色印刷有限公司
网　　址：www.hrbcbs.com　www.mifengniao.com
E - mail：hrbcbs@yeah.net
编辑版权热线：（0451）87900271　87900272
邮购热线：4006900345　（0451）87900345 或登录蜜蜂鸟网站购买
销售热线：（0451）87900201　87900202　87900203

开　　本：787mm × 1092mm　1 / 16　　印张：16　　字数：250 千字
版　　次：2015 年 5 月第 1 版
印　　次：2015 年 5 月第 1 次印刷
书　　号：ISBN 978-7-5484-1743-9
定　　价：29.80 元

凡购本社图书发现印装错误，请与本社印制部联系调换。服务热线：（0451）87900278
本社法律顾问：黑龙江佳鹏律师事务所

前言

Foreword

“密码”是最高智慧的搏杀，是最隐蔽的文字较量。

自从人类历史上产生文字开始，人们就开始利用文字来记录自己的“秘密”。利用某种文字或符号来记载特殊的事件往往可以起到“己知彼不知”的效果。目前发现最早的、具有实用价值的密码是公元前1500年左右的一份为陶器上釉工艺配方的密文。

随着人类文明的发展，由于其高度的保密性，“密码”逐渐被应用于军事通信领域，大大提高了作战的胜率。据记载，古罗马军团就开始使用密码进行军事通信，那时的密码系统只是简单的替换加密式，后世称之为“恺撒密码”。

到了二战时期，交战各国为了通信安全，各施所长。不断提高自己密码系统的安全程度，并不断对敌方的密码系统进行破译。在此期间，最著名的莫过于德国的恩尼格玛密码机。恩尼格玛密码机是当时世界上算法最复杂的密码机，除非人为失误，否则几乎不会被攻破。英、法、波三国在通力合作之下，最终成功发明了“炸弹”，以此来破译恩尼格玛密码机，从此盟军对德军的动态了如

指掌，大大加速了德国法西斯覆灭的进程。而“炸弹”的发明，也开启了电子计算机时代的大门，为人类走入信息化奠定了基础。

密码安全一向被视为国家的最高机密。在二战期间，有无数名数学家和后勤人员在为破译密码而辛勤劳动。丘吉尔称赞他们为“下了金蛋却从不叫唤的鹅”。正是他们的默默奉献，才有了前线的胜利，才挽救了前线无数士兵的生命。就像美海军陆战队一位军官说过的：“如果没有使用纳瓦霍语，美国永远无法攻克硫黄岛。”

如今，对“密码”的研究已经催生出一门独特的学科——密码学。密码学越来越受到各国军事界的高度重视。正所谓:“学人之长，为己所用;或用己之矛，攻敌之盾；知己知彼，方能百战不殆！”

为了帮助广大读者了解“密码”在战争中的重要作用，作者以第二次世界大战为背景，从无数的“密码战”中精选出 10 个战例，编写了本书。在二战这场人类的浩劫中，涌现出一个个默默无闻的幕后英雄，而由于情报工作的特殊性，他们的功绩多年后才为世人所知晓。

本书适合大众读者阅读，也是密码、数学、军事等领域的研究者和爱好者珍贵的参考读本。

目录

Contents

第一章　闪击波兰……1

夹在大国间的波兰，拥有全欧洲最先进的密码破译技术，对德国的军用密码有着较高的破译率。但是到了1928年，波兰人在与德国人的密码竞赛中败下阵来，这是怎么一回事？波兰人难道在坐以待毙吗？在1939年9月，德国闪击波兰之际，波兰的密码破译部门还没能做出正确的判断，这又是怎么一回事？德国人到底使用了什么方法来对付波兰人？

第二章　德国“狼群”的覆灭……29

在决定英国命运的大西洋战役中，德国“狼群”肆虐，大肆猎捕盟国货轮，这首要归功于“狼群”的秘密通信。也就是说，若想挽救大英帝国，必须击败“狼群”；若想击败“狼群”，必先破译“狼群”的秘密通信，这个任务最终落到了英国数学家图灵的肩上。图灵是怎样终结“狼群”的？中间又发生了哪些波折？

