◎每个人都应学点密码学

王旭正 著

给秘密加把锁

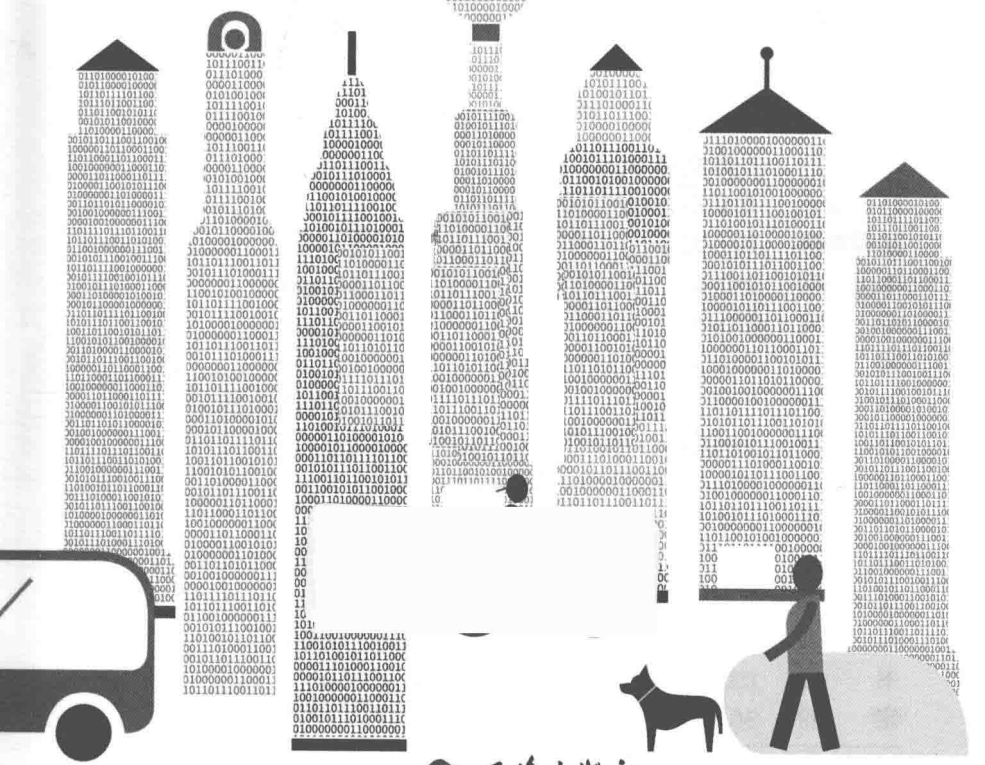
◎ 你的第一本隐私防护书！不懂密码学，你将面对生命、财产不设防的未来！“滑时代”不可不知的关键知识；数字时代守住个人信息与财产安全的第一道防线！

西苑出版社
XIYUAN PUBLISHING HOUSE

给秘密加把锁

每个人都应学点密码学

王旭正 /著



西苑出版社
XIYUAN PUBLISHING HOUSE
北 京

图书在版编目(CIP)数据

给秘密加把锁：每个人都应学点密码学/王旭正著. —北京：西苑出版社，2015. 11

ISBN 978-7-5151-0530-7

Ⅰ. ①给… Ⅱ. ①王… Ⅲ. ①密码-普及读物 Ⅳ. ①TN918.1-49

中国版本图书馆 CIP 数据核字（2015）第 261474 号

给秘密加把锁：每个人都应学点密码学

著　　者	王旭正
责任编辑	李明辉
出版发行	西苑出版社
通讯地址	北京市朝阳区利泽东二路 3 号
邮政编码	100102
电　　话	010-64228516
传　　真	010-64228516
网　　址	www.xiyuanpublishinghouse.com
印　　刷	三河市鑫利来印装有限公司
经　　销	全国新华书店
开　　本	880mm×1230mm　1/32
字　　数	120 千字
印　　张	6.5
版　　次	2016 年 1 月第 1 版
印　　次	2016 年 1 月第 1 次印刷
书　　号	ISBN 978-7-5151-0530-7
定　　价	36.80 元

（凡西苑出版社图书如有缺漏页、残破等质量问题，本社邮购部负责调换）

推荐序

悄悄走入你我日常生活的密码技术

密码学长久以来都被视为一门艰深难懂的理工课程，对大多数人而言，密码学更是遥不可及，而且毫不相关的。

然而，近年来由于网络技术及应用的蓬勃发展，密码技术已无声无息地融入每一个人的日常生活当中。例如现在很多人使用的通讯软件 LINE、社交软件 Facebook、实时照片分享软件 Instagram、网络银行、电子商务、在线游戏、物联网等等，都是使用大量的密码技术，来确保其中的信息安全与用户的个人隐私。大多数人不必学会设计密码算法或密码协议，也不需要会破解密码，但是身为数字时代的一分子，我们对认知哪些密码技术可保护哪些信息的安全及个人的隐私，是有其必要的。

