精妙的密码科学 CRC Press Taylor & Francis Group 生动的史实故事

# SECRET

## The Story of CRYPTOLOGY

# 密码历史与传奇

## 真相比故事更精彩

[美] 克雷格·鲍尔（Craig P. Bauer） 著
徐秋亮 蒋瀚 译

# HISTORY

中国工信出版集团 人民邮电出版社 POSTS & TELECOM PRESS


# SECRET

The Story of
CRYPTOLOGY

# 密码历史与传奇

## 真相比故事更精彩

# HISTORY

[美] 克雷格·鲍尔（Craig P. Bauer） 著
徐秋亮 蒋瀚 译

人民邮电出版社
北京

**图书在版编目（CIP）数据**

密码历史与传奇 : 真相比故事更精彩 / (美) 克雷格·鲍尔 (Craig P.Bauer) 著 ; 徐秋亮, 蒋瀚译. -- 北京 : 人民邮电出版社, 2019.5
ISBN 978-7-115-49396-5

Ⅰ. ①密… Ⅱ. ①克… ②徐… ③蒋… Ⅲ. ①密码学 Ⅳ. ①TN918.1

中国版本图书馆CIP数据核字(2018)第216810号

## 内 容 提 要

本书以通俗易懂的方式讲述了密码学的历史和密码算法，并生动地介绍了密码学的一些应用实例。本书通过许多案例故事将原本非常专业的内容讲述得生动有趣，因此，即使你没有数学或密码学的知识基础，也可以阅读本书。同时，作者在写作本书时整理和引用了大量的首次公开发表的珍贵资料，使密码学专业人士也能够从书中获得新知识和新资料。本书适合对密码学感兴趣的大众读者阅读，也适合大学相关专业将之作为课程教材使用，尤其适合大学教师将其作为教学参考书使用。

◆ 著　[美]克雷格·鲍尔（Craig P. Bauer）
译　徐秋亮　蒋　瀚
责任编辑　代晓丽
责任印制　彭志环

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京印匠彩色印刷有限公司印刷

◆ 开本：700×1000　1/16
印张：34　2019 年 5 月第 1 版
字数：667 千字　2019 年 5 月北京第 1 次印刷

著作权合同登记号　图字：01-2016-9744 号

定价：198.00 元

**读者服务热线：(010)81055493　印装质量热线：(010)81055316**
**反盗版热线：(010)81055315**

## 版权声明

本书献给书中所有引用到其文献内容的作者

# 译者序

当统稿完成最后一页的时候，我长长舒了一口气。这本书的翻译持续了一年多的时间，倾注了整个实验室所有师生的心血，今天终于看到了曙光。这本书对密码学领域的历史、现状做了一个非常完整的总结，并对未来进行了展望，其中含有丰富的史料，有些史料是第一次被呈现在读者面前。

本书作者追求轻松诙谐的写作风格，因此原文书中大量使用了英文俗语、俚语和一些著名人物、组织的别称或外号，这使本书的翻译充满了挑战。随着这本书翻译进程的继续，我越来越能够感觉到这本书的魅力，从而被这本书所展现的密码学瑰丽风景所吸引。

这本书资料丰富，语言风趣，而且涉及了各个历史时期有关密码学的历史事件。这给远离那个时代、远离那种文化的我们在理解、翻译上带来了极大困难。有时，我们为了查找相关的历史资料，整晚坐在电脑前搜索；有时，我们为了准确翻译一句对全文看似不那么重要的话，讨论两三个小时。因此，当这本书的翻译走到最后一页的时候，我忍不住激动心情立即写下这篇译者的话。

在这本书的翻译当中，我的博士生李真、张平原、王晨光、杨晓燕、蔡杰、赵圣楠、宋祥福、杨如鹏、丁杭超，硕士生柯俊明、刘怡然、尹栋等参与了大量的翻译工作，查阅历史资料，搜寻历史事件，查找合适的词语，讨论恰当的表达方式，付出了极大的努力。蒋瀚、魏晓超、王皓、赵川四位博士，在其中做了重要的组织工作，张波博士刚从国外归来，就也参与了书稿的校订工作。

