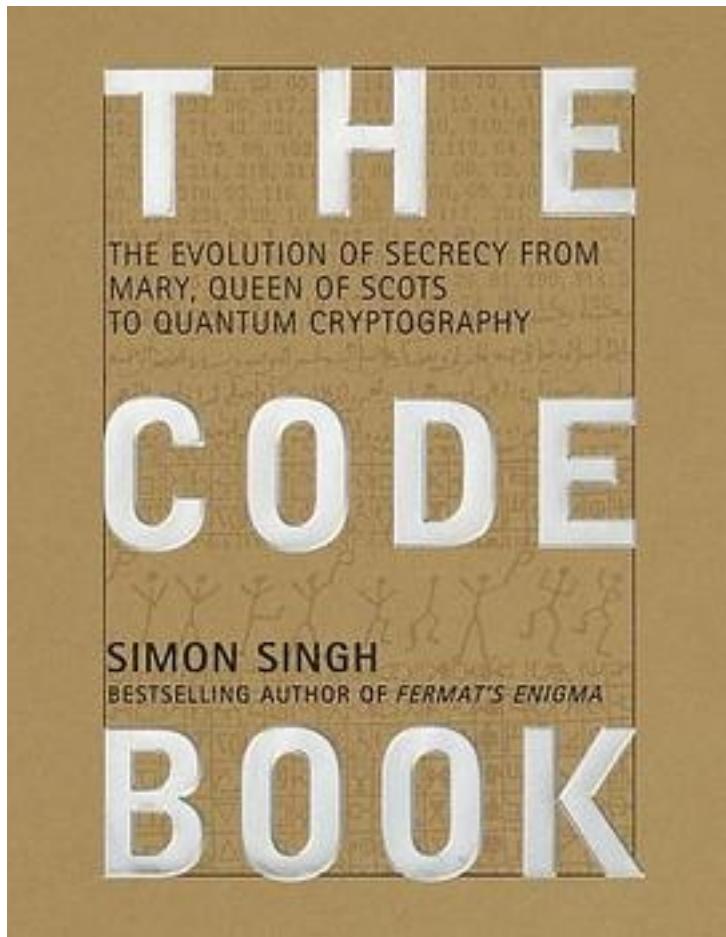


# The Code Book



[The Code Book 下载链接1](#)

著者:Simon Singh

出版者:Doubleday

出版时间:1999-09-14

装帧:Hardcover

isbn:9780385495318

Codes have decided the fates of empires, countries, and monarchies throughout recorded history. Mary, Queen of Scots was put to death by her cousin, Queen Elizabeth, for the high crime of treason after spymaster Sir Francis Walsingham cracked

the secret code she used to communicate with her conspirators. And thus the course of British history was altered by a few sheets of cryptic prose. This is just one link in humankind's evolutionary chain of secret communication, and just one of the fascinating incidents recounted in *The Code Book*, written by bestselling author Simon Singh.

Combining a superb storyteller's sense of drama and a scientist's appreciation for technical perfection, Singh traces the evolution of secret writing from ancient Greek military espionage to the frontiers of computer science. The result is an epic tale of human ingenuity, with examples that range from the poignant to the peculiar to the world-historical.

There is the case of the Beale ciphers, which involves Wild West escapades, a cowboy who amassed a vast fortune, a buried treasure worth \$20 million, and a mysterious set of encrypted papers describing its whereabouts--papers that have baffled generations of cryptanalysts and captivated hundreds of treasure hunters.

A speedier end to a bloody war was the only reward that could be promised to the Allied code breakers of World Wars I and II, whose selfless contributions altered the course of history; but few of them lived to receive any credit for their top-secret accomplishments. Among the most moving of these stories is that of the World War II British code breaker Alan Turing, who gave up a brilliant career in mathematics to devote himself to the Allied cause, only to end his years punished by the state for his homosexuality, while his heroism was ignored. No less heroic were the Navajo code talkers, who volunteered without hesitation to risk their lives for the Allied forces in the Japanese theater, where they were routinely mistaken for the enemy.

