破译者

〔美〕戴维·卡恩 著
艺 群 译

群 众 出 版 社

破 译 者

〔美〕戴维·卡恩 著

艺 群 译

群 众 出 版 社

一九八二年·北京

破　译　者

〔美〕戴维·卡恩　著

艺　群　译

群众出版社出版　　新华书店北京发行所发行

北京印刷一厂印刷

850×1168毫米　32开本　13.25印张　333字　插页4

1982年6月第1版　1982年6月第1次印刷

统一书号：13067·64　　定价：1.25元

印数：00001—20000册

译 者 的 话

《破译者》(《The Codebreakers》)是一部以小说体裁描述密码发展史的著作。它以介绍第二次世界大战结束前美、日和欧洲各国的密码编制和破译为主，兼及其他形式的秘密通信；对第二次世界大战以后的情况，特别是技术性的东西，也概略地涉及到一些。原著取材相当广泛，据称"来自对密码学家们的采访，档案馆中未公开的文件，以及学术性著作"，具有一定的参考价值。作者脱稿后曾于一九六六年交美国国防部审查并付印初版。但全书相当庞杂繁琐，共分二十六章，约一百万字，其中最后六章的内容荒诞无聊，参考价值不大。为了便于阅读，我们节译了前二十章的有关部分，以供读者参考。删节后各章内容提要如下：

第一章。珍珠港事件及其前夕，美国和日本在通信保密上的斗争。

第二章。简述古代密写史。着重介绍单表代替的频率分析基础知识。

第三章。文艺复兴时期，西方的初期密码与破译。

第四章。多表代替的起源(十五——十六世纪)。

第五章。十七——十八世纪欧洲各国秘密情报机构，以及美国独立战争与建国初期的密码与破译情况。

第六章。十九世纪各种代替密表的再次兴起。

第七章。美国南北战争及其后所用的字移位体制。

第八章。十九世纪末至第一次世界大战前法国的几个著名密码学家。

第九章。第一次世界大战时英国海军破译机构及其重要破译战例。

第十章。第一次世界大战时法、德、英、奥、意等国的战地密码。

第十一章。第一次世界大战时，美国在欧洲战场的密码及协约国的一次重要破译战例。

第十二章。美国近代的两位破译专家：亚德利和弗里德曼，着重介绍弗里德曼。

第十三章。第二次世界大战前几个主要的密码商及其所设计的密码机或思路。

第十四章。第二次世界大战中德国密码机构及其破译情况。

第十五章。第二次世界大战中英国、瑞典及美国在欧洲战场的密码与破译。

第十六章。简述隐语与话密的基本原理。

第十七章。珍珠港事件后至第二次世界大战结束期间，美国和日本在通信保密上的斗争。

第十八章。俄国密码(着重介绍两次世界大战中的情况)。

第十九章。美国国家保密局的发展及现状。

第二十章。概述密码破译和通信保密的原则以及信息论的基本原理。

因水平有限，译文中肯定有不少错误，请读者批评指正。原文个别处有错，翻译时我们酌情作了修改，不再另行注明。

艺　群

一九七二年一月

目　录

第一章 “魔术”的一天

一九四一年十二月七日晨，一时二十八分，在西雅图附近的班布里奇岛上，海军无线电台的巨大耳朵在以太中颤动。一份电报正在东京-华盛顿线路上过来。这份电报是发给日本大使馆的，班布里奇电台在它掠过上空时侦察到信号，抄下了电报。电报很短，无线电传送只用了九分钟。

在华盛顿宪法路海军部大楼一六四九室内的页式印字电报机上，这份截收到的电报重新出现。在这里和在隔壁军需大楼内陆军部一个类似的房间里，美国通过剥开来往电报的密码外皮来探明其想定敌国的最机密的意图和计划。

一六四九室设有海军密码机构通信保密科(代号OP-20-GY)的密码分析股。值班军官布拉泽胡德海军中尉，立刻从这份电报的用于指示日本译电员操作的指标上看出，这份电报是用日本最高级密码体制加密的。这是一种美国密码分析人员称为“紫密(PURPLE)”的极为复杂的机器密。在陆军通信兵团主任密码分析员威廉·弗里德曼领导下，一个密码破译小组破译了日本加密电报，推出密码字母变换的机械原理，苦心研制出一个同日本密码机对口的装置。

布拉泽胡德把转接器拨到十二月七日密钥上，并在电动打字机上打出这份加密电报。电脉冲通过错综复杂的线路还原加密程序。电报的明文是日文。布拉泽胡德不是翻译人员，但是在隔壁的翻译分发股无人值班。他在脱密电报上贴上一个“优先”的红标签，把脱密电报送到海军通信保密科的陆军同行通信情报处。这时在华盛顿已经是上午五时过后了——这份电报在横越北美洲经过三个时区已经失去三小时的时间。

