Broadview
www.broadview.com.cn

看雪 安全技术大系

加密与解密

段钢 编著

第4版

专注软件安全，深耕逆向分析

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

加密与解密

第4版

段钢 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书以软件逆向为切入点，讲述了软件安全领域相关的基础知识和技能。读者阅读本书后，很容易就能在逆向分析、漏洞分析、安全编程、病毒分析等领域进行扩展。这些知识点的相互关联，将促使读者开阔思路，融会贯通，领悟更多的学习方法，提升自身的学习能力。

本书适合安全技术相关工作者、对逆向调试技术感兴趣的人、对软件保护感兴趣的软件开发人员、相关专业在校学生及关注个人信息安全、计算机安全技术并想了解技术内幕的读者阅读。

图书在版编目（CIP）数据

加密与解密 / 段钢编著. —4 版. —北京：电子工业出版社，2018.10
（安全技术大系）
ISBN 978-7-121-33692-8

Ⅰ. ①加… Ⅱ. ①段… Ⅲ. ①软件开发 - 安全技术 Ⅳ. ①TP311.522

中国版本图书馆 CIP 数据核字（2018）第 029455 号

策划编辑：郭 立
责任编辑：潘 昕
印 刷：三河市良远印务有限公司
装 订：三河市良远印务有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编：100036
开 本：787 × 1092 1/16 印张：58.5 字数：1570 千字 彩插：4
版 次：2001 年 9 月第 1 版
2018 年 10 月第 4 版
印 次：2018 年 10 月第 1 次印刷
定 价：198.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

看雪

作者简介

本书由看雪学院创始人段钢主持编著。在本书的编写过程中，参与创作的每位作者倾力将各自擅长的专业技术毫无保留地奉献给广大读者，使得本书展现出了极具价值的丰富内容。如果读者在阅读本书后，能够感受到管窥技术奥秘带来的内心的喜悦，并愿意与他人分享这份喜悦，将是作者最大的欣慰。

主 编：段 钢

编 委：（按章节顺序排列）

accessd　张延清　张　波　沈晓斌　周扬荣　温玉杰　段治华　印　豪　程勋德

snowdbg　赵　勇　唐植明　李江涛　林子深　薛亮亮　冯　典　tankaiha　罗　翼

罗　巍　林小华　崔孝晨　郭春杨　丁益青　阎文斌

主 编

段 钢

国内信息安全领域具有广泛影响力的安全网站看雪学院的创始人和运营管理者，长期致力于信息安全技术研究，对当前安全技术的发展有深入思考。参与和组织专业人士推出了数本技术专著和相关书籍，影响广泛。2016 年创建上海看雪科技有限公司，以看雪学院为基础，致力于构建一个覆盖 PC、移动、智能设备安全研究及逆向工程的开发者社区。

编委档案

accessd

看雪学院技术专家，资深网络安全专家。在软件架构设计与开发、软件加解密、漏洞挖掘、漏洞分析与利用、逆向工程、入侵取证、虚拟化安全技术等领域有丰富的经验。

参与章节：第 2 章　2.3　MDebug 调试器

张延清

武汉科锐安全教育机构技术总监，软件逆向教育专家。精通 Windows 系统下从 32 位到 64 位、从系统层到应用层、从设计到实现的所有逆向方向。在移动端大潮来临前，技术兴趣集中在 Windows 内核软件的开发与逆向上。之后，技术兴趣转向移动端，成为国内第一代 Android 逆向工程师。在工程实践之余从事软件逆向实训教学工作，为国内逆向行业培养人才。

电子邮箱：77919437@qq.com

参与章节：第 4 章 4.2 64 位软件逆向技术

张波

看雪首席版主，看雪论坛 ID 为 Blowfish，经验丰富的大龄程序员。从 1992 年上大学起接触计算机，1997 年读研期间接触网络并自学加解密技术，一发不可收拾，其时常在教育网 BBS“灌水”。喜多方涉猎，亦能抓住一点深入钻研，对逆向分析技术尤为痴迷。常驻看雪论坛，见证了论坛的风风雨雨，也结识了一些不错的朋友。