在《给秘密加把锁》中，作者以深入浅出的方式，引导读者进入密码的世界，让读者了解，密码技术如何帮人们解决日常生活中所面临的各种问题。对非相关专业人士而言，本书以故事模式导引读者，轻松有趣、难易适中，读者可获取日常生

活各种活动中，保护我们信息与隐私的密码技术及原理，十分值得推荐！

雷钦隆

台湾大学电机系教授

推荐序

现代公民必读的“密码学故事书”

这是一本非常适合广大读者阅读的科学普及读物。我有幸提早阅读到全书原稿，忍不住兴奋之情，想跟未来的读者分享一点心得。

首先，这本书应该是现代公民必读的。因为我们的生活已经离不开信息科技与计算机网络了，了解一些信息安全、计算机犯罪、数字鉴识的基本概念，有助于保障自己的权利。其次，这本书让我有非常愉快的阅读体验。作者充分运用其深厚的专业知识背景，站在更高更宽广的角度，用平易近人的写作方式，将信息安全各种相关知识镶嵌在有趣的问题与故事当中。

作者从古代数字的起源谈到各种数字系统背后有趣的意义，并介绍了数字的基本计算。将古代的密码技术之间加以比较对照，还以“咸鱼翻身”的说法带领读者认识现代的数字密码。提及“公开密钥密码”时，坦白说，这是一般读者最难理解的部分，作者竟然能想到用“蛋炒饭”等思维来导

出公开密钥密码的概念，生动又有趣。网络的历史故事、现代的网络应用与问题、网络的可信度问题、数字鉴识正面的效用与背后应有的反思，内容发人深省，但都以富想象力的通俗故事精彩解说。

这样的写作方式，让阅读本书就像读故事书一样轻松愉快，却又能有知识上满满的收获，我极力推荐大家一起来阅读这本好书。除了愉快的阅读体验与知识上的收获之外，各位读者可能也会跟我一样，被作者投入的心血深深感动！

张仁俊

台北大学资讯工程系教授

推荐序

轻松认识“密码”这门学问

本书首先介绍一些基础观念，包括数字的起源、质数的奥秘、数学的规律，接着密码登场，从过去密码学、对称/非对称加解密、公开/秘密密钥、数字签名到凭证中心；通过各种网络应用的介绍（如 WWW、Email、Blog、Facebook、网络购物、无线网络、智能型手机等），谈到其中的各种犯罪和陷阱（如网络色情、计算机病毒、侵害著作、网络钓鱼、妨害名誉、身份窃盗等）；最后探讨数字证据与计算机鉴识。

全书文句简明通畅、深入浅出，可以看出作者的用心，是要“将困难的定理，用简单的话语表达”，这其实并不容易，作者确实煞费心力。更难得的是，这本想要写给一般读者的科普读物，穿插许多小故事，如“韩信点兵”“罗密欧与朱丽叶”“福尔摩斯”，更借用《断背山》《全民公敌》《网络惊魂 2》《猎杀 U-571》等经典电影情节，使读者在轻松阅读之余，获取大量宝贵的知识。

若有读者能因此受到激励，而投入此一学问的探索，或能

通过本书深植科技使用的概观与认知，则本书功劳大矣。

廖有禄

台湾“中央”警察大学刑事系教授

作者序

资讯安全的基础，在于对机密信息的敏感意识

从事学术工作多年，陆续完成了信息安全与密码、影像隐藏与应用、数字鉴识等领域的相关著书，这些书在内容上的设计与目的，主要是课堂上课教材及学生学习的依据。但如果想让这些知识更普及，让不分年龄、领域的一般人都能轻松接触、深入生活，对于科技上的深植与应用有所认识，就需要科普书而不是教科书了。我试着通过故事，鼓励读者一起来认识“密码学”的起源及发展，当然，也希望大家在了解之后，有机会爱上密码，而乐于寻求更多信息充实自己，妥善运用这项科技资源。

“密码学”在现今数字时代的运用看似新颖，却其实是一门历久弥新的有趣学问。早在中国周朝的兵书《六韬·龙韬》中，便已运用密码作为军事通讯的方法与策略，例如阴符与阴书。古罗马时期，恺撒将密码运用于军事通讯中。第二次世界大战期间，密码也没有缺席，英格玛密码机的破解，成为盟军最后胜利的关键。我们可以说：密码演变的过程，见证了人类

