

<<密码传奇>>

图书基本信息

书名：<<密码传奇>>

13位ISBN编号：9787030200822

10位ISBN编号：7030200829

出版时间：2008-4

出版时间：科学出版社

作者：赵燕枫

页数：360

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<密码传奇>>

内容概要

密码战，向来是人类智力最残酷、最高级的较量。

而本书所讲述的，也正是密码史上最扣人心弦的一段往事…… 二战前夕，随着世界上最先进的密码机Enigma在纳粹德国的铺开使用，波兰、法国、英国等国家的顶尖智慧群体，陆续被卷入了这场旷日持久的密码战。

加密、破译，疯狂升级，天才、叛徒，粉墨登场。

一切不仅仅是机器的对抗，更是人的对抗。

聪明人制造了密码，等待更聪明的人去毁灭它…… 全书用个性化的语言精彩描述了密码史上最传奇的故事，图文并茂，适合大众读者阅读，也是数学、密码、军事等领域的研究者和爱好者是珍贵的参考读本！

谢尔比乌斯（德国）打造转轮密码机鼎盛王朝的“开国功臣”，荣华富贵却与他无缘……雷耶夫斯基（波兰）首开破译机器密码记录的“平乱先锋”，光荣却一次次地擦肩而过……图灵（英国）奠定机械化破译基础的“科学先知”，等待他的，却是最大的人生悲剧……在混沌的密码底色上，凸显的正是人的传奇！

<<密码传奇>>

作者简介

赵燕枫，网名1001n，男，北京人。

喜欢军事、历史、科技、文化，也挺喜欢玩儿。
读书杂而不专，酷爱胡思乱想，毫无系统却始终兴味十足。
在网上涂鸦多年，主要根据地在西西河中文论坛。
目前共创作长篇作品两部：一为《密码传奇》系列，其中关于Enigma的篇目即为本书；一为《完颜亮的一生》（暂定名），在西西河中文论坛与天涯论坛煮酒论史版连载，即将出版。

<<密码传奇>>

书籍目录

第一章 密码并不神秘 一、密码就是错别字 二、密码之王 第二章 Enigma：横空出世 一、小老板谢尔比乌斯 二、更强、更强、更强！ 三、丘吉尔先生托起的灿烂星座 第三章 波兰：绝地反击 一、重压之下 二、绝密：总参二部密码处 三、他的代号叫“灰烬” 四、雷耶夫斯基初露锋芒 五、在决斗场倒下的群论之父 六、指标组！ 指标组！ 七、“数学三杰” 八、最高机密拱手相送 九、战火中流浪的数学精英 十、迟来的荣光 第四章 英国：凯歌高奏 一、碌碌无为的八年 二、黄金分割点上的小站 三、上尉的射击队 四、从“C先生”到“M先生” 五、密码破译是这样进行的 六、怪老头诺克斯 七、悠然起舞的智慧精灵 八、科学英雄：图灵 九、传奇之外 第五章 雾中之谜：回眸一代名机Enigma 一、那个转轮密码机爆发的年代 二、我们为什么要研究Enigma 三、Enigma终极解剖 四、如何操作Enigma 五、技术性花絮 六、回眸Enigma 七、Enigma究竟输在哪里 八、尾声 附录 推荐阅读

<<密码传奇>>

章节摘录

三、丘吉尔先生托起的灿烂星座 图14一台保留到今天的Enigma 看看这个装在木头盒子里，似乎长着两副并排键盘的古怪机器吧。

无论是从机器代替手工的角度出发，还是从它的强悍功能考虑，Enigma都是史无前例的。因此自出生那天起，这台机器就注定不会是昙花一现的发明。

虽然如此，我们的谢尔比乌斯先生还是为它发愁了很久…… 在每一本谆谆教诲我们上进的书中，往往都能找到这么一句话：知识是无价的。

至于Enigma这个机器到底是不是天才级别的发明创造，看来谢尔比乌斯也是有清醒认识的。

就在1918年，他做了3件事：注册了Enigma的专利；注册了Enigma的商标，和朋友一起开了家公司。之后他很快将科技转化成了第一生产力，制造出了商品型的Enigma，并且开始出售了——虽然，这第一种打着“Enigma”商标的转轮密码机还远远没有那么复杂，甚至连Enigma家族后来最具标志性的反射板都还没有出现。