通信情报处的翻译人员把日文翻译成："请贵大使在当地时间七日下午一时将我国的答复递交美国政府（如可能则递交国务卿）。"电报中提及的"答复"已经在过去十八个半小时内由东京分十四部分发来，而布拉泽胡德只是刚刚在"紫密"密码机上脱密出第十四部分。东京发来的电报脱密出来是英文，兆头不好的最后一句是："因此日本政府遗憾地通知美国政府，鉴于美国政府的态度，日本政府不得不认为通过今后的谈判不可能达成协议。"

在上午七时布拉泽胡德下班的时候，那份指令在下午一时递交答复的电报译文还未从通信情报处送回，他把情况交代给接班的佩林海军中尉。半小时后，主管翻译股和分发截收电报的日文专家克雷默海军少校上班。他立刻看到这个很长的日本外交照会最重要的结论部分已经来到，因为他曾在昨晚前分发出这个照会的前十三部分。他照着潦草的脱密电报整理好一份，由助手用打字机按规定一式打十四份。其中十二份分发给总统、国务卿、陆军部长和海军部长，以及少数几个陆海军高级将领；其余两份存档。这份脱密电报是截收到的整个一连串日本电报的一份。一方面为了保密，另一方面为了便于查阅，在很久以前，这些日本电报由前海军情报主任沃尔特·安德森海军少将给它一个集体代号。无疑，由于每天生产情报的神秘感和蒙在密码学外面的玄妙气氛的感染，他把它称为"魔术(MAGIC)"。

在脱密电报打完时，克雷默分送给通信情报处七份；八时，他送给他的上司海军情报处远东科科长阿瑟·麦克勒姆海军上校一份。九时三十分，他离开办公室把东京答复的第十四部分分发给海军作战部长哈罗德·斯塔克海军上将、白宫和海军部长弗兰克·诺克斯。诺克斯星期日上午十时在国务院同陆军部长亨利·史汀生和国务卿科德尔·赫尔开会，研究他们已经从照会前十三部分得知的美日谈判事实上已进入绝境的危险性质。十时二十分左右，克雷默回到办公室，那份指令在下午一时递交照会的电报译文，在他在外奔走的时候已经从通信情报处送到。

这份电报立即引起了克雷默的注意。电报要求日本同美国的谈判在某一限定的时间破裂，限定日本大使送照会的时间在一个星期日的下午一时，这是十分异常的。克雷默查看领航员时差表，很快查明华盛顿下午一时，相当夏威夷时间上午七时三十分，相当日本已派出军舰和部队加以威胁的马来亚周围的紧张的远东地区拂晓前两小时。

From: Tokyo
To: Washington
December 7, 1941
Purple (Urgent - Very Important)

#907. To be handled in government code.

Re my #902[a].

Will the Ambassador please submit to the United States Government (if possible to the Secretary of State) our reply to the United States at 1:00 p.m. on the 7th, your time.

a - JD-1:7143 - text of Japanese reply.

日本人关于下午一时递交照会的电报的"魔术"译底*

克雷默立刻带着那份电报走出办公室。他先到斯塔克海军上将办公室，那里正在举行会议。他向拿去那份电报的麦科勒姆指出那份电报的性质和电报上时间的重要意义。麦科勒姆立刻会意，

*自：东京
至：华盛顿
一九四一年十二月七日
"紫密"(特急-非常重要)
#907 本电用政府密码加密处理。
参照我 #902[a]。
请贵大使在当地时间七日下午一时将我国的答复递交美国政府（如可能则递交国务卿）。
a-JD-1:7143——日本答复的本文。

走进斯塔克办公室。克雷默转身走出海军部大楼，向右拐到宪法路，直朝八个街区外的国务院举行会议的地方走去。

就在克雷默携带着事关紧要的电报在华盛顿行人很少的街道上走的时候，正是日本大使馆内困乏的译电员把那份电报脱密出来之前一小时，正是日本舰载机自航空母舰起飞，前往执行它们背信弃义的任务之前一小时，这或许是密码史上最微妙的时刻。

为什么当时没有防止珍珠港事件呢？因为日本从未发出过象"我们将攻击珍珠港"那样的电报。因此，密码分析人员不可能解决这个问题。已经截收和破译许多关于日本异常关心军舰进出珍珠港的电报，但是负这方面责任的情报军官们却把这些电报与许多其他电报等同评价和处理。珍珠港惨祸的原因是多而复杂的，但是无人责难原因出在通信保密科和通信情报处。相反，调查攻击珍珠港事件的国会委员会称赞这两个单位履行本身职责"值得高度赞扬"。