在本书的翻译中，蒋瀚主要负责第 1 章～第 5 章，赵川主要负责第 6 章～第 10 章，魏晓超主要负责第 11 章～第 14 章，王皓主要负责第 15 章～第 20 章。他们分工合作，协调统筹，保证以高质量、高效率完成了本书的翻译工作。这本书最后由徐秋亮、蒋瀚主持统揽全稿，并做校订工作。

本书讲述了精彩的历史传奇，向读者展现了密码学发展过程的美丽画卷。在翻译过程当中，译者也学到了很多知识。我真心希望读者能喜欢这本书。这本书对于密码学工作者来讲，是了解密码学发展历史的一本不可多得的好书，它注定应该出现在密码学教师的书架上，它是一个可以提供丰富教学材料的“宝库”。

这本书的翻译是我们实验室集体努力的结晶，在此，我向实验室的全体师生表示真诚的谢意。

鉴于水平和知识面所限，书中必定存在翻译不准确、不恰当的地方，敬请读者批评指正。

感谢在翻译过程中给我们提供帮助的所有人。

译　者

2018 年 5 月

# 引 言

这个简短的引言定义了必要的术语，并且给出了本书的概览。读者可以随时翻阅引言的内容来查找后文中多次使用的术语，或利用详细索引找到该定义首次出现的位置。

从处处可见的通用产品码到邮政编码，编码已经成为日常生活的一部分，它并不是为保密而生。编码的一般方法是：用一组字母（有时是可发音的“单词”）或数字代表其他的单词或短语。事物和它的编码之间的联系通常不是数学法则。用于保密的编码通常要频繁变化，而非保密用的编码则不需要这样。例如邮编，数十年不变。事实上，不变更方便。

电报发明之后，人们希望缩短消息长度以降低费用（电报不像电子邮件一样免费），从而催生了非保密的商用编码，这种编码把短语换为短字母组（见图 I.1）。这是一个数据压缩的早期例子。数据压缩这个主题会在 2.13 节再次被提及。

当然，战争中用过的秘密编码多到不能在这里列出，更不用说整个历史中数不胜数的阴谋诡计中用到的秘密编码了。直到当今时代，秘密编码依然和我们如影随形。现在，我们只举一个例子。很多复印机和打印机都会在它们输出的每一页纸上产生一个编码，用来标识这张纸使用的是哪个机器。你需要蓝光、放大镜或显微镜才能揭示那些圆点的信息，所以很少有人注意到它们[1]。连环杀手 BTK（丹尼斯·雷德[2]）使用大学的一台复印机，复印了他给警方的挑衅信。尽管警方不是通过信纸上的编码锁定 BTK 的，但是这个编码也成为了抓捕他的一部分证据。

复印机和打印机的编码还是隐写术的例子。在隐写术中，消息是被故意隐藏的。隐写术采取的其他形式包括使用不可见的油墨和微小圆点。

编码和隐写术的例子在本书中随处可见，但不是本书的重点。本书的重点是加密。加密通常应用于单个的字符或比特以及成组的字符或比特，其方式为代换、置换（重新排序）或者两种方式组合。不同于编码，现代密码常常用数学法则和数学运算来定义。但是在早期，密码并不是这样。事实上，伟大的计算机科学先

1 电子前沿基金会（Electronic Frontier Foundation, EFF）有一个关于这个主题的网页。

2 译者注：BTK 由 3 个英文单词“捆绑、折磨、杀死”的开头字母组成。丹尼斯·雷德在给警方的信中自称 BTK。

驱查尔斯·巴贝奇（1791—1871），常常被认为是第一个用数学给密码建模的人，但这并不正确。本来有些工作比查尔斯·巴贝奇所做的工作更早，但是它们都没有流传开来[1]。无论如何，直到 20 世纪，密码学才真正数学化了。这里再多给出一些定义会使后续工作容易些。

49

The Signal Letters on the right denote the Universal Signals of Part I.

