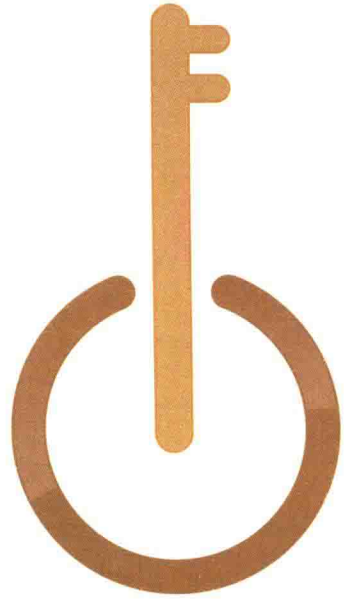
TURING
图灵程序
设计丛书

图解密码技术 第3版

畅销书全面升级，新增**椭圆曲线密码、比特币**等前沿内容！

[日] 结城浩 著　周自恒 译



史上最好懂的密码学

《程序员的数学》《数学女孩》作者
2014年日本数学协会出版奖得主

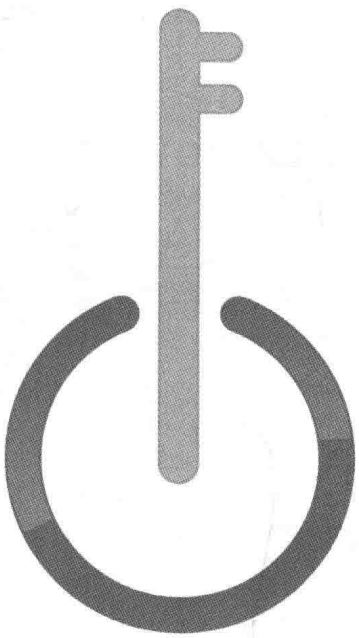
结城浩重磅力作

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

TURING
图灵程序
设计丛书

图解密码技术 第3版

[日] 结城浩 著　周自恒 译



人民邮电出版社
北　京

图书在版编目（CIP）数据

图解密码技术：第3版 /（日）结城浩著；周自恒译. --2版. -- 北京：人民邮电出版社，2016.6
（图灵程序设计丛书）
ISBN 978-7-115-42491-4

Ⅰ. ①图… Ⅱ. ①结… ②周… Ⅲ. ①密码术－图解
Ⅳ. ①TN918.3-64

中国版本图书馆CIP数据核字（2014）第129495号

内 容 提 要

本书以图配文的形式，详细讲解了6种最重要的密码技术：对称密码、公钥密码、单向散列函数、消息认证码、数字签名和伪随机数生成器。

第1部分讲述了密码技术的历史沿革、对称密码、分组密码模式（包括ECB、CBC、CFB、OFB、CTR）、公钥、混合密码系统。第2部分重点介绍了认证方面的内容，涉及单向散列函数、消息认证码、数字签名、证书等。第3部分讲述了密钥、随机数、PGP、SSL/TLS以及密码技术在现实生活中的应用。第3版对旧版内容进行了大幅更新，并新增了SHA-3、比特币、椭圆曲线密码等内容。

全书讲解通俗易懂，凡是对密码技术感兴趣的人，均可阅读此书。

◆ 著　　[日]结城浩
译　　周自恒
责任编辑　乐　馨
执行编辑　杜晓静
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
北京天宇星印刷厂印刷
◆ 开本：800×1000　1/16
印张：26.5
字数：590千字　　2016年6月第2版
印数：10 501－14 500册　　2016年6月北京第1次印刷
著作权合同登记号　图字：01-2015-8766号

定价：89.00元

读者服务热线：(010)51095186转600　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广字第8052号