参与章节：第 5 章 5.1 序列号保护方式

第 17 章 17.5 关于软件保护的若干忠告

沈晓斌

看雪核心专家团队成员，看雪论坛 ID 为 cnbragon，“密码算法”版块版主，密码学专业硕士学位。对密码学的各个方面都有涉猎，尤其擅长密码学在软件保护中的应用，熟悉各种商业软件的保护机制。对 Rootkit 查杀、Windows 系统实时防护技术、漏洞攻击技术皆有较深入的研究。译作有《程序员密码学》《安全之美》，是加密算法库 CryptoFBC 的作者。

电子邮箱：cnbragon@vip.qq.com

参与章节：第 6 章 加密算法

周扬荣

周扬荣，硕士毕业于中科院软件所。擅长 C/C++ 和系统内核安全开发，具有丰富的内核安全开发经验。曾就职于阿里巴巴、360、北大计算机研究所，并于 2011 年与 wowocock、linxer 等一同创立麦洛科菲（mallocfree.com）信息安全培训机构，长期致力于信息安全技术的普及与推广，培养了大量活跃在百度、阿里巴巴、腾讯等一流公司一线的优秀安全人才。曾著有《程序员求职成功路：技术、求职技巧与软实力培养》等书籍，业余爱好包括旅游、历史、地理、古生物、宇宙学等。

电子邮箱：zyr@mallocfree.com

参与章节：第 7 章 Windows 内核基础

温玉杰

看雪核心专家团队成员，看雪论坛 ID 为 Hume。酷爱计算机，对操作系统、面向对象程序设计、网络及网络安全、加密与解密等较感兴趣并有较深入的研究。曾翻译出版《Intel 汇编语言程序设计（第四版）》。

电子邮箱：humewen@263.net

参与章节：第 8 章 Windows 下的异常处理

段治华

看雪资深技术权威，看雪 ID 为 achillis，常用网名“黑月教主”。13 岁时第一次接触计算机就被它的神奇深深吸引，高中时忙于学业，进入大学之后陆续接触了漏洞、脚本、破解、病毒、网络攻防和各种安全工具，成了“工具小子”，最终觉得编程才是王道，从此踏上编程之路，至今已近 10 年。目前主要研究方向为 Windows 底层开发、Rootkit、逆向分析及服务器运维，常用语言为 ASM、C、C++，正在学习 Python。学的越多，越感觉学海无涯——路漫漫其修远兮，吾将上下而求索！

电子邮箱：achillis@126.com

参与章节：第 8 章 Windows 下的异常处理
第 12 章 注入技术
第 13 章 Hook 技术

印 豪

看雪资深技术权威，看雪论坛 ID 为 Hying。擅长加壳技术，拥有独立创作的加密利器。

电子邮箱：newhying001@163.com

参与章节：第 9 章 Win32 调试 API
第 19 章 外壳编写基础

程勋德

看雪技术专家，看雪论坛 ID 为 Joen Chen，开源插件 DdvpDbg 的作者，来自湖南。资深程序员，曾就职于百度软件研究院，对 CPU 硬件虚化技术理论有深入的研究与独立的见解，对 VT 技术的实际应用也具有丰富的经验。熟悉 Windows、Linux 和 Android 平台的逆向工程技术，热爱安全行业，并希望在安全领域好好沉淀。

参与章节：第 10 章 VT 技术
第 22 章 22.2.6 利用 VT 技术

snowdbg

看雪核心专家团队成员，2005 年毕业于西北大学电子信息工程专业，反病毒工程师、某文玩店兼职伙计。从业 10 年，主要从事漏洞样本分析、木马样本分析、攻击溯源等工作。通过长期在反病毒岗位工作，总结了一套关于漏洞样本分析、Shellcode 编写及漏洞利用的实践经验。