| | | | |
|---|---|---|---|
| | CREDENTIALS—*cont.* | CQWT | —Crop of ———. |
| | Have you (*or has person indicated*) the necessary credentials or certificate? - - - - - - - NWB | | A good crop of ———. Crops look well. - - - - - - - - - NSM |
| | CREDIT-S. CREDIT ON. - - PJD | | Crops not much injured yet. NSP |
| | Can you get credit? - - - PJV | | Crops have suffered severely. NSQ |
| | Have you a credit on ———? PJG | | A short crop of ———. - - NSR |
| | I will give you credit for ——. PJM | CQWV | CROSS-ES-ING. |
| CQVW | —Letters of Credit. | | Cross jack-yard. - - - - JLS |
| | CREDITOR-S. - - - - - - PJR | CRBD | —Cross trees. |
| CQWB | CREEK-S-ER. | | Cross heads. - - - - - KHP |
| CQWD | CREEP. CREEPERS. | CRBF | —Cross ways. |
| | CREW. (*See* HANDS.) - - - DHN | CRBG | —The Victoria Cross. |
| | Boat's crew. - - - - - JBP | CRBH | CROW-S. Crow-bar. |
| | By the crew. - - - - - DHW | CRBJ | CROWD-S-ED-ING. |
| | Full crew. Hands enough. DJN | | A crowd. - - - - - - - WRL |
| | Crew (*number to be shown*) have left the ship. - - - - - DJP | CRBK | CROWN-S-ED-ING. CORONET. |
| | Crew not all on board. - - DJQ | CRBL | CRUEL-LY-TY-TIES. |
| CQWF | —Native crew. | CRBM | CRUISE-ING—OFF ———. |
| CQWG | —Foreign crew. | | CRUISER-S. - - - - - - - CHQ |
| | Is your crew all on board? DJV | CRBN | —Cruisers are very vigilant. |
| | Crew not heard of. - - - DKC | CRBP | —Enemy's cruisers. |
| | Part of the crew (*indicate the number* ———). - - - - - DKF | CRBQ | CRUSH-ES-ED-ING. |
| | Crew will not pass. - - - DKG | CRBS | CRUTCH-ES. |
| | Not safe to go on with the crew as at present. - - - - - - DKH | CRBT | CRYSTAL-LINE-IZE-ES-ED. |
| | Crew will not leave the vessel. DKJ | | CUBIC CONTENTS. - - - - VNK |
| | Crew sick. - - - - - - DKL | | Cubic foot—feet. - - - - VNL |
| | Crew healthy. - - - - - DKM | CRBV | CUDDY-IES. |
| | Crew discontented, will not work. DKN | | Cuddy passenger-s. - - - NQT |
| | Crew deserted. - - - - - DKP | CRBW | CULPABLE-ILITY. |
| CQWH | —Crew have appealed to the authorities. | CRDB | CULTIVATE-S-D-ING-ION-URE. |
| CQWJ | —Some squabble or fight on shore with crew. | CRDF | CUNN (*or* CONN)-S-ED-ING. |
| | Crew imprisoned. - - - - DKQ | CRDG | CUNNING-LY-NESS. |
| CQWK | CRIME-S-INAL-LY. | CRDH | CUP-S. |
| CQWL | CRIMP-S. | | CUPOLA SHIPS. - - - - - SCP |
| CQWM | CRIMSON. | CRDJ | CURE-S-D-ING-ABLE. |
| CQWN | CRINGLE. | CRDK | CURIOUS-LY. CURIOSITY. |
| CQWP | CRIPPLE-S-D-ING. | CRDL | CURB-S-ED-ING. |
| | CRISIS. - - - - - - - - PCH | CRDM | CURL-S-ED-ING. |
| | Has not reached the crisis. PCJ | CRDN | CURRANT-S. |
| | Crisis is over. - - - - - PCK | CRDP | CURRENT-S-LY. |
| CQWR | CRITICAL-LY. | | What current (*rate and direction*) do you expect? - - - - MJN |
| | CROCKERY. - - - - - - - NPC | CRDQ | —Do we feel any current? What is the current? |
| CQWS | CROOKED-LY-NESS. | CRDS | —Try the current. |
| | CROPS. - - - - - - - - NSK | | Current will run very strong (*indicate miles per hour if necessary*). MKL |
| | What is the opinion of the ——— crop? - - - - - - - NSL | | |