站在巨人的肩上

Standing on Shoulders of Giants

iTuring.cn

译者序

中文里的“密码”是个有点难以捉摸的词汇，你认为它很简单，其实它却包含着几种看似差不多但本质上却完全不同的含义，还真的是不简单呢。

我们平时登录淘宝或者 QQ 时都需要输入用户名和密码，刷信用卡或者在 ATM 上取钱时也需要输入密码。一提到“密码”，大多数人都会想到上面这些情形。然而很不巧的是，上面这种“密码”跟我们在这本书中要探讨的“密码”几乎是完全不同的两码事。无论是上淘宝还是刷卡时输入的密码，都只是一种身份验证的凭据，换句话说，也就是向系统证明你才是这个账号或银行卡的主人的一种证据——跟“天王盖地虎!”“宝塔镇河妖!”差不多是一回事。严格来说，这种“密码”应该叫作“口令”（对应英文中的 password、passcode 或者 pin），在本书中我们也是这样叫的。

我们还习惯把 DNA 称作“遗传密码”，这里的“密码”又代表什么意思呢？其实，DNA 的功能是将一种信息（主要是蛋白质的构成信息）转换成另一种信息（碱基的序列）并记录下来。这就像将人们说的话转换成文字，将歌曲转换成 MP3 文件一样，本质上是一种“编码”（encoding）的过程，只不过我们还没有完全搞清楚这种编码机制的所有细节，因此这里的“密码”实际上应该理解为“神秘的编码”吧！很遗憾，这也不是我们在这本书中要探讨的那个“密码”。

那么这本书里所说的“密码”到底是什么呢？简单来说，密码（对应英文中的 cryptography）是一个非常庞大而复杂的信息处理体系，涉及信息的机密性、完整性、认证等许多方面，由此衍生出的技术无时无刻不在保卫着我们生活中的各种信息的安全。密码技术如此重要，但它们又是那么的不起眼，我们很少注意到它们的存在，更鲜有人知道我们为什么需要它们，以及它们究竟是怎样工作的。对于密码技术，可以说大多数人都处于一种“既不知其然，亦不知其所以然”的状态。

在如今这个信息爆炸的时代，我们每个人都和信息安全脱不了干系，因此正确理解“密码能做到什么，不能做到什么”对于培养安全意识是非常重要的。况且密码技术其实并没有那么枯燥，密码攻守双方交锋的过程更可谓是步步惊心。当然，密码技术的背后存在着非常复杂的数学原理。不过别担心，本书的作者结城浩曾经出版过《数学女孩》《程序员的数学》等多本数学方面的读物，深谙如何将复杂的数学问题用通俗易懂的方式讲给读者，这本《图解密码技术》自然也不例外，比如其中用时钟来讲解数论中的模运算这一部分就十分形象，让人印象深刻。

最后留给大家一段密文权当消遣。这是一段用经典的恺撒密码加密的文字，大家读完这本书之后，要破译它应该是轻而易举，有兴趣的话来试试看吧！

```
ZW PFL NREK KF CVRIE DFIV RSFLK TIPGKFXIRGYP Z IVTFDDVEU RE FECZEV TFLIJV ZEJKILTKVU SP
GIFWVJJFI URE SFEVY WIFD JKREWFIU LEZMVIJZKP ALJK JVRITY TIPGKFXIRGYP RK TFLIJVIR.FIX
```

周自恒

2014 年 9 月于上海

写于第 3 版发行之际

这本《图解密码技术》的第 1 版是 2003 年在日本出版的，2008 年在日本发行了第 2 版，2015 年才正式引进发行中文版，其实已经算是姗姗来迟了。不过俗话说“好饭不怕晚”，中文版出版之后，在读者当中的评价还是非常不错的，而且我个人也从这本书的翻译过程中学到了非常多的东西，这本书可以说是我的译作中让我收获最多的一本了。

有些读者在评论中指出，这本书漏掉了一些重要的技术细节，比如对 CBC 模式的填充提示攻击。的确，这本书的中文版引进得有点晚了，其实里面的内容还是 2008 年的嘛。然而说好的福利还是来了，作者结城浩先生对这本书又做了修订并发行了第 3 版，于是我也抓紧时间把中文版修订了一遍，从修订的文字量来看大约占到了原书的 20%，应该说还是非常有料的，至于具体的修订内容，请大家看结城浩先生的前言吧。

