Legends of the Enigma

密码传奇

赵燕枫/著

最高级的智力 最隐蔽的搏杀

科学出版社
www.sciencep.com

密码传奇

Legends of the Enigma

科学出版社
北京

图书在版编目（CIP）数据

密码传奇 / 赵燕枫著 . —北京：科学出版社，2008
ISBN 978-7-03-020082-2

Ⅰ. 密… Ⅱ. 赵… Ⅲ. 密码－普及读物 Ⅳ. TN918. 2-49

中国版本图书馆 CIP 数据核字（2007）第 150258 号

责任编辑：侯俊琳 王 建 胡升华 / 责任校对：陈玉凤
责任印制：钱玉芬 / 封面设计：黄华斌

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www. sciencep. com

中国科学院印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2008 年 4 月第 一 版 开本：B5（720×1000）
2008 年 4 月第一次印刷 印张：23 1/4 插页：2
印数：1—10 000 字数：455 000

定价：38.00 元

（如有印装质量问题，我社负责调换〈科印〉）

序　言

我对作者写这本书一直有些疑惑，也问过作者两个问题：为什么写？给谁看？

作者很老实地回答："没想过……"

在这个充满功利主义气氛的社会里，还有人不为什么就花好几年时间写一本也许根本没人看的书？

我很好奇，于是认真通读了一遍《密码传奇》。

我想，现在我可以提出并回答下面两个问题了。

第一个问题是：这本书是给谁看的？对于我们这些永远也不会去涉猎密码学的外行人来说，读一本关于密码的书，会有什么收获呢？

至少，读者从这本书中可以体会出知识怎样转化为力量，体会到在知识转化为力量的过程中，细致扎实、严守规范的重要性。从这个意义上说，这本书适合一切重视和修炼科学方法的人。

"是什么？""为什么？""怎么办？"在创新过程中，"怎么办"往往比所有其他环节更重要。我们整天说"知识就是力量"，却往往说不出知识怎样才能转化为力量，转化之后会有什么威力。

整本《密码传奇》可以说是知识力量的范本，它着力于介绍思维交锋的具体细节，几乎每一页都记录着加密、破密双方的那些思维巨人的刀来剑往。与国力无关，与阴谋无关，也没有内裤外穿的超人，完全是智慧和知识的较量。洞悉敌人的想法，弥补自己的缺陷，其凶险猛恶、曲折微妙之处，非细读不足以领会。而一旦弄明白巨人们是怎么想到那些天才主意，又是怎么实现自己想法的，读者自己不也就找到了从书呆子变成大师的指路明灯吗？

本书的另一个闪光点在于，它用血淋淋的史实告诉我们，细节里确实有魔鬼。

为了不让敌人听懂，加密的人费了牛劲，把文件弄成天书，用上最新的机器，设定严格的操作规程，却仅仅因为操作者重复了前几个

字母，或者因为偷懒没有及时更换密钥而漏了馅。最终既害了战友，又送了自己的命，甚至搭上了国家的命运。

规章制度是为了保护自己人而设立的。越是不近人情的规定，往往越是从血的教训中总结出来的，每个细节都应该严格执行。可规章制度本质上又是反人性的，它不应该被违反，却最容易被违反。

不能强迫自己严守规范、一丝不苟，就不能完成真正的科学工作。

第二个问题是：科普著作的真正作用是什么？

科普著作的读者，不仅仅是想开阔眼界，或者对别人的结果好奇，也许他们更关心的是科学家的脑子里发生的事情：他们怎么想出这些绝妙的主意？又是怎么做到的？有哪些困难？又是怎么克服的？

读者真正关心的，是思维的方法。高人点石成金，我们不满足于他点给我们的那块金子，我们想要那根手指头。科学思维的方法，就是点石成金的那根手指。学会了科学的思维方法，一定会受益终身。

科普著作的作者，就是把金手指和咒语交给我们的人。写科普著作，是惠及众生的功德。

这本书只要认真读，有益又有趣。

挥洒自如而又不失严谨，是科普写作的极高境界。能够把问题讲明白的是专家，能够把问题讲得既明白又有趣的就是高人了。《密码传奇》文字流畅活泼，又处处显示着清晰强大的逻辑力量和对细节的充分把握；既说明作者天资高卓，更说明作者用功至勤。