第三章　不列颠之战的“超级机密”.....49
随着英国密码破译技术的提高，不仅能够破译德国“狼群”的通信密码，更是破译了德国“鹰群”的通信密码。破译出来的信息，就是英国人的“超级机密”。不过生性多疑的希特勒渐渐怀疑“超级机密”的存在。他决定轰炸考文垂，来试探丘吉尔。丘吉尔如何接招？会升空拦截德国“鹰群”吗？

第四章　阿拉曼战役.....67
世人皆知，英军蒙哥马利元帅在阿拉曼击败了德军隆美尔元帅，成为二战北非战场的转折点。但鲜为人知的是，阿拉曼战役在开战前，胜负就已经确定了。隆美尔曾写道：“这一仗在打响前就由双方的军需官们决定了胜负。”蒙哥马利也说：“我们相当清楚敌人的实力，以及进攻的时间和方向。”这是怎么回事？阿拉曼战役的真相真的那么简单吗？

第五章　偷袭珍珠港.....93
日军偷袭珍珠港，日军联合舰队主力仅以 29 架飞机的代价就将美军太平洋舰队主力击毁于珍珠港内。日本为何如此大胆，竟以联合舰队主力为赌注，豪赌珍珠港？难道美国就一点动静也没察觉到吗？世界都在问美国此时在做什么。也许，被忽视的“魔术”才会告诉世人一切。

第六章　中途岛海战.....115
美国海军上将尼米兹曾说过：“中途岛的胜利实质上是情报的胜利。”那么美军是通过什么方法获得日军情报的呢？又是谁截获并破译了日军的密码？中途岛海战真的像某些人说的那样，是美军误打误撞大获全胜的，还是说美军精心设伏、巧妙布局，打日军一个措手不及呢？

第七章　猎杀山本五十六.....139

日本联合舰队司令山本五十六偷袭珍珠港，成为了美国人的眼中钉、肉中刺。1943年4月13日，一串神秘的电波从山本五十六的指挥所发往太平洋的日军前线。不久后，山本五十六就因为这串电波而葬送了性命。这是怎么回事？这串电波为什么能葬送了日军联合舰队司令山本的性命呢？

第八章　血战硫黄岛.....159

为了防止密码被日军破译，美国海军陆战队特意发明了一套新的口语密码——纳瓦霍密码，并在太平洋战争中得到了实战的检验，日军对此根本无法破译。从此以后，头戴耳机、手持话筒、背负电台的纳瓦霍通信员成为美海军陆战队的标准形象，走入了人们的视线中。那么，纳瓦霍密码就是纳瓦霍族的土语吗？又是谁把它们挖掘出来的呢？

第九章　北极行动.....185

“北极行动”是史上最著名、争议最大的密码“逆用”事件。在整个行动期间，荷兰牺牲了47名特工和1200多名地下抵抗人员，而这仅仅是由于英国密码部门的疏忽。难道这真的是疏忽吗？还是英国人有意而为？直到今天，英国和荷兰仍然争辩不休。这到底是怎么一回事？什么又叫作密码“逆用”呢？

第十章　破获“独臂大盗”的密码.....205

雅德利是美国密码和破译工作的开创者和奠基人，他的那班人马后来发展成为国家情报署，比中央情报局的资格都老。这个大名鼎鼎的雅德利曾有一段在华时光，帮助重庆国民政府破译汪伪政权和重庆卧底的密码通信。这是怎么回事？他为什么会来到中国呢？这个密码是什么样子的呢？

第一章
闪击波兰

夹在大国间的波兰，拥有全欧洲最先进的密码破译技术，对德国的军用密码有着较高的破译率。但是到了1928年，波兰人在与德国人的密码竞赛中败下阵来，这是怎么一回事？波兰人难道在坐以待毙吗？在1939年9月，德国闪击波兰之际，波兰的密码破译部门还没能做出正确的判断，这又是怎么一回事？德国人到底使用了什么方法来对付波兰人？