文明与科技的进步。而在生活中，所谓“商场如战场”，能多掌握一些情资，也就多一分人际相处及制胜的筹码，社会生存法则即是“变”与“通”，密码的概念无所不在。

拜科技进步之赐，我们随时可以不受时间、空间限制遨游网络世界：网购、收发 E-mail、用 Line 聊天、使用 Facebook、Instagram……但在使用网络的同时，我们是否有所警觉：网络真的那么安全吗？没有人会希望自己的隐私遭人窥探，这正是各国政府制定“个人资料保护法”的目的。网络是一个公开且开放的空间，数据的传递过程，其实有相当的风险，这也是信息安全如此受到企业及政府部门重视的原因，资讯安全认证标准“ISO 27001”更是这几年来的当红炸子鸡，而信息安全的基础，正是“密码学”。

现今智能型手机日渐普遍，不论达官贵人或市井小民皆能“人手一机”，人人都能轻易运用到的屏幕锁定图形锁及唤醒密码，就是密码学的延伸利用。表面上，密码只是一门加密、解密的技术而已，但其真正的精神，是对于机密信息的敏感意识，也就是我们常说的“资讯安全意识”。

也许有人会问：“我们需要了解‘密码’吗？为什么要学呢？对生活有什么帮助吗？”正如“道高一尺，魔高一丈”，科技进步，犯罪手法也在进步。举例来说，LINE 及 Facebook 确实丰富了我们的生活。数十年未联络的同学、故旧，失散已久的亲朋好友，都能重新取得联系。Facebook 甚至利用其特有的算法，不断以“你可能认识的朋友”主动为使用者提供扩张人

际网络的名单。从某种程度而言，Facebook 所形成的社交网络关系，验证了“六度分隔理论”的真实性（即平均只需要五个中间人，就能与世上任何一人认识）。而 LINE 更可说是中老年人接触智能型手机的第一个 APP（应用程序）。LINE 可爱的贴图、免费的语音通话及信息同步功能，不知让多少婆婆妈妈、少男少女为之疯狂着迷。在 MSN、Yahoo Messenger 流行的年代，曾有句话是“No MSN，No Friends”，而在 MSN 中止服务、Yahoo Messenger 式微的今天，LINE 移动通讯软件霸主的地位可说是难以撼动。

但光鲜亮丽的背后，随处可见各类负面新闻：“LINE 诈骗猖獗，今年诈欺案暴增五成”（http：//goo.gl/bASnCZ）、“别点！‘骗’脸书账号遭检举，盗取个人资料”（http：//goo.gl/lMQojY），在在证明了现今使用者咨询安全意识的不足，财物及名誉上受损害的案件层出不穷。享受便利之余，反而严重牺牲基本的个人隐私及财产安全，却很少人理解到，只需要对“密码”这道安全防线有所意识，其实就能更理性运用网络、科技带来的好处。

密码学，了解密码的学问。说穿了，也就是隐藏秘密、处理秘密、鉴定秘密的学问。每个人都会有深藏在心底、不愿为人所知的秘密，各种隐藏秘密的方式，其实也正是密码中的各个加解密技术。希望在阅读本书的过程中，也让读者有机会重新思考何谓隐私及隐私所代表的意义。

最后，本书得以出版，要感谢许多人、许多事：我的工作

单位（台湾）“中央”警察大学；我的编辑团队——信息暨密码建构实验室（ICCL）伙伴：陈育廷、范亚亭、柯博淞、张雅婷、陈彦霖、郭彤安及方素贞等；圆神出版事业机构究竟出版社的编辑群。他们在第一次闲叙时对这本书的肯定，以及为稿件费心修润等编辑作业，使这本书得以顺利付梓。借此机会表达我所有心底的感动与喜悦的秘密，向所有人员的努力致上最深挚的感谢。

王旭正

2015 年 1 月

前　言

学习密码学之前，请想一想……

我们用我们个人的隐私作为货币，来换取网络的“免费服务”。我们需要真正意识到目前正发生在我们身上的隐私问题，了解免费的代价，认识网络定义隐私、个人空间及“人”的方式。

你相信网络吗？

计算机的出现，让密码研究与应用成为一门重要学科，密码不再止于推理与狭隘的数字游戏，而是与现代的科技生活息息相关。

《西游记》中齐天大圣孙悟空凭借着金箍棒与筋斗云两样利器，斩妖除魔完成了艰巨的取经任务。我们现今同样面临严峻多变的考验，信息与挑战复杂且多元，面对各项任务，网络就好比筋斗云，一翻十万八千里，让我们不出门也能得知天下事，实时即地掌握信息。计算机则如同金箍棒，协助你我完成各种工作。正因为知识的传递更便利，现代人生活、工作中的一切几乎全面仰赖计算机及网络，不容易察觉其中的危机，使