在这个浮躁的世界里，这本书也许可以提醒我们，潜心于一些看不见经济效益的事，做一个愿意为喜欢的事付出心血的人，也照样有它的价值。

此外，这本书的写作方法也给了我很大的启发。

与一般的科技史话不同，它不是从源流写下来，而是从业余爱好者学习研究的角度，从一个具体产品入手逐渐扩展到一般原理的探讨。这种写法提供了一个科学思维的范本，有着它特殊的价值。

作者描写的那些破解 Enigma 的高人、大牛们，他们的工作，从思维的角度看，就是力图由一斑而窥全豹，通过对一些具体直接的零散问题的研究，推导出解决这类问题的通则。

从苹果落地推断出天体运行法则，有本事小中见大，得一端而知

全局，这正是高人的不凡之处。高人与我们看见的是同样的事实，大家也都想着解决问题。只不过我们是就事论事，而高人们解决具体事的同时，念念不忘的是两个问题：这件事的实质是什么？有没有什么规律？

高人不凡，这不凡在于心。

也许是巧合，这本书的写作，最精彩的部分就是破解者们如何在一团乱麻中发现规律的，一旦你发现了这些规律，艰苦单调的工作立刻变成庖丁解牛。刀锋所向，瓦解冰消。

我们都可能成为高人，只要不被表象迷惑，而是注重发现规律。

这本书告诉我们，发现规律的道路也许曲折，但掌握规律之后的生活很甜蜜。

最后要说一句，1001n 兄命余为序，而不请名家，是个挺特别的做法。究其原因，多半是自信作品自身有其价值，不需借名家提升；当然，也不排除他有自认为找了名家作序也卖不出去，还不如不连累人家的厚道心思。

是为序。

抱朴仙人

前　言

2005年4月的一天，我在西西河中文论坛看到了一个讨论密码史的帖子，看完觉得很对胃口，就凭着自己的印象跟贴回答了几句。没有想到的是，这个跟贴被当时的版主“不爱吱声”设置为了精华。虚荣心作怪之下，我决心挑出Enigma这个密码史上的著名代表，来写一个稍微长些的东西。计划中，打算以每篇长达两三千字的篇幅，壮观地写它五六篇，还要很生猛地附上十几张图，让这个系列帖能够在长达半个月的时间里，经常出现在论坛科学版的首页，以达到虚荣心的最大满足。

我完全失算了。

现在，作为一个答案呈现在各位朋友面前的这本书，有将近30万字，图片则将近300张，早已大大突破了我起初所能想到的最伟大的结果。而在时间跨度上也远非半个月，它的逐渐成形加上后来的反复修改，居然一直延宕到了2007年的12月。

在这两年多的时间里，“密码”二字就像一个魔咒，几乎是天天摁在我这个外行的脑门上。无论是在路上，在家里，在单位，意识中总是不自觉地闪过相关的问题。从一开始的“讲故事”，到中期的“想原理”，再到最后的“融汇贯通”，整部书的写作思路也在不断地调整着。就在这个过程中，搜集的资料也渐渐泛滥成灾：各种图片收集了数百张、PDF格式的电子文档近百份；500页一包的A4打印纸至少用掉了5包，连家里的激光打印机都为此换了一次硒鼓、重新灌了两次墨粉；相关书籍摞起来，更是大约有1米高……

以上这些，其实只不过是很外化的一些表象，跟这本书“好看不好看”、“事实准确不准确”之类，根本一点关系都没有。但也是从以上这些“代价”，我倒是越来越明白“密码”二字被误读的根本原因了，概括一下就是两个字：门槛。

“密码”有门槛么？我个人的看法，也有也没有。说它有，是因

为密码学本身是数学的一个分支，严格符合逻辑和推导，想要弄明白，一定要有比较强悍的逻辑思维；说它没有，则是因为密码学的一般应用很简单，不用去深入探究它的基本原理，我们每个人都可以很熟练地掌握一些最简单的密码操作——就如当年德国报务员完全不需要知道什么叫多表加密，一样可以把 Enigma 玩得滴溜转。

密码学是一种专门的学问，我们知道，对任何一种专门学问，被挡在门槛之外的公众都很容易产生误读。比如，前几年非典流行的时候，某些地区的白醋意外脱销，就很形象地说明了这个问题。对于“密码”来说，这两个貌似神秘的汉字下面，更是许许多多怪力乱神容身的最佳场所——毕竟，要去正确地了解到底什么是密码，总是要付出一些时间和精力的。而这个代价，在当下这个速读时代，肯定是不受追捧的。