随着战争高潮的临近，这两个卓有成效的密码破译机构的成就达到了前所未有的高度。调查惨祸责任的国会委员会，暴露了这两个单位差不多是每分钟的业务活动，把这一现代密码破译组织在一个危急时刻的活动，详细拍摄下来。就是这部影片，描写攻击珍珠港前二十四小时海军通信保密科和陆军通信情报处的工作，并用过去的事件作为影片的序幕。这就是《"魔术"的一天》的本事。

一九三一年，一个日本将军突然占领了满洲，树立了一个满洲傀儡皇帝，日本岛帝国的政府落入军国主义者手中。他们开始扩充陆军。他们宣告废除海军军缩条约，开始了一个几乎是疯狂的造舰竞赛。他们也不忽略他们的密码资产，作为他们战争资本的一部分。一九三四年，日本海军购买了一部德国"恩尼格马"商业密码机。同年，外务省采用这种密码机，这种密码机发展成日本最机密的密码体制。还有几种其他密码体制作补充。陆军省、海

军省和外务省在相互通信中，共同使用“鸠（HATO）加表数字密本”。每个省还有自用的密码系数。例如，外务省使用了四种主要密码体制，每种体制有一定的保密范围，另外还有一些其他杂密。

同时，现代的幕府将军们侵入没有设防的中国，侵犯美国在华利益的事端不断发生。越来越明显，日本侵略的进军最后总会同美国的立场冲突。美国密码分析部门日益增加的情报生产，跟上了日益紧张的事态。在一九三六年仅是点点滴滴的“魔术”，在一九四〇年成了源源不断的情报。这个功绩，首先要归于一九三七年十月起担任通信兵主任的约瑟夫·莫博恩陆军少将。

莫博恩在一九四一年九月退休，留下一个庞大的很有工作效率的机构。当时，日本已经完成了拂晓袭击珍珠港的基本方案。计划已经在日本帝国海军联合舰队司令官山本五十六海军大将多思的脑子中构成。一九四一年初，山本海军大将命令进行这个作战课题的研究，坚决主张“如果我国同美国作战，除非能摧毁夏威夷海域的美国舰队，否则我国将无战胜之望。”一九四一年五月，研究结果表明实施一次突然空袭的可行性，已收集了有关统计资料，作战计划工作在着手进行。

一九四一年五月中旬，美国海军任命约瑟夫·约翰·罗彻福特前往改组和加强驻在珍珠港的无线电情报单位。一九四一年六月，罗彻福特接任设在夏威夷的十四海军区无线电小队司令。为隐蔽业务性质，他把这个小队的番号改为作战情报小队。他的任务是通过无线电情报尽量查明日本海军的部署和活动。为了这个目的，他组织破译日本海军全部小型密码和两个大型密码体制中的一个。

罗彻福特的主要目标是最难破的、机密最深的日本海军司令长官密码。自一九二六年前后至一九四〇年十一月末，这种密码的前几版曾向美国海军提供大量关于日本海军的情报。但是，最新一版是一种用移位加表作业的四码文字密本，正在顽强地抵抗美国海军最熟练的密码分析人员所作的最大努力，要求罗彻福特

集中力量在这个密本上。另一种主要密码体制，是最广泛使用的主要舰队密码体制，这是一个加上其他数字作密钥使体制更复杂的五码数字密本。美国海军名之为“五码数字密体制”，或更正式地名之为 JN25b——JN 表示“日本海军”，25 是一个识别编号，b 表示第二版(即现用版本)。设在华盛顿和菲律宾的海军密码分析单位正在破译这个密本。罗彻福特的单位没有破译这个密本，而在破译八个或十个同人事、工程、行政、气象和舰队演习有关的小密本。

密码分析只不过是这个单位任务的一部分。这个单位的一百名官兵中，绝大多数从事无线电情报的其他两方面工作：测向和报务分析。测向不仅能掌握日舰每日位置，而且成为开展报务分析这门更有成果的技术的基础。报务分析通过查明何台对何台谈话，推出陆海军部队的指挥系统。由于军事行动通常带来通信的增加，报务分析可通过注视来往报量，推断军事行动的迫近。同测向结合，报务分析往往可以大致估计一个计划行动的时间和地点。