最后说点题外话。我在上一版译者序的最后写的那段密文大家破译出来了吗？其实那段是跟大家推荐一个 Coursera 上的公开课，那门课叫“密码学 1”，是斯坦福大学的 Dan Boneh 教授主讲的，然而传说中的续集“密码学 2”一直在跳票，都跳了快两年了还没开课呢，只好在这里吐吐槽……

周自恒

2016 年 4 月于上海

前　言

我们每个人都有自己的秘密，所谓秘密就是不希望被别人知道的信息。例如，你肯定不想让别人知道你的银行卡口令。还有信用卡号、贷款金额、异性关系、犯罪履历、病历、电子邮箱口令等，这些敏感信息恐怕谁都不希望泄漏给他人。别说这些敏感信息了，有些人就连年龄、身高和体重都想保密，某些情况下甚至不希望对方知道自己的姓名。

在现代社会中，很多信息都存储在计算机里，这让信息的使用变得非常方便：不但可以快速复制，还可以很容易地修改其中的错误；你可以发邮件给位于世界上任何地方的人，也可以通过博客和社交网络将信息分享给世界上任何人。

不过，也正是因为如此，在现代社会中要保护好自己的秘密信息已经变得非常困难。

即便别人复制了你的秘密信息，你也不会有所察觉，因为你手上的信息并没有丢失；正是因为信息可以很容易地被修改，所以你的重要文件也存在被他人篡改的风险；此外，如果有人将你的秘密信息通过邮件发送给第三者或者公开发布在博客和社交网络上，也会给你带来大麻烦。

为了解决这些问题，人们开发出形形色色的**密码技术**。例如，“密码”可以让窃听者无法解读窃取的消息，“单向散列函数”可以检测出消息是否被篡改过，“数字签名”可以确认消息是否来自合法的发送者。本书中介绍的各种密码技术，其存在的意义正是帮助在生活和工作中经常使用计算机和网络的我们保守秘密，并确认信息的正确性。[①]

然而，无论多么高级的密码技术，都存在一个巨大的弱点，那就是“人”。如果用户无法正确运用密码技术，就无法真正确保信息安全。就算用再强大的加密手段对文件进行保护，如果用户设置的口令非常弱，也会让加密形同虚设。要正确运用密码技术，就需要理解这些密码技术的特点，特别是必须理解“我现在正在做什么”以及“这个技术到底有什么意义”。

本书是一本以通俗易懂的方式介绍密码技术的入门书，希望在尽量减少繁冗的数学公式的前提下，能够让各位读者理解各种密码技术的功能和意义。

密码已经不再仅仅属于专家和研究人员，而是我们每一个生活在现代社会的人都必须要掌握的一门技术。希望各位读者能够通过本书，学习到密码技术以及信息安全方面的基础知识。

---

① 在本书中，“密码”一词指的是安全传送消息的方法（即英文的 cryptography），通常包括密码算法和密钥等部分，并不是我们俗称的，在网站和 ATM 中输入的那种“密码”（即英文的 password、passphrase 或者 pin）。为了以示区别，本书中将后者统一翻译为“口令”。——译者注

本书的特点

本书的特点如下。

通俗易懂地讲解密码技术

密码技术分为很多种类，无论哪一种都是非常复杂而难以理解的。本书中精选了其中特别重要的几种，并通过大量的图示对它们进行通俗易懂的讲解。

讲解密码技术的相互关系

每一种密码技术都不是单独存在的，而是通过相互关联、相互补充，形成了一个巨大的框架，就如同一块巨大的拼图一样。本书中将为大家讲解组成这一巨大拼图的各种密码技术之间的相互关系。

讲解“密码的常识”

一般常识与密码界中的常识之间存在一定的差异。例如，一般人往往会认为“保密的密码算法比较安全”，然而，密码界中的常识却是“不要使用保密的密码算法”。本书中会关注一般常识与密码界中的常识存在差异的地方，以便引起读者的注意，不要做出错误的判断。