尽管如此，我还是做了这样的尝试，看看到底能不能把一个对大多数人来说是全新和陌生的领域，用平实的文字来讲清楚。我基本上是毫无理由地相信，这本书的内容，对一些读者朋友来说会很新鲜、也挺有趣；对另一些读者朋友来说，或许会有一些思考方面的助益。假如真的能够实现这些愿望的话，那么这本严格说来属于技术史的科普作品，应该说已经超额完成了它的任务。

真实的对抗最好看，人的对抗最好看，智慧的对抗最好看。以这三个好看为标准，Enigma 的历史当然也是非常好看的。当然，限于作者的学识水平和文笔，埋头苦干之下，倒是很可能把三个好看变成了一个不好看。果真如此，那就完全是作者个人的问题，只能请大家包涵了。

尤其令我难忘的是，在本书的创作过程中，得到了难以计数的朋友们的热情鼓励和大力支持。如前所述，本书最初以连载的形式首发于西西河中文论坛。在那里，大家以相当平和、理性的态度进行了热烈的探讨，不仅让我在具体的技术问题上受益匪浅，整个的讨论氛围，更让我感觉如饮甘露般的惬意。有了这么多朋友的帮助，如今这部书的硬伤才能更少，也渐渐有了一点点值得大家阅读下去的理由——更重要的是，写这部书其实是个很痛苦的过程，毕竟让我这样的外行来研究一个比较专业的领域，还要整理成文，难度是客观存在的。而在

西西河，大家一直在鼓励我；摸着良心说，这确实是我能够坚持到底的一个极为重要的理由。在此，对以下朋友表示诚挚的感谢（排名完全不分先后）：

铁手、不爱吱声、雪个、抱朴仙人、ArKrXe、ragtime、韩亚梓、landlord、马鹿、老叶、非、林小筑、一直在看、萨苏、吴健、landkid、懒厨、思考得人、导演刘化卿、孔雀王、晨枫、葡萄干、夏翁、碧血汗青、禅人、睡虫、acms、望京雨默……

其中，

雪个：不仅多次在技术性问题上给予了相当关键的帮助，而且以柔弱之躯，不远万里、不辞辛苦、不嫌麻烦、不止一次地为我邮寄甚至亲自扛来了大量参考书籍（我估计总重量应该超过她的体重了……），实在无以为报，只好在这里鸣谢了。

抱朴仙人：对书稿的主线和写作方法进行了归纳，明显增强了全书的内在逻辑结构。如今又在百忙之中答应了我的不情之请，为全书作序。顺便说一句，与仙人闲谈，实在是件很快乐的事情。

不爱吱声：若不是他将首帖设置为精华，从而极大地鼓励了我的虚荣心，那么这本书基本上是不可能写出来的。之后我们的多次沟通，不仅对我是极大的鼓励，而且从此多了一位好朋友，不亦快哉。

等等等等，实在太多了……

Enigma大致可以说是由谢尔比乌斯一个人发明的，而为了对付它，同盟国几乎调动了所有的智力资源；这本书的情况也很类似，Enigma还是那位老兄发明的，但是为了帮助我把它的经历讲得更好一些，许许多多的朋友都做出了贡献。借这个机会，我很想诚心地说一句：谢谢你们！

在科学出版社科学人文分社社长胡升华博士的直接推动下，在侯俊琳编辑、王建编辑的辛苦操作下，时至今日，这本书终于能够与大家见面了。对他们的深切感谢，渐渐变成了一个惶恐：希望这本书别让出版社赔本才好，呵呵……

最后，还要很私人地感谢一下我的爱妻。在历时两年多的写作过程中，她极为耐心地给予了一切可能的协助，从一起思考转轮加密规律到协助整理文稿，始终以逻辑思维帮助我、以热情言语鼓励我、以