**图 I.1　1875 年的编码本中的一页，这个编码本包含常用短语，例如“Some squabble or fight on shore with crew. Crew Imprisoned（船员与岸上群众发生了群体性的争吵和打架，全体船员被捕）”的短编码组。**

（来自 B.F.格林编辑的《各国信号编码》美国版的第 49 页。该书在海军部长的授权之下，由美国政府印刷所的导航局于 1875 年出版，出版地为美国华盛顿特区。承蒙美国国家密码博物馆的关照得以将该图收录到本书）

1　BUCK F J. Mathematischer Beweiß: daß die algebra zur entdeckung einiger verborgener schriften bequem angewendet werden könne[Z]. Königsberg, 1772. 这是已知的最早的关于代数密码学的工作。

密码编码学（cryptography）是建立加密系统的科学，这个词来自希腊语“κρυπτός”，意为“隐藏”以及“γραφία”，意为“书写”。密码分析学（cryptanalysis）是破解加密的科学与艺术（不使用密钥）。密码学（cryptology）是最一般的术语，包含密码编码学和密码分析学。大多数密码书是关于密码学的，这是因为若不试图破解密文，就不能确定加密是否安全。了解一个系统的弱点才能反映另一个系统的优点。换句话说，不研究密码分析学而研究密码编码学是没有意义的。尽管如此，“密码编码学”使用得更为广泛，而且等同于“密码学”。

“encipher”和“encrypt”都是指用密码算法把一个消息转化为一个伪装的形式（密文）的过程。“decipher”和“decrypt”是指上述过程的反过程，即揭示原来消息或明文的过程。有一个关于密码术语的标准（7498-2）。ISO 的标准使用术语“encipher”和“decipher”。

现代的加密通信不仅包括不能让窃听者恢复出原来的消息，还包括更多的内容。例如，人们希望在传输过程中，消息的任何改变都能被发现，这就是所谓的“数据完整性”。假设一个加密的指令被发出，其内容为“以特定价格购买指定的股票 500 股”。某人可能截获密文，并且使用其他字符替换其中一部分，这样做并不需要具有解密能力，只需要知道消息中的“股票”“数量”及“价格”等内容所处的位置。改变其中任何内容将会导致一个不同的指令被发出。如果能够阻止未经授权而改变的消息被发出，这种危害就不会造成问题。另一个重要的性质是认证性，即可以判定消息是否真正出自它的原始发送者。如果不能达到数据完整性和认证性，可能会损失掉数百万美元。

加密既可以保护个人隐私，也可以保护商业秘密。例如金融交易，从个人业务，包括你在自动提款机上的提款和在线信用卡支付，到国际银行之间的资金转账和跨国公司的主要交易，都有可能被截获，所以都需要保护。加密从来没有像现在这样保护这么多的数据。

在当今世界，密码系统就是一个算法集合，试图解决上面罗列的各种问题。其中一种算法负责实际的加密，而其他多个算法也在系统安全上起重要作用。在后文中，有时会把极为简单的加密算法作为密码系统。在这样的情况下，只是为了将它们与其他加密算法区分出来，并不表示它们有现代密码系统的特性。

即使你读到以下这些材料，也并不代表你一定要来从事密码学，除非你想得到更多有关密码学的知识。

1.“在法国，密码学被认为是一种武器，而且需要一种特殊的执照。”本书的写作花费多年，我把这条引述放在这里是因为它很有趣，而且它曾经确实是真的，但是在 1998 年和 1999 年法国废除了它的反密码学法。一般来说，欧盟成员国比其他国家对密码学限制得更少一些。

2.《爱经》把保密通信作为女人必须了解并会使用的 64 项技能之一（保密通

信是第 45 项[1]）。

3. “不得任意干涉他人的隐私、家庭、住宅或通信信息，同时也不能攻击他人的荣誉和名誉。人人有权受到法律保护以免受到这种干涉或攻击。”《人权宣言》第十二条。Universal Declaration of Human Rights, United Nations, G.A. Res. 217A（III）, U.N. Doc A/810at 71, 1948.[2]