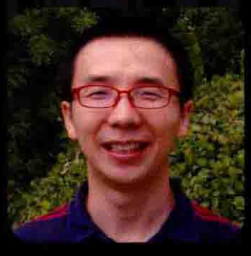
参与章节：第 14 章 漏洞分析技术

赵 勇

看雪技术专家，来自江苏江阴，环境工程硕士，高级工程师。目前从事化工产品开发、市场研究和市场拓展工作，擅长将管理工作与计算机技术有机结合，兴趣广泛，对计算机安全技术、系统应用技术、信息存储技术、组装技术等有积极的研究和心得。

参与章节：第 16 章 16.6 附加数据

唐植明



看雪技术核心权威，看雪论坛 ID 为 DiKeN，iPB（inside Pandora's Box）组织创始人。2002 年毕业于兰州大学计算机科学与技术专业，爱好逆向工程。在 2002 年编写了《加密与解密实战攻略》一书的算法部分。

参与章节：第 16 章 16.10 静态脱壳

李江涛

看雪技术核心权威，看雪论坛 ID 为 ljtt。喜欢学习编程技术，常用编程语言为 VC 和 MASM。对 PB、VFP 的反编译有深入的研究，编写过 DePB、FoxSpy 等程序。平时大部分时间都在计算机上耕作，最大的希望是能够领悟编程的精髓，写出一个自己比较满意的作品。

电子邮箱：shellfan@163.com

参与章节：第 17 章 17.2.2 SMC 技术实现

林子漾

看雪技术导师，看雪论坛 ID 为 forgot，看雪论坛外壳开发小组组长。熟悉 Win32 平台和 80x86 汇编，擅长代码的逆向，对壳的研究比较多。

电子邮箱：forgot@live.com

参与章节：第 15 章　15.4.1　虚拟机介绍

第 17 章　17.2.4　简单的多态变形技术

第 18 章　反跟踪技术

薛亮亮

15PB 信息安全教育教学部经理，北京蓝森科技有限公司联合创始人。从事信息安全工作近 10 年，曾参与安全取证软件开发工作，分析过多款商业软件，有丰富的项目经验及教学经验。目前专注于软件逆向、移动安全等领域。

参与章节：第 19 章　19.4　用 C++ 编写外壳部分

冯　典

看雪技术天才，看雪论坛 ID 为 bughoho。逆向安全工程师，擅长对软件进行逆向分析。对虚拟机壳和编译原理有特别的兴趣。在目前移动端兴起的大潮下，正将重心放到移动端软件的逆向安全研究上。

个人主页：bughoho.me

电子邮箱：bughoho@gmail.com

参与章节：第 3 章　3.2　反汇编引擎

第 20 章　虚拟机的设计

第 21 章　VMProtect 逆向和还原浅析

tankaiha

看雪核心专家团队成员。生于六朝古都南京，硕士研究生毕业，现任某研究所工程师，工作之余好与计算机为伴。2002 年接触汇编并热衷于病毒技术，后偶遇看雪学院，遂终日游戏于程序加密与解密中无法自拔。2006 年与 kanxue 及论坛中数位好友成立 .NET 安全小组，共同探讨 .NET 平台上的软件安全技术。

参与章节：第 24 章　.NET 平台加解密

罗 翼

看雪技术专家，资深程序员。从学习加解密知识开始接触编程，多年来对 Windows 底层机制有丰富的研究经验。后来由于工作需要，接触了 C++、ATL、COM 等技术。致力于研究各种 Moder C++ 元素的应用范围及其对降低程序复杂度所起的作用，密切关注 ISO C++ 及分布式计算相关内容的进展。