具体行动支持我，点点滴滴，令我没齿难忘。我很希望能把这本书作为送给她的一份礼物，现在也终于可以成真了。这份纪念，我想我们都会很看重的。

2008 年 1 月于北京三里屯

目　　录

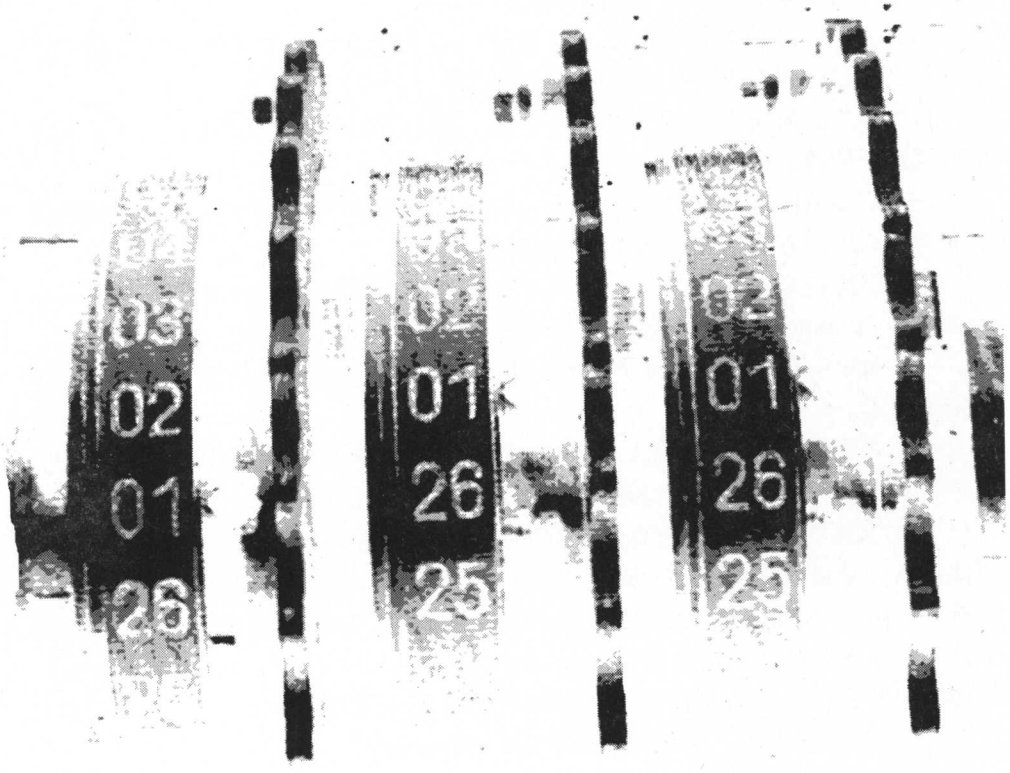
Enigma 在密码学界里，绝对是划时代的丰碑。并且，它所凝聚而成的不是一座丰碑，而是两座：研究并制造出 Enigma 是一座，研究并破解掉 Enigma 是另一座。只要稍微了解一下 Enigma 的历史，或许很多人就会被其中闪耀的人类智慧之美所折服；而如果要向这样辉煌的智慧敬献花环的话，我想，主要应该献给 3 个人：首先是德国人亚瑟·谢尔比乌斯（Arthur Scherbius）；其次是波兰人马里安·雷耶夫斯基（Marian Rejewski）；然后是英国人阿兰·图灵（Alan Turing）。

这 3 个人中，德国人发明了 Enigma；波兰人初步破解了简单的 Enigma；而英国人彻底终结了最高难的 Enigma。

那么，就让我们顺着时间的主轴，先从德国人亚瑟·谢尔比乌斯说起吧！

第一章

密码并不神秘



伴随着第一次世界大战（以下简称一战）的千里烽火，时间转眼就跨入了1918年。就在这一年，密码学界的一件大事“终于”发生了：在德国人亚瑟·谢尔比乌斯的努力下，人类历史上第一台能够投入实用的密码机器——Enigma，横空出世了！

说是“终于”发生，也还真不是夸张。在工业革命浪潮席卷西方世界那么多年以后，在一切新技术都必然首先应用于军事领域的大背景下，攸关战事成败的数学分支——密码学——的发展，竟然不可思议地始终是停滞的。放眼当时的战场，天上已经有了飞机，地上已经有了坦克，海中已经有了潜艇，甚至连空气里都已经掺杂了毒气；可就在这种情况下，人们用来加密文件的办法，竟然还是千百年来流传下来的纯手工的传统方式！