得密码成为传递所有信息时关键的第一道防线。

一般人所不熟知的是，网络最初始的发明与运用，其实与秘密的隐藏和传递有关。

20 世纪 60 年代，美国国防部各单位的计算机及通讯设备因规格不尽相同，造成彼此间交换信息的困难，妨碍了军事机密信息的传递。除了需要解决这个问题外，美国国防部也针对国家军事防卫系统的联机提出“确保永不断线”的要求，让系统联机不会因为某部计算机故障而无法进行，而这种技术的研发，就是互联网的起源。

想想看，生活中没有了计算机与网络，造成的影响会有多大！通过智能型手机和移动通讯设备，工作不再限制于办公室内；GPS 系统使我们能在陌生的环境依然悠闲自得；只要连上网络，在家就能购物，不必在大卖场人挤人，还能多方比价，甚至买遍全世界！“滑世代”可说是以指尖在过生活，用来打发剩余时光的数字娱乐更是五光十色，应有尽有。

网络的发展为食、衣、住、行、育、乐添入了不同的元素，使生活多姿多彩，我们得以突破时间与空间的限制，运用庞大资源解决生活问题。不过，网络却如双面刃，正确与错误的信息同样因网络而流通迅速，不想传递、不该传递的数据也可能遭有心人蓄意广传。太过于依赖，反而容易遭到网络的制约，造成遗憾。

网络确实能为我们带来更好的生活质量及更多的可能性，但在使用的拿捏上，我们必须拉出一条界线。

不设防的便利之下，潜藏的危机

虽然随时都能自由徜徉于浩瀚的信息之洋，但你可曾理性权衡过，便利的代价是什么？

“电子邮件”让我们可以在弹指之间完成信息的交换，但也协助了病毒的传播。“网络购物”的方便成为非法人士觊觎的目标，产生了“网络钓鱼”的诈骗手法。开设“博客”可在世界的一角为自己发声，却也可能难以掌控公开发言引起的争端，甚至因情绪性的发言而触犯法律。“社交网络”服务网站促进与朋友间的互动，竟成为歹徒搜集个人资料的天堂。“全球信息网”的技术让知识的传播更容易，却助长了网络色情的发展。互联网的技术，可以是知识传播的媒介，也可能应用在各式非法网站的建置。

随着网络发展所兴起的科技犯罪，便是我们所需面对的课题，借由网络而生的许多方便，诱发犯罪丛生。例如成长快速的电子商务，网络购物、网络银行、网络拍卖等虚拟交易中，消费者只要输入账号、密码、信用卡卡号等信息，便可进行金融交易，无须亲自到实体店面。庞大的消费者群体成为非法人士觊觎的目标。

国际间层出不穷的网络诈骗中，通过诈骗网站与诱骗邮件的“网络钓鱼”，是非法人士最常使用的一种手法。歹徒制作与知名网站相仿、几可乱真的假网站，发送伪造的电子邮件，伪装成某银行或重要入口网站，如假借土地银行“landbank”

之名行骗改造成“1andbank”（前者为“L 的小写 l”，后者为“阿拉伯数字 1”）。诈骗信件则以使用者账号有问题、提醒更换密码、账号验证、系统更新、赠送礼物等，防不胜防的各式恐吓与利诱，诱骗使用者登入假网站以获取其信息。由于制作钓鱼网站与发送钓鱼垃圾邮件都相当容易，而且使用者不易察觉，因此成为网络犯罪的大宗，造成大量金融损失。

还有另一种经常发生在个人身上的金融犯罪手法。例如银行账户出现一笔不明消费，而买受人的身份竟是本人，很可能是身份被盗窃了。想象一下，若是出现与你拥有一模一样身份的人，姓名、身份证号、出生年月日、电话、信用卡号码、印章、签名、指纹等，这些代表自己的信息，却有另一个人正使用着，会是怎样的情景？

在数字生活下，身份是虚拟的，我们靠着账号、密码或者一串数码，用以证明身份，所以当身份遭他人窃用，甚至有诈骗取财、申请或盗刷信用卡、贷款、毁谤他人等犯罪行为时，根本无法判断“虚拟身份”所代表的人是真是假。由于网络的匿名性，加上许多人缺乏个人资料保护的概念，尤其是在社交网络服务网站，容易成为犯罪者搜集个人资料的平台。

另一方面，近期成为网友制裁利器的“人肉搜索”，借由为数众多的网友，对新闻事件主角或特定对象、事件进行信息搜集比对，试图找出真相或个人资料。群众在网络时代有了具体的力量，但这样的力量究竟伸张了正义还是侵害隐私，颇有争议，有时更沦为有心人士炒作知名度的手段。