目标读者

本书的目标读者主要包括以下人群：

- 对密码相关知识感兴趣的人
- 希望理解公钥密码、数字签名等密码技术原理的人
- 对信息安全感兴趣的人

数学不好的人也能看懂

数学是密码技术得以成立的基础，因此难免会碰到复杂的数学公式。为了让数学不好的读者也能够理解，本书中尽力避免使用大量的数学公式，而是更多地采用示意图来进行讲解。

通过小测验确认理解的程度

本书正文中会提供一些帮助确认理解程度的小测验，其中的题目在阅读本书的过程中大多都能够很快回答出来。在每一章的最后可以找到本章小测验的答案，读者可以在阅读本书的过程中，随时确认自己的理解程度。此外，在本书的最后还有一篇“密码技术综合测验”，读者可以通过这些题目来确认自己对本书内容的整体理解程度。

本书的结构

第 1 部分：密码

第 1 章**“环游密码世界”**将对密码技术进行整体性的讲解。

第 2 章**“历史上的密码”**将讲解一些在历史上扮演了重要角色的密码，并对密码的破译进行思考。

第 3 章**“对称密码（共享密钥密码）”**将讲解加密所使用的基本技术——对称密码（共享密钥密码），包括长期以来被作为标准采用的 DES 算法以及最新的 AES 算法。

第 4 章**“分组密码的模式”**将讲解对称密码中描述加密具体实现步骤的模式，内容包括 ECB、CBC、CFB、OFB、CTR 等各种模式，以及分组密码和流密码的相关知识。

第 5 章**“公钥密码”**将讲解现代密码技术中最重要的部分——公钥密码。在讲解密钥配送的相关问题之后，还会对 RSA 公钥加密算法进行实际计算。

第 6 章**“混合密码系统”**将讲解通过将对称密码和公钥密码相结合来实现更安全的加密和解密的方法。

第 2 部分：认证

第 7 章**“单向散列函数”**将讲解能够产生消息指纹的单向散列函数。这一章将讲解单向散列函数所具备的性质，并介绍 MD5、SHA-1、RIPEMD 等具体的单向散列函数。

第 8 章**“消息认证码”**将讲解通过将对称密码与单向散列函数相结合来确认消息是否被正确传送的技术。此外，我们还将介绍近年来备受关注的认证加密技术。

第 9 章**“数字签名”**将讲解采用公钥密码技术来进行认证的技术，这些技术能够防止伪装和篡改。

第 10 章**“证书”**将讲解用来表示公钥合法性的证书以及颁发证书的认证机关的相关知识，同时还将讲解公钥基础架构（PKI）的机制。

第 3 部分：密钥、随机数与应用技术

第 11 章**“密钥”**将讲解管理密码中所使用的密钥的相关知识，并探讨我们日常使用的“口令”（password）。

第 12 章**“随机数”**将讲解用于在计算机上生成随机数的伪随机数生成器。伪随机数生成器在密钥的生成过程中发挥了重要的作用。这一章将讲解密码中所使用的随机数所具备的性质，并介绍使用对称密码和单向散列函数构建伪随机数生成器的方法，同时还会介绍在密码中使用线性同余法的危险性。

第 13 章 **“PGP”** 将讲解一种广泛使用的加密软件——Pretty Good Privacy（PGP）。PGP 集成了多种重要的密码技术，如对称密码、公钥密码、单向散列函数、数字签名、密钥管理、随机数生成等。通过学习 PGP 的结构，我们就可以理解密码技术的组合方法。

第 14 章 **“SSL/TLS”** 将讲解 Secure Socket Layer（SSL）和 Transport Layer Security（TLS）。SSL/TLS 是我们在 Web 上进行网上购物等操作时用来确保安全性的技术。

第 15 章 **“密码技术与现实社会”** 将对之前的章节中所讲解的密码技术进行梳理，并对密码技术在现实社会的安全方面所发挥的作用进行思考。此外，我们还将介绍通过结合多种密码技术来实现的虚拟货币——比特币。