“昨天，一切都按计划进行。飞往柏林，飞往华沙，在那里进行谈话视察，又飞回柏林，在帝国总理府汇报，在元首餐桌上吃饭。华沙满目疮痍，几乎没有一个建筑物不受到破坏，没有一块完整的玻璃，人们一定遭受到很大的痛苦。7 天来一直没有水，没有吃的……市长估计有 4 万人死亡或受伤……除此之外，一切都很平静。我们来了，他们的折磨了结了，人们也许得到了援救。NSV（纳粹福利组织——国家社会主义福利协会）和‘巴伐利亚’营救护送队，还有战地厨房正被饥饿的人们围困，他们已精疲力竭。”

1939 年 10 月 2 日，号称“沙漠之狐”的德国将军隆美尔走访华沙后，这样写信给他的妻子。华沙的景象让制造这一切的侵略者也感到有些无所适从。

1939年10月，战后的华沙一片废墟，80%的市民逃离了这座城市

波兰为什么会如此不幸地成为希特勒野心计划的第一个牺牲品呢？这就要从波兰的地理位置说起。

波兰的难题

波兰的西面，是日益强硬的德国；波兰的东面，是极力输出社会主义的苏联。一个极右，一个极左；一个极黑，一个极红。所有的欧洲人都在关心，这两个国家什么时候打起来。但对于波兰人来说，他们还要多考虑一个问题："到底谁会先越过我的边境？"面对虎视眈眈的两大国，波兰人开始拼命地截获任何有关德国或苏联的电报，并且竭尽所能去破解。

其实，就在波兰独立后的半年时间里，波军总参二部密码处就率先破译了苏联红军的通用密码，随即发挥出重要作用。在1920年的苏波战争中，在苏联红军大兵压境、兵临华沙之际，波军密码处破译了重要情报——苏军左翼出现

1920年8月，一名波兰士兵操作M1895式柯尔特-勃朗宁机枪在华沙附近组织防御阵地

巨大裂隙。有“波兰独立象征”之称的约瑟夫·毕苏斯基将军，抓住这个稍纵即逝的机会，迅速插入红军左翼的裂隙之中，展开全线反攻。众志成城的波兰军队竟然扭转了战局，全线击溃苏军。而后，密码处再次破译重要情报——苏军第4集团军已与苏军司令部失联。波军便乘胜追击，将第4集团军完全堵住并全歼。可以说，在苏波战争中，波军密码处立下了汗马功劳。

虽然波兰人的国力远不如欧洲列强，但是波兰的密码破译技术却是欧洲顶尖的。对苏联、对德国，波军密码处都保持着相当高的破译率。这使得在波谲云诡的国际形势中，波兰人总能占得一些先机。可惜好景不长，波兰人的好日子到1926年年初为止了。1926年2月，密码处开始无法破译德国海军电报。1928年7月，密码处开始无法破译德国国防部电报。

那些看似与过去无异的德军新密文，在进行常规分析时，竟然失去了波兰人掌握的所有特征。

这给波兰人出了一个难题。德国新密码到底是什么？破解德国新密码的道路在哪里？波兰人感觉危机正在降临，而自己却无能为力。那么德国采用的新式密码到底是什么呢？它到底有多么强大？