参与章节：第 22 章 22.2.1 跨进程内存存取机制
22.2.2 Debug API 机制
22.2.3 利用调试寄存器机制

罗 巍

飘云阁安全论坛创始人，资深逆向工程师，曾就职于阿里巴巴，现任广州啦咔网络科技有限公司逆向总监。擅长 Windows 和 macOS 逆向开发、iOS 越狱开发、App 协议级分析。2000 年前后一次偶然的机会加入看雪论坛，其间一直在探寻逆向工程的奥秘，在逆向路上失败过、沮丧过，但从未放弃过。

主页：http://www.chinapyg.com
参与章节：第 22 章 22.2.5 利用 Hook 技术

林小华

看雪资深版主，看雪论坛 ID 为 linhansh，武汉大学电力系统及其自动化专业毕业。现任看雪论坛“工具分区”版块版主，十年如一日，对版块的发展作出了重大贡献。

个人主页：http://blog.csdn.net/linhanshi
参与章节：第 15 章 15.3 加密壳
第 22 章 22.4 补丁工具

崔孝晨

看雪核心专家团队成员，看雪论坛 ID 为 hannibal，team509 创始人之一。上海公安学院工程师，软件工程硕士。2001 年起从事电子数据鉴定工作，其间因侦破“2009.7.18 上海私车额度拍牌网站遭 DDoS 攻击案”等重大案件荣立个人二等功。发表和翻译过《MS Word 加密算法弱点利用》《软件加密与解密》等文章和书籍。

参与章节：第 25 章 数据取证技术

郭春杨

看雪技术专家，看雪论坛 ID 为 Yonsm。对 Windows Mobile 有比较深入的了解，开发过 CeleDial 等广受好评的软件，多年来在逆向工程和软件安全方面保持着好奇心和关注度。曾在 ArcSoft 从事视频编解码和多媒体软件的开发和优化工作，使用汇编和 Intrinsics 指令，充分利用 CPU 和 GPU 的特性对 Video Codec 进行了极致优化。目前就职于支付宝移动技术团队，对 iOS 软件开发、逆向工程和系统分析依然兴趣盎然。

个人主页：www.yonsm.net
电子邮箱：yonsm@163.com
参与章节：附录 B 在 Visual C++ 中使用内联汇编

丁益青

看雪论坛资深会员，看雪论坛 ID 为 cyclotron。加密与解密及逆向工程爱好者，主要作品有 EmbedPE、IDT Protector、PEunLOCK 等。

参与章节：附录 D D.3 伪编译

周文斌

看雪论坛“编程技术”版块版主，北京娜迦信息科技发展有限公司创始人。擅长编程、病毒分析、密码学等，目前从事移动软件安全方面的研究。

参与章节：附录 D 加密算法变形引擎

关注微信，发送“加密与解密”
加入本书读者交流群

专家寄语

十几年来，尽管技术不断更替，看雪论坛一直都在专业安全领域坚韧地发展着，不断有人加入，不断有人分享，高手越来越多。

十几年来，很多安全论坛已经成了明日黄花。我本人是安全焦点论坛的核心成员，安全焦点论坛曾是中国乃至全球 0day 技术研讨能力最强的论坛之一，后来也转型为安全会议。

为什么看雪论坛会有如此强大的活力和进化能力？我觉得这与其创始人段钢对新人成长的细致关照密不可分。看雪论坛在入门文章的编写、入门帖的整理及精华提高帖的审校和传播方面做了大量的工作，不仅注重高手之间的研讨，还关注新人的上手和提高，仅从此书就能看出这一点。

软件逆向涉及很多枯燥的技术，例如汇编、操作系统底层、外壳对抗等，这很容易让新手放弃。本书注重由易到难的学习顺序，每个章节都提供了实战 CrackMe 程序。这很像玩游戏打关，书中的技术语言就是通关攻略，带领初学者一步一步成为高手——练习代替了说教，实战代替了知识点的罗列，每过一关就多一分自信、多一分成就感。

