《密码故事》

图书基本信息

书名：《密码故事》

13位ISBN编号：9787544302180

10位ISBN编号：7544302180

出版时间：2001-10

出版社：海南出版社

作者：[英] 西蒙·辛格

页数：364

译者：朱小蓬,林金钟

《密码故事》

内容概要

自从人类开始会用笔书写，他们就开始用密码通讯了。密码并不仅仅与电报、军事或爱情相关，它已进入人类生活的很多层面：信用卡、保险柜、电脑等等。密码无处不在，同时又随时可能被破译。围绕密码所展开的斗争甚至远胜于战争本身，它既是人类智力的另类较量，又是数学的神秘之美的比拼。在《密码故事》中，作者西蒙·辛格讲述了关于间谍、阴谋和聪明才智的精彩故事，揭示了密码学引人入胜的历史。

《密码故事》

作者简介

西蒙·辛格（Simon Singh）在剑桥大学得到了物理学博士学位，曾在BBC做制片人。执导的纪录片《费马大定理》荣获了BAFTA（英国电影和电视艺术学院）大奖，同时他撰写了与纪录片同名的畅销书。

《密码故事》

书籍目录

《密码故事》

精彩短评

《密码故事》

精彩书评

1、西蒙辛格是个很会讲故事的学术普及作家。他还写过有关一元五次方程的书和费马大定理的书。这本密码故事算是他比较早的书，我在高一2001年的时候看到这本书的时候爱不释手。看完这本书的之后就试着去解答后面的题。第一题是在一节自习课上解答出来的，频度分析是非常好用的一种方法，而第二题的解答则直到2009年。第二题是凯撒移位密码，本来这是一种非常简单的密码，最多通过26次移位就可解决。这道题难就难在，它的原文是拉丁文，很可能你已经挪到了位置，但是看不懂就当做没有做出来。第三题的时候我就开始有很多疑问了。第一：我不清楚这是什么语言写的。第二：里面可能有干扰字符。第三：是不是严格按照同音替换加密的？我们能做的，只能对着文本分析。2009年的时候，我对这个密码是一点头绪也没有，因为想得太多，也没有去做单字母的频度分析，因为我首先假设，既然是同音密码，频度分析将是无效的。后来又尝试过几次，都没理出头绪。知道今天早上，我突然又想到这个密码，我觉得可以通过同音密码的特性去先求出到底有哪些同音单元。如果严格按照同音密码执行，同音单元出现的频率应该是相近的。不过我还是没有得到什么可以进一步执行的结果。在网上搜索的时候，发现了西蒙辛格的博客，http://simonsingh.net/cryptography/cryptograms/hint-monoalphabetic-cipher-with-homophones/这里对这个密码有个很含蓄的提示。Do any of the letters or symbols have a particularly high frequency? Perhaps the frequency is too high for it to represent a letter. What else could it be a substitute for?研究过这个密码的人都知道，里面的x出现频率非常高，几乎满篇都是x，无疑西蒙辛格的意思是，x是空格。这我也曾想过，我还曾想过x可能是一个操作符，代表紧跟其后的字母是单字母做同音单元。但是无论把x做空格还是做操作符，有难以解决的问题。我的错误就在于，这个密码并不是一个严格的同音替换密码，为了给解题者留下线索，这道题还留下了一个特别的线索，这点我也早就注意到了，就是某些字母只在特定的范围内出现，比如N只在最后几行出现，B只在最开始的几行出现。这是有意识的说这几个字母可能同时代表同一个字母。最终这个密码在国外的网站上找到了答案。它的原文是意大利文。好吧，很早我就清楚，若要学好密码破解，广泛的语言学知识是非常必要的。第四关是维热纳尔密码，再接再厉。PS：第三题的解答可以到我豆瓣日志看到。
2、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，只好托海南的朋友中午跑到出版社买到又邮寄的。希望有更多的读者喜欢这本书，出版社或许能考虑再版吧。
3、两个月以前，从学校的图书馆借了这本书，一直放在床头，断断续续拖着看完了。这不是说这本书不够精彩，而是最近比较懒散，读起书来也就毫无计划可言。我一向青睐写得比较薄的书，小说除外。在我的标准里，这本书厚度还算适中。作者也完全当得起言简意赅的夸奖。里面既不乏史实，又把密码学发展不同阶段的技术说得很明白。最初的单字母替代密码以及对应的频度分析的破译；发展到多字母替代：关键词；加密的机械化以及对恩格码的破译；甚至接着两章一章讲述了破译楔形文字的智慧，；以及把语言上的隔阂（小语种）用于加密：这让我想起了本科时候大家打电话的情形。操普通话的就毫无隐私，而像我操交城话的就可以肆无忌惮。那会儿多以此互相调侃，现在想来令人忍俊不禁。以上所有的加密方法均存在一个缺陷：密钥分发：即加密者必须把自己的密钥告知接受者，而告知过程就存在被截获和破译的风险。70年代以来，几位天才的学者分别独立的证明了密钥分发是不必要的这个令人震惊的结论，并且各自开发出了可行的单向加密函数。这种加密系统革命性地提出了不对称加密的概念。这就是说，解密不再是加密的逆过程。艾丽丝告诉所有人一个公开密钥，欢迎大家用这个密钥给她写信，但是只有她知道如何解密：私人密钥。

《密码故事》

版权说明