Interspersed with these gripping stories are clear mathematical, linguistic, and technological demonstrations of codes, as well as illustrations of the remarkable personalities--many courageous, some villainous, and all obsessive--who wrote and broke them.

All roads lead to the present day, in which the possibility of a truly unbreakable code looms large. Singh explores this possibility, and the ramifications of our increasing need for privacy, even as it begins to chafe against the stated mission of the powerful and deeply secretive National Security Agency. Entertaining, compelling, and remarkably far-reaching, this is a book that will forever alter your view of history, what drives it, and how private that e-mail you just sent really is.

Included in the book is a worldwide Cipher Challenge--a \$15,000 award will be given by the author to the first reader who cracks the code successfully. Progress toward the solution will be tracked on *The Code Book* website.

## 作者介绍:

西蒙·辛格，出生于英国南部萨默塞特郡，是印度旁遮普遗民后裔，曾在伦敦帝国学院学习物理，获得剑桥大学粒子物理学博士学位。前BBC资深节目制作人，其制作的《地平线：费马大定理》获得英国电影学院奖，同名科普书成为畅销书。《码书》是作者又一部心血之作，也是BBC系列专题《保密的科学》的底本，博得世界性声誉。

译者刘燕芬，台湾师范大学英语系毕业。曾任国中英语教师，现旅居德国，从事中-德、中-英文之笔译与口译，并教授中文。

目录:

[The Code Book 下载链接1](#)

标签

密码

数学

密码学

cryptography

code

Simon\_Singh

科普

科学

评论

前面的若干章都是老生常谈包括enigma什么的也都是文献综述，最后一章的alice-bob密钥交换实验是全书精华，轻松理解量子密钥。不过量子计算机还是很遥远的。

---

密码学 看了一半 有点意思 但是我数学无能 基本看完就忘

---

>

-----  
非常有意思的一本书呀呀啊

-----  
很生动 又不失准确

-----  
Superb

-----  
结合历史发展介绍密码和解密学的发展，很浅显的书。前面写得比较精彩，RSA加密算法部分数学的原理没有讲透彻，看得不够爽。不知道作者是不是有意为之。作者对目前发展出来的加密算法也太有信心了吧？我个人是相信加密算法一定有被破解的一天的。

[The Code Book 下载链接1](#)

## 书评

牛牛是某大学计算机系的大二学生，小伙儿颜值很高，而且也潮，一点儿也没有技术宅男的气质。性格也很顺和，平时不管讨论什么，或者开他开涮开黑开玩笑，他都总是笑眯眯的。我有次很好奇的问他：你是不是从不生气啊？他顿时一脸的苦相：谁说的，每次放假回家回到家里那些亲戚...

-----  
揭开秘密的冲动是人类根深蒂固的天性。就是最不好奇的心，也会为即将得知他人的秘密而悸动。有些幸运的人能以解谜为业，我们大部分的人却得靠解开那些供消遣之用的矫造谜语来满足这种欲望。对一般人而言，侦探故事或纵横字谜便已足够，极少数人则是以破解玄秘的符号为志业。约...

-----  
1586年10月15日星期三早上，苏格兰玛丽女王受到叛逆罪的庭审。主要证据是截获的玛丽与安东尼·贝平顿的来往信件。它们经过一番伪装，表面上看去很普通，实际上包含了一起阴谋——针对伊丽莎白女王的刺杀计划。英国情报部门成功破译密码，遏制了

一起尚未成型的凶案，最终把玛丽...

---

书本身无话可说，内容是无可挑剔的棒！一本科普书能写到这个地步真的是太不容易了。问题是翻译，本书的翻译在语言上没什么大问题，文笔非常流畅，读起来毫无晦涩之感。只是，似乎译者对二战史一窍不通，很多常见的人名竟然翻译错了。比方说“尼米兹”被翻译成了“里米茨”，“...