阅读此书，会让你在逆向和对抗技术方面收获满满。

知道创宇 CTO、COO　杨冀龙

认识看雪学院，源于 2001 年对加密和解密技术的痴迷。认识段钢，缘于同在电子工业出版社出书。段钢老师的《加密与解密》被奉为一代经典，看雪学院与《加密与解密》培养了一代又一代技术青年。而我，知道自己永远不可能追上段钢老师的步伐，转而专心研究数据恢复技术，从此沿着段钢老师的脚步一路前行，复制着版权输出、改版、再版的过程。欣闻段钢老师的经典作品《加密与解密》要出版第 4 版，特来表达自己的“不满”——这还让不让人活啊？不知道我退出江湖已经很多年了吗？

这次改版，让我们的友谊再次加深，因了《网络安全法》的实施，因了信息安全体系、取证技术的发展，我们永远是一对“若即若离”的兄弟。好兄弟，祝福你！愿你拓展自己的领域，在保持技术特质的前提下，在商业模式上越来越成功，为技术人才的发展做好榜样！

中国政法大学教授　戴士剑

Windows 软件逆向是一个难度比较大的技术方向，因此，在入门阶段有一本好书作为指引就显得尤为重要。我曾向很多年轻人推荐过《加密与解密》，这是一本真正源自实战、指导实战的技术书。

腾讯玄武实验室负责人　TK（于旸）

看雪论坛十几年来培养了众多软件逆向分析人才，这些人现在已经成为中国网络空间安全的中坚力量。《加密与解密》这本书非常经典。对那些对二进制代码分析和调试、病毒与木马分析、软件破解、版权保护感兴趣的人来讲，这本书是一本非常好的入门书籍，只要阅读、实践、钻研，就会有收获。

360 公司首席安全官　谭晓生

《加密与解密》第 1 版出版至今已经有十几个年头，十多年前我也曾买过一本。此次《加密与解密（第 4 版）》出版，受看雪学院段钢之邀为本书寄语，用两个字表达我的感受，那就是——力荐！一本书 18 年，从 Windows 2000 到 Windows 10；一个网站 18 年，从一个软件调试板块到现在的多平台、多板块……我佩服段钢的坚持。正因为这种坚持，他影响了一批又一批人，为国内安全行业的技术水平提高贡献了很大的力量。尽管本书名叫“加密与解密”，但内容覆盖了加密与解密、调试和反调试、破解与保护及漏洞分析和利用等技术。本书从基础知识开始，辅以各种实例，由浅入深，是安全研究人员、开发人员不可多得的入门及提高书籍。最后，希望看雪学院能够在知识分享和人才培养方面再接再厉，把更多的安全爱好者变成安全专家。

霸众信息（盘古团队）创始人、CEO　韩争光

30 年前，中国最早的一批黑客所活跃的领域就是软件加解密。今天，曾经的一个个社区、一个个 ID 都已消逝，成了让人唏嘘的回忆。成立于世纪之交的看雪学院成为中国软件加解密的旗帜，是段钢老师理念和坚持的必然。在逆向破解领域，一批批爱好者从入门到成为现在国内安全领域的专家，段钢老师的看雪论坛和《加密与解密》功不可没。我本人也是《加密与解密》最早的忠实读者之一，直到今天，在这本书的字里行间，我还能感受到那个年代技术爱好者的纯真和认真。愿看雪越来越好！

腾讯 KEEN 实验室和 GeekPwn 创办人　大牛蛙（王琦）

加密与解密是信息安全技术的核心基础。看雪论坛是国内安全人才的黄埔军校，对逆向人才培养功不可没。18 年，4 个修订版本，段钢始终坚持做逆向社区交流这件事，矢志不渝，令整个安全业界敬佩。

京东首席信息安全专家　Tony Lee

软件安全的本质是对抗博弈，而对抗博弈的关键在于知己知彼。《加密与解密》是每一个软件安全研究者的必读专业书籍，它能帮助我们快速构建完整的专业知识结构，更重要的是，它能赋予我们不断深入分析与改造软件系统的能力。