那么，也许是因为传统办法十分安全？或者说，制造密码、加密文件的技术，并没有遭到强有力的挑战，所以“能用就行，够用就好”？

当然不是。何止不是——在密码分析，也就是破译密码的新手段面前，它简直已经到了崩溃的边缘！

——诸如斯巴达人发明的“天书”（skytale 或 scytale）之类，严格说来都算不上密码的加密方法，死得已经很难看了。

——堪称最经典的传统手工加密手段、那种所谓的“单表替代”（monoalphabetic substitution），也早就被“频率分析法”毫无难度地破解了。

——简单的移位密码，种类倒是不少，花样也一再翻新，可依然被一个个揪出来干掉了。

——之后密码界的一代王者，曾经傲视群雄将近300年的“多表替代”（polyalphabetic substitution），终究也没有逃过数学刀锋的屠宰。在复杂的“多表替代”大家族中，那个几乎算是“硬度”最高、技术性最强、安全强度最高，因此被认为是最完美的维吉尼亚（Vigenère）密码，最终仍被英国人查理斯·巴贝奇（Charles Babbage）给捂死了。顺便说一句，这个查理斯·巴贝奇还真不是个凡人，他先后设计了差分机（difference engine）和分析机（analytical engine）；而这么一对宝贝儿，从原理上讲正是现代计算机的老祖宗——可他老人家生于1792年，死于1871年，说起来可得算是19世纪的人！

实际上，从这位查理斯·巴贝奇开始，我们就已经步入了一个新的世界。在

这个迥然不同的世界里，触目所及，真是风景无穷、高手遍地。随着我们一路走去，那一个个惊心动魄、异彩纷呈的故事，也不间断地从我们的身边闪过。

嗯？前面那座拔地而起、高入云霄的山峰，真是漂亮啊！

走，我们看看去。

一、密码就是错别字

本书要讲的是密码史上的一段传奇故事。在具体讲述以前，我们还是先来泛泛地看一下，到底什么才叫“密码”吧——这“密码”二字，如今实在是被用得太滥了，以至于神秘兮兮的。比如一本新书，明明是本菜谱，书名非叫《饮食密码》；明明在讲养生，非叫《健康密码》；明明是白话历史，非叫《帝王密码》；明明是散布迷信，非叫《风水密码》……这都哪儿跟哪儿啊……

其实，我们可以极不精确、简而言之地为密码下个朗朗上口的定义：密码就是错别字。与小学生在课堂上无心写出的错别字相比，密码唯一的不同，就是“有意写错”的。老师能认出学生的错别字，因为毕竟学生再错“也还是那个意思”；而密码这种“有意写错”的字，压根儿就没打算让非授权的人认出来。

此外，有时候我们生活中习以为常的某些“密码”，严格说来也还不是真正意义上的密码。一个最常见的例子，就是刷银行卡时，机器要求我们输入的“密码”，它就不是真正的密码。精确地说，它应该被称为“口令”。事实上，“口令”并不是依照正常的加密规则对“用户名”之类的信息进行加密后得到的，而且也不能通过正常的脱密规则“还原”出初始的用户名（真要能还原出来那就糟了，想像一下：假如大家的银行卡都能根据口令还原出用户名的话……），它只不过提供了一个额外的身份验证信息而已。而类似这种并非使用标准加密变换机制生成的所谓“密码”，当然也就根本不能算是真正的密码。也许有人会说，我的银行卡的“密码”就是我自己对“用户名”进行某种加密之后得到的，怎么能不算密码呢？对此我们的回答是，也许你个人的口令的确是这么得到的，但是从口令的生成规则上讲，没有人要求你必须这样去做，因此这样的特例并不具备普遍意义。从一开始，“口令”就没有被设计成必须与“用户名”相关，尽管你可以让它们之间产生某种密码对应关系，但是我们永远也无法找到一个规则，可以通过它将所有的（包括你的，也包括别人的）用户名信息“还原”出来。换言之，从普遍意义上讲，“用户名”与“口令”，实际上是并行不悖的两驾马车，彼此之间，谁也不能替代谁——无论通过什么变换规则，你也不能肯定地将任意的某个用户名转换为相对应的口令，或者把任意的口令转换成相对应的用户名。而这一点，与真正的密码形成了鲜明的对照。

关于“口令”并非“密码”的情况，我们还可以进一步扩展说明。比如，