附录 A **“椭圆曲线密码”** 将简要介绍近年来日益重要的椭圆曲线密码。

附录 B **“密码技术综合测验”** 中为大家出了一些关于密码技术的简单题目，大家可据此来确认自己对密码技术的理解程度。

谢辞

感谢《应用密码学》（*Applied Cryptography*）一书的作者布鲁斯·施奈尔（Bruce Schneier，1963— ）以及 PGP 的作者菲利普·季默曼（Philip Zimmermann，1954— ）。

感谢在本书执笔过程中提供宝贵信息并给予鼓励的山形浩生先生。

感谢我所著书籍、杂志连载和邮件杂志的各位读者、光临笔者网站的朋友们以及一直以来为我祈祷的天主教教友们。

本书成书过程中，我在撰稿的同时，还将书稿发布在互联网上接受了审阅。审阅者不分年龄、国籍、性别、住址和职业，全部都是在网上公开招募的，且所有的审阅工作都通过电子邮件以及网络来进行。在这里对参加本书审阅工作的各位朋友一并表示感谢。其中特别感谢提供宝贵意见、改进建议并给予我鼓励的以下各位朋友（按五十音图排序，敬称省略）：

青木久雄、新真千惠、天野胜、ANDO Yoko、池田大、石井胜、石川昭彦、石野幸夫、伊藤浩一、稻毛一行、井村 yuki 乃、岩泽正树、上原隆平、植松喜孝、植村光秀、江口加奈子、榎本直纪、大澤日出男、大竹宏志、大谷晋平、大谷祐史、奥田佳树、尾关善行、织田京子、小原刚、小柳津靖志、katokt、角田直行、加藤近之、角征典、金子统浩、上山誉晃、彼谷哲志、川合元洋、川崎昌博、川岛光博、川村正安、北川敦史、木村岳文、久保山哲二、久米川昌弘、小山毅、近藤晋也、后藤英雄、榊原知香子、贞池克己、佐藤正明、佐藤康二、佐藤勇纪、佐山秀晃、澤义和、重信和行、SHIBAMURA Shinobu、末石淳一郎、铃木隆介、平良公一、高岛修、高桥英一郎、高桥健、高桥立明、泷口幸子、竹内康二、武智仪明、竹中明夫、辰巳晋作、田中笃博士、津田昌树、富长裕久、鸟海喜代江、

土居俊彦、中岛能和、中村圭辅、中森博久、野田知哉、野野垣一义、林孝彰、春冈德久、比嘉一朋、比嘉阳一、檜垣健太郎、平澤俊继、廣中利光、古屋智久、细川贤太郎、细野英朋、保户塚贵博、堀正人、volo、米田重治、前原正英、松浦正枝、松冈正恭、MATUSHIMA Hideki、松户正春、松本悠希、松森久也、丸下博宣、御簾纳一、美马孝行、三宅喜义、宫成敏裕、宫本信二、村上佳久、持尾聪史、盛寻树、森川浩司、森田大辅、矢野正谨、倭聪、山本耕司、山本哲也

感谢一直以来支持我的 SoftBank Publishing 株式会社书籍局第 6 编辑部的野泽喜美男总编。将本书献给我最挚爱的妻子，感谢她与我分享了数不清的秘密。

结城浩

2003 年 8 月于横滨

写于新版发行之际

在新版发行之际，除了按当前情况更新了正文内容之外，为帮助理解还添加了附录。

本次改版的一部分内容得到了五十岚邦明先生的重要指导，在此表示感谢。

结城浩

2008 年 11 月于横滨

写于第 3版发行之际

第 3 版对本书内容进行了全面修订，并基于 NIST、CRYPTREC、各种 RFC 等信息对内容进行了更新。此外，在这一版中还增加了一些新内容，例如对 SSL/TLS 的 POODLE 攻击、“心脏出血”漏洞、Superfish 事件、SHA-3 竞赛、Keccak 的结构、认证加密、椭圆曲线密码、虚拟货币比特币等。

结城浩

2015 年 8 月于横滨

目 录