无线电情报工作就这样对舰队的行动和组织保持长距离、隐蔽而连续不断的监视，提供成本低而有价值的情报。当然，它也有它的局限性。无线电发报台呼号的变化可以妨碍它。拍发伪电可以迷惑它。无线电静默可以使它听不见。但是，除非加给通信以无法接受的限制，无线电情报工作是不能完全受阻的。因此，在一九四一年日本加强保密期间，海军越来越依赖无线电情报，以取得关于日本海军活动的情报，尤其是在七月以后，总统的贸易冻结令使海军对不在中国海岸活动的日舰无法进行目力观察，使无线电情报几乎成为唯一的手段。

在一九四一年夏秋，时局的压力促使美国的两个密码分析部门，逐渐发展成这两个部门在十二月七日那时的组织形式。至珍珠港事件日，在华盛顿配备 181 名军官、士兵和文职人员，在各地截收站配备 150 名人员的通信情报处，已在三月份由通信兵职

业军官雷克斯·明克勒陆军中校主持。弗里德曼担任他的首席技术助理。通信情报处设有一所训练从事密码工作的陆军军官的通信情报学校，负责配备各截收站人员的第二通信勤务连，以及设在华盛顿通信情报处本部的四个科：A 科(行政)，兼负责制表机的操作；B 科(密码分析)；C 科(密码编制)，负责编制美国陆军新的密码体制，研究现用密码体制的密度，监听陆军报务以杜绝违犯保密事项；D 科(实验室)，调制密写墨水和试破可疑文件。

哈罗德·杜德陆军少校领导的B科，担负破译日本以及其他国家军事和外交密码的任务。在这方面，虽然由于材料缺乏，在十二月七日那时未能破译以一种四码数字密本为主的日本军事密码，但这个科显然至少取得了良好的成绩。杜德的技术助理是文职人员弗兰克·罗利特。负责日本外交密码破译的是斯文森陆军少校。

海军番号 OP-20-G 表示这个单位是作为海军总部编制的海军作战部长办公室第二十处 G 科。第二十处是海军通信处，G 科是通信保密科。这个慎重选用的番号，掩蔽这个科的密码分析活动，虽然这个科的任务也包括编制美国海军密码。

通信保密科科长是劳伦斯·萨福德海军中校，他是海军的主要密码专家。一九二四年一月，他成为新设在海军密码通信科研究组的负责军官。他在那里创立了海军的通信情报组织。一九三六年，萨福德担任通信保密科科长。他在战争爆发前的主要成绩之一，是建立中太平洋战略测向网和在大西洋建立一个同样的网，大西洋战略测向网在对付德国潜艇的大西洋之战中，起到了非常重要的作用。

萨福德领导的科包罗范围广泛的密码业务。但这个科的主要业务集中在密码分析上。这种业务活动分散在华盛顿、夏威夷和菲律宾的各单位进行。只有设在华盛顿的单位，破译外交密码体制和在大西洋战区使用的海军密码(主要是德国的)。罗彻福特的主要责任，是破译日本海军密码体制。设在菲律宾的单位突破了

JN 25 密，并用华盛顿供给的密钥把一些外交密码电报脱密。这个配属给当地（十六）海军区的单位，安置在科里吉多岛要塞的一条坑道内，由鲁道夫·费比恩海军上尉指挥。在他的密码分析组有军官七名和士兵十九名，同华盛顿和设在新加坡的一个英国组交换 JN 25b 密本组的可能破译结果。每个组互派一名联络员。

在海军无线电情报系统全部约七百名官兵中，三分之二人员担负截收或测向工作，三分之一人员从事密码分析和翻译工作。

在萨福德领导下，业务同密码分析密切关连的三个股是：乔治·韦尔克海军少校领导的截收测向股；李·帕克海军少校领导的密码分析股和克雷默领导的翻译分发股。密码分析股破译新密码和还原已破密码（如"紫密"）的新密钥。但在密码分析股对密本破头以后，具体的密本组还原工作（同更多是数学问题的密表破译相比，密本还原主要是文字问题）就交给翻译分发股负责。

克雷默处在一种独特的地位。虽然他在翻译分发股工作，但他却正式配属于海军情报处远东科。这样安排的目的，部分在于摆脱日文的困难，象克雷默这样精通日语的军官在通信部门工作，可能在密码破译上提出一些成功的措施；部分在于有一个熟知广泛情报背景的军官负责分发"魔术"，可以回答收阅人提出的问题。