图15Enigma的注册商标 对于这么优秀的发明，谢尔比乌斯当然极有信心，以至于直接把它的零售价格定成了一个天价。

折算过来，大概相当于现在的3万美元/台，或者约24万元人民币/台。

即便曾经是知识分子，等到变成小老板以后，那小刀片也得举起来不是？

不过，玩笑归玩笑，这位谢尔比乌斯博士还真不能算是奸商。

且不说机器构造复杂得要命，单从这种大步跨越密码学发展时代的发明而论，区区3万美元，还真不能算贵！

图16拧在Enigma木箱上的商标铭牌 他用尽浑身解数，向密码机最有可能的买主，也就是企业家们和军队推销。

但是，这个世界上绝对不是每个人都是伯乐，也绝不是每个人都通晓什么叫密码、什么叫更安全的密码机制。

不出意外地，他叮叮当地碰了一堆钉子：企业家们无法相信，这四四方方、三个齿轮、两副键盘、一堆电线的怪东西，居然可以拿来保守商业机密；何况，到底又能有多少商业机密，能贵到值得用至少6万美元去保护呢？

毕竟，想要Enigma正常运转，至少也得买两台用于双方通信才行，否则只有自己加密再自己解着玩了…… 从理论上讲，任何一种密码机最有可能的潜在大买主，自然就是军队。

可是，抱着极大希望的谢尔比乌斯怎么也没有想到，德国军方的回应居然是懒洋洋的：有必要么？

我们自己的密码好得很啊。

再说，这么贵的新玩意儿，又不像我们自己的密码经过一战的考验，谁知道你安全不安全…… 就这样，谢尔比乌斯在自己的责任田里惨淡经营了几年，化肥施了不少，收成却不怎么样。

虽然他决定跳楼大减价，竭力拉住可能的顾客，但是往往人家听了听，就礼貌地转身走开了——他的优惠是：每台可以便宜13%（大约相当于今天的4000美元），前提是你得购买1000台以上…… 虽然卖得不好，可谢尔比乌斯并没有失去信心。

他觉得，市场反应不佳，并不能说明Enigma的设计思路就是错误的。

在这个信念的指导下，他没有拼命降价以夺取市场，而是继续不知疲倦地改进着他的宝贝儿机器。

莫非刚下海的科学家都是这样的？

不知道了…… 沉寂了5年之后，在1923年，Enigma的升级型号——带有反射板的Enigma-A终于问世了。

从这个A型开始，Enigma走上了一条家族兴旺的繁衍之路，也正因为如此，很多资料都把Enigma-A视为Enigma系列的真正元老。

这也难怪，它的前辈“原型Enigma”，实际上只能算是粗糙的转轮加密机，虽然起点也非常高，但是和现在一比，那就逊色太多了。

比如，原型Enigma的显示板下面，是一长串小灯泡；而现在，它们的排列方式被改进成了键盘式样。我个人认为，谢尔比乌斯的这个改进非常重要。

<<密码传奇>>

至少，如果我是报务员，还必须整天盯着长长一串此起彼伏、闪来闪去的灯光的话，也实在太容易头晕了…… Enigma-A不仅配置了后来型号一直保留的键盘式显示装置，还明确了输入键盘的键位设置。

为了保密，也为了符合电报加密的要求，Enigma-A取消了所有的标点，生成的密文非常紧凑，按我们老祖宗的说法正是“句读之不知”。

此外，它还保留了三个德语中特有的变异元音字母“、A、O、U”，同时又删去了26个德文字母中不常用的Y。

这样，在Enigma-A键盘上，一共有着28个键位。

之后第二年，也就是1924年，Enigma-B再次粉墨登场。

这次，键盘上恢复了包括Y在内的所有标准字母，变异元音“A、O、U”也不留了，键位也恢复成了标准的26个。

顺便说一句，关于“A、O、U”，在后来的Enigma机型上，有时保留，有时又取消，估计是按客户的意思设计的吧；此外，后来的某些型号上，又增加了若干标点符号，用意为何？

不是很清楚，估计还是那句“客户永远是大爷”才是局部真理吧。

<<密码传奇>>

媒体关注与评论

知识力量的范本 ——《密码传奇》序言 抱朴仙人 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，还有人为什么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、破密的双方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？

密码传奇（ENIGMA卷）序言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，才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。

<<密码传奇>>

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，而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，而是从业余爱好者的学习研究角度，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，推导出解决所有这一类问题的通则。

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，不需借名家以提升；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。

<<密码传奇>>

编辑推荐

著名海外中文网站西西河论坛经典作品，十大专家推荐2008年最值得阅读的好书！

密码战，向来是人类最残酷、最高级的智力较量。

而本书所讲述的，也正是密码史上最扣人心弦的一段往事.....起伏跌宕的故事情节，悲欢离合的人物命运，精辟诙谐的语言风格，严密智慧的逻辑推理，带给读者前所未有的情感共鸣和智力挑战！

清华大学刘兵教授推荐：对一部科普书而言，精彩的故事、让人可以愉快地动动脑筋思考的内容，该是最起码的基本要求了。

如若此前，未有过类似的书籍谈论过类似的话题，这样的科普书就更有价值了。

《密码传奇》这本书，应该就算是这样的作品。

抱朴仙人推荐：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、破密的双方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。

<<密码传奇>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>