坚不可摧的密码机

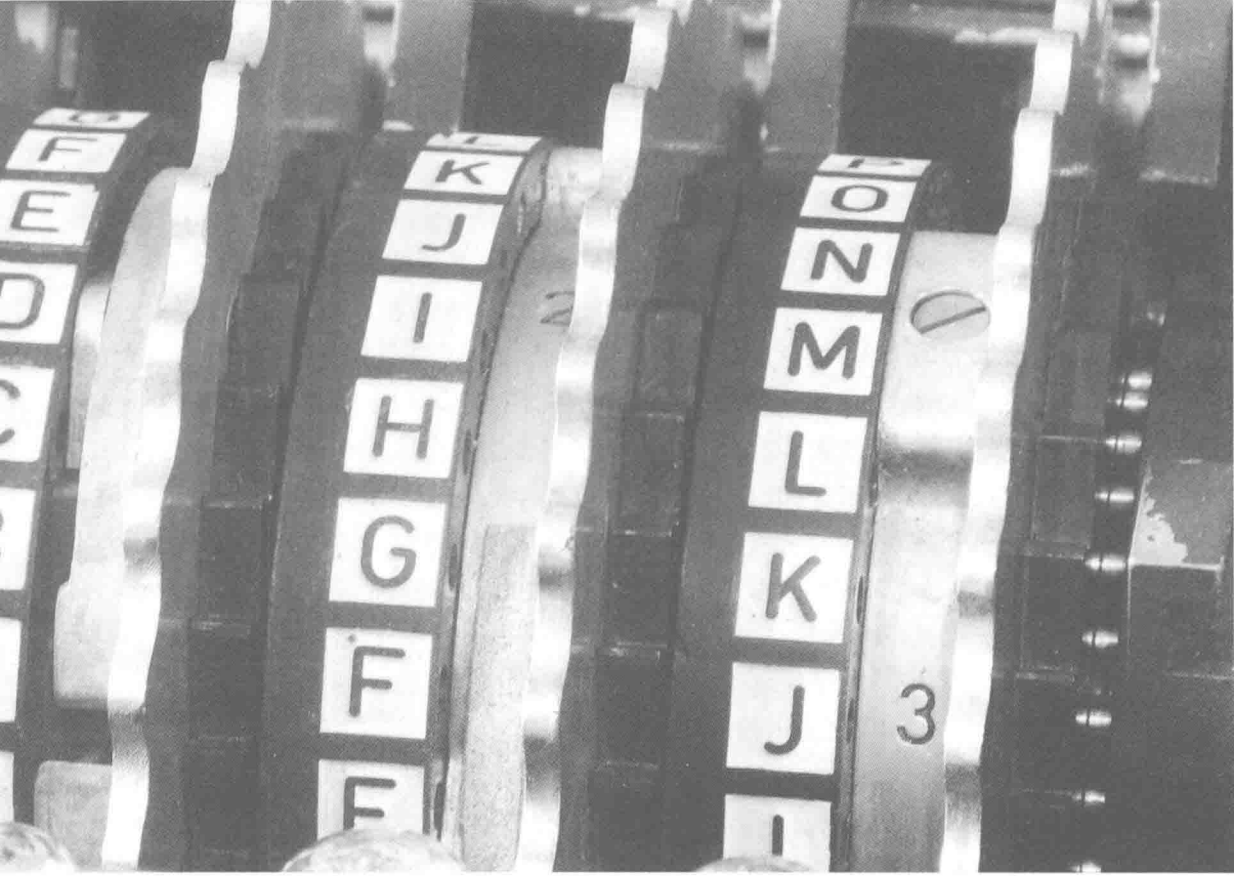
德国人的新式密码就是日后大名鼎鼎的恩尼格玛密码机（德语：Enigma，又译哑谜机或谜）。确切地说，恩尼格玛密码机是对二战时期纳粹德国使用的一系列相似的转子机械加解密机器的统称，它包含了多种型号。

恩尼格玛密码机是在1918年由德国发明家亚瑟·谢尔比乌斯和理查德·里特研制成功的，1920年用于商业用途。1926年，德国海军首先装备并使用恩尼格玛密码机的军用版。它的外形很普通，就是个装满了各种复杂而又精致的元件的普通盒子，和打字机十分相像。结构也很普通，大致可分为3个部分：键盘、显示器和转子。

键盘上的键子有26个，键位排列与现在的家用电脑十分相近，只是为了使电文尽量短小与难以破译，恩尼格玛密码机把空格、数字和标点符号都统统取消，只保留了字母键。这样做，也能减小恩尼格玛密码机的体积，便于携带。