通信保密科和通信情报处的首要任务，是获取供密码分析用的素材。从空中截取电报，海军主要靠设在普吉特海峡班布里奇岛、缅因州冬港、马里兰州切耳特纳姆、瓦胡岛赫伊亚和科里吉多的截收站，其次依靠设在关岛、加里福尼亚州美国滩、长岛阿马根塞特和佛罗里达州丘辟特的截收站。每个站指定守听若干个频率。班布里奇截收站（代号 S 站）固定抄收在东京和旧金山之间定时通报的日本政府电报。陆军的截收站称为监听哨：一号哨在新泽西州汉考克堡；二号哨在旧金山；三号哨在圣安东尼奥的萨姆豪斯顿堡；四号哨在巴拿马；五号哨在檀香山的谢夫特堡；六号哨在马尼拉的米尔斯堡；七号哨在弗吉尼亚州亨特堡；九号哨在里约热内卢。

起初，这两个部门把各截收站抄来的电报当作航空邮件寄往华盛顿。但这样做事实证明太慢，迫使海军在一九四一年在华盛顿和美国本土各截收站之间，设立电传专线。陆军和海军驻海外截收站，则挑出带有某些密码指标的日本电报，在日本密报上加上一层美国密码，然后用无线电发往华盛顿。这样重新加密，是为了使日本人不致察觉美国在密码分析方面所作的广泛努力。只有三种日本高级密才用这种费钱的无线电重传："紫密"、"红密(RED)"("紫密"启用前的一种机器密，在各主要大使馆已由"紫密"代替，但在各公使馆如驻海参崴公使馆仍在使用)、J字编号的加表密本(J series of enciphered codes)。陆军直到一九四一年十二月六日下午才安好一台电传机，接收美国本土各监听哨发来的截收电报。首批电报(旧金山发来)在十二月七日清晨收到。

截收工作漏报很少。一九四一年三月至十二月，在东京和华盛顿之间来往关于日美谈判的电报共227份，除漏报四份外，全部抄到。

在檀香山，大量日本移民引起了到处刺探情报、潜伏破坏的恐怖，十四海军区情报官梅菲尔德海军上校，早在设法获取日本总领事喜多长雄所发海底电缆电报的复本。一九四一年三月二十七日，在梅菲尔德担任现职不到两星期，专门收集美国海军情报的一个日本帝国海军青年少尉吉川猛夫到达檀香山，充当收集珍珠港情报的唯一军事间谍。化名"森村正"，他被任命为领事馆秘书。吉川猛夫想方设法周游夏威夷群岛，并在一个月内发出这样的电报："〔一九四一年五月〕十一日在珍珠港停泊的军舰如下：战列舰十一艘：《科罗拉多》号、《西弗吉尼亚》号、《加里福尼亚》号、《田纳西》号……"电报用领事馆使用的外交密码发出，不是用海军密码。

但是，梅菲尔德想通过破开密码的窗眼注视这些秘密活动的希望，由于电报局拒绝违犯关于禁止截取的法令而受到阻碍。由于

其他来源未能取得任何反间谍活动所需的情报，他的希望越来越强烈。因此，他同美国无线电公司总经理约定：美国无线电公司处理的日本领事馆电报，今后悄悄地转给海军有关当局。但是，日本领事馆在业务上轮流同檀香山好几个电报公司来往，直到十二月一日才轮到同美国无线电公司打交道。

然而，在华盛顿，截收来的电报多到压得密码分析股和通信情报处透不过气来。密码分析班子的人数不多，不能迅速处理全部来报。这个困难采用两种方法解决。

一种方法是除去两个部门的重复工作，另一种方法是倾全力破译截收到的重要电报，放过其他电报，至少是要先破译完重要电报。全部电报不可能单用一种密码拍发，因为报量大会使密码分析人员很快破译这种密码。因此，大多数国家都把密码分成级别，而限定最高级密码供紧要之需。

日本也不例外。虽然外务省使用几乎令人吃惊的多种密码，有时还用横滨正金银行私用密本、汉字密本表和一些含片假名(如タ、ジ或ヘン)的密本，但是外务省主要使用四种密码。美国密码分析人员根据每种密码破译的难度和每种密码所发的电报，把这些密码分成四级，然后按优先等级破译来报。

其中最简单的、因而等级最低放在最后处理(明报除外)的密码是LA密本，之所以这样命名是由于密文前的指标组是LA。LA密只是把片假名化成罗马字母便于电报传输和编用一些缩字以求节约电报费。这样，假名キ就由密本形式CI代替，假名ト由IF代替，两个假名的组合カン由CE代替，LA密的两码文字密本组是母音字母-字音字母或子音字母-母音字母的组成形式，并包括如密码ZO代表数字4的编制，另有一个四码文字密本组的附表：如TUVE代表“圆”，SISA代表“领事”和XYGY代表“横滨”。这类密本通常称为“护照密本”，因为这类密本往往用来处理日常行政电报，如签发护照和护照背签。LA密是一种特别