武汉大学计算机学院教授、博士生导师，全国网络与信息安全防护峰会联合发起人、执行主席　彭国军

安全可以分成很多领域，加密与解密是这些领域中最需要扎实功底的。多年来，难得看到像看雪这样在安全领域坚持这么久的团队。今天，看雪作为国内为数不多的专业技术团队，依然保持着对安全技术的纯真追求，《加密与解密》从 2001 年的第 1 版到 2018 年的第 4 版，正是看雪对技术追求最好的诠释。

Goodwell（龚蔚）

在大学里，我对计算机的兴趣始于病毒和游戏的加解密。作为专业书籍，《加密与解密》是一本向过去与未来致敬的技术佳品，既能体现 IT 产业特别是安全领域经典的传承，也是看雪多年的魅力所在，值得收藏与学习。

IDF 极安客实验室联合创始人　万涛（老鹰）

当年，《加密与解密》首次出版时引起了轰动。这本书是国内这个领域的第一本权威著作，我也仔细读过，获益良多。如今，《加密与解密（第 4 版）》与时俱进，新增了不少流行的内容，让我恨不得先睹为快。

腾讯 KEEN 实验室　wushi

加密与解密是安全领域永恒的话题。作为一名安全爱好者，我有幸见证了《加密与解密》这本书的发展历程。这本书全面剖析了软件调试的方方面面，是每一个安全从业者的必备书籍。

腾讯云鼎实验室负责人　killer

我买过《加密与解密》的第 2 版，虽说书名看上去像是密码学相关书籍，但实际上这本书更多地讲述了代码的破解与保护、程序的逆向分析与调试等软件安全领域非常实用的技术。我和我的很多同事、学生等都读过这本书。可以说，这本书伴随了几代软件安全从业者的成长。

清华大学网络科学与网络空间研究院教授　段海新

无论是开发人员还是信息安全工作人员，案头总会有一些书籍值得反复翻看，《加密与解密》正是其中之一。虽然书的名字是“加密与解密”，但其内容与传统密码学技术不同，覆盖了软件领域的大量关键技术，这些关键技术则构成了整个二进制攻防领域的基础。从最初“未公开的实现”类信息的发掘，发展至漏洞发现技术与漏洞缓解技术的全面对抗，技术的更新和发展使《加密与解密》迎来了它的第 4 版。这是一本历经 18 年仍然具有强大生命力的书，无论是新人还是老手，都一定会从中获益。

Inside Programming lu0，上海高重信息科技有限公司联合创始人　陆麟

逆向工程对我来说是一种智力游戏。时间走到 2018 年，尽管这个游戏中的某些具体方面可能已经过时，但蕴藏其中的上升到哲学层面的方法论永不过时。对那些永远充满好奇心的人，本书是一部很好的打怪升级指南。

NSFOCUS 研究员　scz

《加密与解密》一直是国内有志于从事二进制安全相关工作的技术人员的入门圣经，从 2008 年第 3 版出版到 2018 年第 4 版出版，时间过去了 10 年。在这 10 年中，我们迎来了 Web、移动互联网、云计算，IoT 也一步步走到了产业聚光灯之下。在这 10 年中，尽管技术的变化非常大，但回过头来审视，Windows 平台依然是企业办公的首选，而且随着越来越多的非 IT 企业开始进行数字化转型，企业办公的需求量必然还会增加。从安全行业的角度看，PC 桌面从个人终端病毒木马的时代升级到了企业用户定向木马、勒索软件的时代，黑灰产在 PC 上投入的兵力丝毫没有减少。而由于 PC 在 Windows 平台上的开放性，Windows 平台上黑灰产层面的硝烟不仅从来都没有散去，甚至专业性、对抗强度都在不断提高。因此，《加密与解密》这本经典之作的第 4 个版本的出版恰逢其时。