## 本书的路线图

以第二次世界大战（后文简称“二战”）为代表的时期是密码学历史的主要转折点，因为它标志着计算机的引入。发明计算机其实是为了破解密码。当然，计算机很快就被发现有其他的用处，例如，寻找黎曼 ξ 函数的零点和玩视频游戏。二战前使用的密码系统构成了古典密码系统。有些这样的系统仍然被业余人士使用，但是绝大多数被使用计算机的方法（现代密码）取代了。我认为二战时期的密码也属于古典密码，因为尽管人们将加密和解密过程机械化，但是它们使用的算法都是从旧时期算法直接派生出来的。另一方面，现代密码学中的密码算法真正是计算机时代的产物，大部分是对比特或比特分组进行操作的。

因此本书分为两个部分。第一部分梳理古典密码学的知识，包括二战密码系统。第二部分梳理现代密码学的知识。本书内容安排的顺序，是平衡了严格的编年体顺序和概念发展的逻辑顺序之后产生的。举例来说，“一次一密”的想法可以自然地从“运动密钥密码”中得到。尽管两者产生的历史时间过程当中涌现了很多其他的密码编制方式，但是从逻辑的角度来看，“一次一密”还是被安排在“运动密钥密码”之后来介绍。

本书的简要框架如下所述。

## 第一部分

第 1 章详述了古希腊人和维京人使用的密码系统以及隐写术在古希腊历史中的影响力。第 2 章研究了单表代换密码（Mono Alphabetic Substitution Cipher，MASC），既包含单表代换在历史上真实的应用，也有埃德加·爱伦·坡、亚瑟·柯

1 VATSYAYANA. Kama sutra: the hindu ritual of love[M]. New York: Castle Books, 1963:14.

2 GARFINKEL S. Database Nation: the death of privacy in the 21st century[M]. Sebastopol, CA: O'Reilly, 2001: 257.

南·道尔（夏洛克·福尔摩斯故事的创作者）、J·R·R·托尔金以及其他作者创作的小说里出现的情节。一些重要的思想，如模运算等在本章首次出现，此外，本章还包括对单表代换的精巧现代攻击以及数据压缩、名字手册（同时利用加密和编码的系统）和图书密码的若干小节。正如前文已经提到的，第 3 章展示了从（使用多表代换的）维吉尼亚密码到运动密钥密码，进而到不可破解的一次一密的逻辑进程，提供了一些美国内战（涉及维吉尼亚密码）和第二次世界大战（涉及一次一密）的历史案例。第 4 章将视角转向换位密码的内容。在换位密码里，字母或单词被重新安排位置，而不是被替换成其他字母或单词。因为大多数现代系统混合使用代换和换位的方法，所以这样安排章节内容对讲述后面的章节（如第 6 章、第 12 章、第 19 章），提供了条件。在第 5 章里，我们会讲解一个隐写系统。据说这个隐写系统揭示了或许威廉·莎士比亚戏剧的真正作者是弗朗西斯·培根。尽管我希望这种推理是不对的，但事实上，隐写系统随处可见。本章也梳理了托马斯·杰斐逊的密码轮，该密码公开可见的最后使用案例是在第二次世界大战中。本章还可以见到，约翰·F·肯尼迪是如何在二战中依靠 19 世纪波雷费密码的安全性，从命悬一线状态下逃出生天。这里又一次讲到对古老密码系统的现代攻击。在第 6 章中，自然历史时间往回走了一点，本章梳理了密码学对第一次世界大战的影响，并且仔细审视了密码人物赫伯特·O·亚德里。他被精确地描绘成“密码界的汉·索罗”。本章还包括对审查制度的简要说明，重点是使用密码术的写作审查制度。第 7 章讲到了矩阵加密，在这里线性代数显示出其重要性。本章也展示了对这个系统的两种攻击，这些攻击从未以书籍形式被披露过。第 8 章的场景中出现了电子机械，这是因为德国人试图用恩尼格玛密码机保护他们二战时期的秘密。本章详述了波兰人如何在他们自己的机器的辅助下，破解了德国人的密码。随着波兰的沦陷，场景转向了英格兰的布莱奇利庄园以及计算机科学的先驱——阿兰·图灵的工作。本章还简要回顾了德国的洛伦兹密码以及英国人破解该密码用到的计算机。第 9 章转向第二次世界大战的太平洋战场，详细谈了一下日本外交密码和海军密码以及对这些密码的分析及其在二战中的作用。我们以纳瓦霍密码员在保证盟军胜利中扮演的角色结束本章以及第一部分。