亚瑟·谢尔比乌斯（1878年10月20日—1929年5月13日）德国工程师。他在1918年发明的恩尼格玛密码机一度成为盟军的梦魇

一台标准的恩尼格玛密码机，体积为28×34×15立方厘米，重量约为12千克



恩尼格玛密码机的核心部件——转子，这是一个标准的3转子的恩尼格玛密码机

显示器就是标示了字母的 26 个小灯泡，它位于键盘的上方。当键盘上的某个键子被按下时，就会显示所按字母被加密后的密文字母。

转子是整个恩尼格玛密码机设计中最巧夺天工的核心部件。当操作员按下键盘上的 1 个字母时，相应加密后的字母在显示器上显示出来，而转子就自动地转动 1 个字母的位置。举例来说，当第一次按 A 时，可能灯泡 B 亮，转子转动 1 格，各字母所对应的密码就改变了；第二次按 A 时，亮的灯泡可能是 C；第三次按 A 时，又可能是灯泡 D 亮了。同一个字母在明文中的不同位置，可以被不同的字母所替换；密文中不同位置的同一个字母，又可能代表明文中的不同字母，这就大大地增加了破译的难度。

但是这会产生一个致命的问题：如果连续输入 26 个字母，转子就会转 1 个圈，回到原始的方向上，这时编码就和最初重复了。而在密码战中，重复是最大的破绽，因为这可以使破译密码的人从中发现恩尼格玛的秘密。

为了避免这种情况的出现，恩尼格玛密码机开始增加转子的数量：当第一

个转子刚好转动 1 圈以后，它上面有 1 个齿轮拨动第二个转子，使得它的方向转动 1 个字母的位置。假设第一个转子已经整整转了 1 圈，按 A 键时灯泡 D 亮；当放开 A 键时第一个转子上的齿轮也带动第二个转子同时转动 1 格，于是第二次按 A 时，加密的字母可能为 R；再次放开键 A 时，就只有第一个转子转动了，于是第三次按 A 时，显示器上亮的可能就是灯泡 S 了。而实际上，恩尼格玛密码机共有 3 个转子，大大增加了破译的难度。到了二战后期，恩尼格玛密码机不断地增加转子的数量。德国海军所使用的恩尼格玛密码机，转子数量甚至达到了 8 个。

当然如果敌人收到了完整的密文，还是可以通过不断试验转动转子方向来破译电文的。为了对付敌人的“暴力破解”，恩尼格玛密码机把转子设计成可以自由拆卸、交换、组装的。这样一来，每个转子初始方向的可能性一下就是原来的 6 倍。假设 3 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 这 6 种不同位置。

而除了转子方向和排列位置，恩尼格玛密码机还有一道保障安全的关卡，就是连接板。通过连接板，操作员可以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 6 根（后期的恩尼格玛密码机甚至达到 10 根连线），这样就可以使 6 对字母的信号两两互换，其他没有插上连线的字母则保持不变。当然，连接板上的连线状况也是收发双方预先约定好的。

就这样，转子的初始方向和相互位置以及连接板的连线状况组成了恩尼格玛密码机 3 道牢不可破的保密防线，其中连接板是一个简单替换密码的系统，使可能性大大增加，而不停转动的转子，虽然数量不多，却使整个系统变成了复式替换系统，暴力破解变得不可能。

我们可以计算一下每一份恩尼格玛密电有多少种可能性。

转子不同的方向组成了 $26 \times 26 \times 26 = 17576$ 种可能性。

转子间不同的相对位置为 6 种可能性。

连接板上两两交换 6 对字母的可能性则是异常庞大，有 100391791500 种。

于是一共有 $17576 \times 6 \times 100391791500 = 10586916764424000$ 种结果！如此庞大的可能性，使破解变得异常复杂困难，而收发双方只要按照约定的转子方向、相对位置和连接板连线状况，就可以非常轻松简单地进行通信了。

这就是坚不可摧的恩尼格玛。

一台罕见的8转子恩尼格玛密码机