---

异常精彩的一本书，介绍了两千多年来编码与解码的战争。

编码与解码双方费尽心机、各施奇技，编码者一次次建立起坚不可摧的铜墙铁壁，而解码者一次次孕育出厚积薄发的摧枯拉。历史在曲折中前进，密码在挫折中完善，如今的编码者倚靠RSA取得了这场竞争的优势地位。使用目前的方...

---

数学是科学的皇后——数学家高斯

2017年，勒索病毒的突然爆发，给大家强制科普了关于计算机的文件加密和计算机系统管理相关课程，因为在此前，对于计算机的广大普通用户而言，哪怕计算机病毒做得再完美，最多就就是对电脑里的现有文件进行破坏，偷偷外传计算机电脑中文件，窃取...

---

曾经翻过这本书，把密码学的原理从古代讲到当代，故事非常精彩，读者看起来也不会觉得累。估计新书很难买到了，因为去年曾经需要买几本新书送人，结果北京的书店和经销商处都没有。只好联系出版社，但也只剩下五本书了。为了不耽误送人的时间，等不及汇款去再邮寄过来，只好托...

---

还是那个最会讲科学故事的西蒙·辛格，将密码学这个人类智力的巅峰对决演绎的淋漓尽致，我们仿佛在看一部惊险悬疑的大片，正反方的两位主角，编码和解码，使出浑身解数希望致对方于死地，随着两位主角的表演，各种引人入胜的故事，精彩华丽的道具，高深莫测的谋略纷纷展现，而最...

1. 加密的基本方法：字母替换 2.

最基本的替换法：使用单套字母一一对应的规则进行加密，将明文中的字母一一按规则替换为密文 通过对字频的分析猜测常用字母和常用单词，进行破解 3.

维吉尼亚密码法：使用多套字母一一对应的规则，通过设定一个密钥，在密钥的指引下，为明文中...

---

从计算机时代到如今以手机为主导的移动互联网时代，数据泄漏事件呈指数式增长，涉及到金融业、医疗行业、通信、教育等多个行业，仅2017年前11个月的全球数据泄露事件，就已经比2016年全年的数量多出10%。各国都开始高度重视网络安全，我国的网络安全法也在2017年6月1日正式...

---

几个世纪以来，密码的故事总能让人神魂颠倒，它总是与阴谋诡计、探寻宝藏、遗嘱确立、特务间谍这些传奇故事息息相关。编码和解码就如同盾与矛，这一防一攻构成了密码学这门技术科学。3000年来，在这场攻防拉锯战中，语言学、数学、通信学、物理学、计算机学等各类学科纷纷投入...

---

前有暗藏玄机的《达·芬奇密码》，后有机关重重的《S：忒修斯之船》，小说中的智力挑战非但没令读者却步，反而大为畅销。要论破解密码，西蒙·辛格的《码书：编码与解码的战争》讲得最详尽。辛格系统地介绍了密码学的历史，不仅有“智力挑战”的乐趣，更直击与我们息息相关的问...

---

密码学首先是信息学，对信息的加密与解密就如同“盾”与“矛”，也如同这个世上没有最强的“盾”，也没有最尖锐的矛。

本书以递进式演绎过程介绍了密码学，就像推理小说般一样，你以为当前的加密方法是牢不可破的时候，总有比你更聪明的人将匕首刺了进来。如果将早期的信息隐匿...

---

这本书就是沿着密码发展的历史线条一路讲下来，其中密码作为 vital

part 影响的事件和迷思也有所记录和发展。譬如 queen

marry，带铜面具的人还有二战中密码扮演的重要角色。

相比编密码的人，作者对破译密码的人着墨更多，有些人真的是有猎犬般的敏锐嗅觉，当然还有坚韧的耐力和...

---

本来是晚上想睡觉前看的 然后一拿起来晚上就没睡觉………… 对密码 数学  
历史感兴趣的话绝对值得一看！

---

[The Code Book 下载链接1](#)