## 第二部分

第 10 章从克劳德·香农的思想是如何塑造了信息时代和现代密码学开始，引出了本书的第二部分。本章阐述了他度量一条消息信息含量的方法[使用术语熵（Entropy）和冗余（Redundancy）]，也提供了计算这些量的简单方法，同时还介

绍了这些概念在其他领域的影响。美国国家安全局的历史在第 11 章中给出。本章还包含了对电磁辐射如何使另外一个安全系统遭受风险的讨论。瞬变电磁脉冲辐射标准技术（Transient Electro Magnetic Pulse Emanations Standard Technology，TEMPEST）（美国防止信息泄露的技术规范）可以保护系统远离这样的弱点。本章还会对美国国家安全局取得的一些成功案例（这些案例是保密的）进行了猜测。关于美国国家安全局的这一章之后，接着在第 12 章中细致地梳理了一个由美国国家安全局参与设计的密码方案 DES。本章充分讨论了关于 DES 的密钥大小和它分类设计准则的争议以及电子前沿基金会对该系统的攻击。第 13 章通过迪菲—赫尔曼密钥交换和 RSA，介绍了革命性的公钥密码学的概念。在公钥密码学里，即使有窃听者存在，那些没有碰面并商定密钥的人们，也能够安全地通信。本章给出了数学背景知识，也给出了历史背景、关键人物的多重人格、美国政府试图控制密码学研究的企图以及受到专制对待的学术界的反应。第 14 章的内容集中在对 RSA 的攻击。本章先给出了 11 种不涉及因数分解的方法，然后讲述了一系列越来越精密的因数分解的方法。第 15 章详述了一些实现方法的考虑，例如，如何快速找到大小符合 RSA 加密需要的素数，也讲了复杂性理论的重要内容。本章还包括瑞夫·墨克（Ralph Merkle）和塔希尔·盖莫尔（Taher Elgamal）的公钥密码系统。尽管本章比其他许多章需要更多技术，但是本章所描述的一些关键工作的首次提出都是由本科生（墨克、卡雅尔、塞克斯那）首次完成的。第 16 章先从二战期间缺少消息认证造成的麻烦开始，然后介绍了 RSA 和 Elgamal 是如何通过允许发送者签名消息获得认证性的。不像传统的手写签名，如果以最直接的数字签名方式签署一个数字消息，其所花费的时间会随着消息大小的增长而增长。为了解决这个问题，散列函数能将消息压缩成较短的表示方法，从而可以快速地签名。因此，本章很自然地出现了对散列函数的讨论。第 17 章覆盖了 PGP 方案，并且展示了这个混合系统是如何安全地结合了传统加密的快速和（慢的）公钥系统的便利。许多在第 12 章、第 13 章中提到的历史事件，在本章中又从历史角度进行了扩展讲述。不可破解的一次一密不是很实用，所以我们使用更为方便的流密码去达到接近一次一密方法的效果。第 18 章叙述流密码的细节，一个现代的例子是它被用于加密实时手机通话。最后，第 19 章介绍椭圆曲线密码和高级加密标准（Advanced Encryption Standard，AES），这是非常好的现代（公开算法的）密码系统中的两个方法，它们都是美国国家安全局认可的系统。第 20 章结束了本书的第二部分以及本书，介绍了量子密码学以及量子计算机和 DNA 计算机可能对未来带来的影响。未来是不确定的，但是密码学家已经准备应对量子计算机一旦变为现实将会带来的威胁。本书还提供了有关后量子密码学这一新兴领域的一些参考文献。

接下来就请翻阅并享受本书的内容吧！

# 致　谢

感谢克里斯·克里斯坦森和罗伯特·莱万阅读了整个文稿，并且提供了有价值的反馈。感谢布瑞恩·J·温克尔，对于很多章内容给予的评论，并且多年来为我提供了很多帮助和很棒的建议以及难以置信的极为慷慨的密码资料。感谢雷内·斯坦，她为我在美国国家密码博物馆里进行了大量的查询。感谢大卫·卡恩为我提供的灵感和慷慨帮助。感谢美国国家安全局的密码历史中心（最佳工作场所）的每一个人。作为2011—2012年的访问学者，我在那里度过了美好的一年。感谢《密码学》期刊的编委们与我分享他们的专业知识。最后还要感谢杰·安德森使我当初对这个学科着迷。

我还要感谢美国密码协会、斯蒂·M·贝劳文、吉勒斯·布拉萨德杰伊·布朗、斯蒂芬·布狄安斯基、詹·贝瑞、基兰·克劳利、约翰·狄克逊、莎拉·福蒂内、本杰明·加蒂、山姆·哈拉斯、罗伯特·E·哈特维希、马丁·赫尔曼、里根·克兰德斯特拉普、尼尔·科布利茨、罗伯特·罗德、安德列·迈耶、维克多·S·米勒、亚当·赖夫斯奈德、巴巴拉·林格尔、肯尼·罗森、富兰克林与马歇尔学院图书馆的玛丽·雪莱、威廉·斯托林斯、鲍波·斯特恩、厄尼·斯迪森尔、帕特里克·瓦登、鲍勃·维斯、艾维·文德森、贝特西·沃尔海姆（DAW Books公司的董事长）、约翰·扬和菲利普·齐默尔曼。

感谢你们所有人！

# 致读者

本书特意使用非正式的幽默语言进行写作。对于那些对密码学的历史或数学内容感兴趣的人来说，本书是一本休闲读物。如果你对某些内容感到疑惑，不妨跳过。本书中介绍历史的部分可自成一书，以供阅读。其他专业人士，特别是数学、历史和计算机科学领域的老师和教授们，应该会认为本书是有用的，因为它可以被当作参考文献使用，或是在课堂里使用的、引人入胜的课本。尽管本书不需要读者阅读前掌握密码学知识，但作者创作本书使用了大量的专业材料，包括书籍、研究论文、报纸文章、信件、原创采访资料以及前人未梳理过的档案材料。因此，如果你是专家，也很有可能会发现本书中相当多内容是新的。

本书打算尽可能在一本书的篇幅里展现出密码学的全貌，同时还要保持易读性，且最重要的历史和数学主题都没有遗漏。本书的主要目标是使读者像我一样也爱上这门学科，而且继续寻找并阅读更多的密码学读物。每章最后的“参考文献和进阶阅读”部分有助于读者进行更深入的阅读。

我已经将本书应用于两个完全不同级别的课程。其中一个是低年级的一般选修课，名为“编码和加密的历史”。这门课面向的学生专业范围较广，而且没有先修要求。另一个是高年级的数学和计算机科学选修课，要求先修过“微积分 I”课程。提出先修要求仅是为了保证学生有一些数学经验，其实这门课本身并没有用上微积分的知识。对于低年级的学生来说，本书大部分数学内容可以跳过，但是对于高年级的学生而言，对其最低的先修要求保证了学生能够看懂本书的所有内容。

其他人如果想使用本书作为密码学课程的教材，还可以利用网上相关链接中提供的补充材料。资料包括数百个练习题。许多练习题提供了历史上真实存在的密码，这可以检验读者的实战技术。这些密码是由不同群体创造的，甚至有一个密码是沃尔夫冈·阿玛多伊斯·莫扎特创造的。有些其他练习题里的密码在小说和短故事中扮演重要角色。有的练习题简单，有的练习题却很难。在某些情况下，练习题需要读者编写计算机程序，或使用其他技术来解决问题，而绝大部分的问题不需要编程语言的知识也可以解决。对于非历史性的密码问题，我们仔细地选

取了明文，使之对解密者有一些娱乐价值，也算是对寻找明文所付出努力的奖励。不是所有练习都与破解密码有关。对于有兴趣的读者来说，本书有很多练习题用来测试读者对一些数学概念的掌握程度，这些数学概念是各种系统中的关键构件。本书有针对不同级别课程的大纲样例和建议阅读路径。

如果你想联系作者，你可以发邮件给他，他的联系方式是 cryptoauthor@gmail.com。

# 目 录

## 第一部分 古典密码学