《加密与解密（第 4 版）》与时俱进，在当下需求强烈、炙手可热的一些领域，例如逆向分析技术、注入、Hook 技术、数据取证技术等方面，单独设置了章节，使得这本经典书籍成为真正意义上的 Windows 平台二进制安全领域的百科全书。非常感谢看雪社区和段钢先生十几年如一日为我们送出经典。我坚信，《加密与解密（第 4 版）》的问世，会为互联网安全技术的推广和人才的培养贡献不小的力量。

阿里巴巴安全部资深总监　张玉东

十几年前的一本《加密与解密》，培养了最早的一批安全爱好者，当年这本书的读者中的很多人已经成为今日网络安全领域的领军人。一直以来，加密与解密、调试与反调试、破解与保护、隐藏与取证都是安全领域最底层、最高深的内容，一本《加密与解密》能够带我们走入二进制安全的神秘殿堂。

小米首席安全官 陈洋

《加密与解密》是信息安全领域难得的经典著作，不仅注重基础知识与原理的讲解，还注重信息安全实战，体现了信息安全的基础性、实战性、实用性和趣味性。《加密与解密》和看雪论坛伴随着一代代信息安全人才成长，有效推动了各层面信息安全人才的培养，引渡无数人将信息安全作为自己的事业追求。信息安全就是要解决实际问题的，这本书及看雪论坛将持续指导大家探索信息安全的基本原理，解决实际的信息安全问题。

西安电子科技大学教授、博士生导师 沈玉龙

软件安全和加解密一直是软件行业最难掌握的技术方向之一，原因就在于涉及面太广，要成为个中高手，必须对硬件架构、汇编语言、调试技术、内核编程、操作系统等进行深入学习。面对众多技术细节，初学者往往不得其门而入。《加密与解密》成体系地讲解了信息安全领域的几乎全部关键技术，由浅入深并辅以实例，不愧是初学者的指路明灯！

北京小悟科技创始人、CEO，《Windows 环境下 32 位汇编语言程序设计》作者 罗云彬

与看雪学院结缘始于 2001 年。《加密与解密》第 1 版出版时我就买过一本，从中受益良多。这本书以由深入浅出的方式讲解了大量 Windows 内核编程的相关知识，包括注入 Hook、结构化异常、PE 文件结构等，不仅对安全研究人员有很大的帮助，对想成为 Windows 编程高手的人来说也是不可多得的教材，强烈推荐。

猎豹移动总经理 姚辉

记得几年前上大学的时候，我就是一边开着 IDA 和 OllyDbg，一边刷着看雪论坛，一边读着第 3 版的《加密与解密》，一点一点地走进了二进制安全的世界。段老师创办的看雪论坛，更是很多痴迷于二进制安全的朋友的精神家园。一件事情做一年容易，做三五年也不难，但如段老师一般，十几年坚持做一件事情，实在难能可贵。作为安全行业的新人，我想对打算学习二进制安全的朋友们说：《加密与解密（第 4 版）》是一本不可多得的、充满实践精神的好书，它一定会给你的学习带来巨大的帮助。

长亭科技 CEO 陈宇森

刚进入安全这个行业时，有几本书对我影响很大，其中一本就是《加密与解密》。这么多年过去，这本书居然出版了第 4 版。我自己也写过一本安全方面的书，很理解出书之不易、过程之烦琐。相信《加密与解密（第 4 版）》会成为我和我的团队进入二进制世界的灯塔。感谢段钢老师！

Joinsec 创始人 余弦

我在上大学时第一次接触《加密与解密》，对逆向技术的学习就是从此开始的。多年过去，现在这本书的第 4 版就要出版了。《加密与解密》不仅是一本书，在它的背后有看雪论坛中大量有关这本书技术内容的交流，这些内容正是这本书的第二生命——读书的同时在看雪论坛找到志同道合的朋友是一种享受！

几维安全联合创始人、CEO　范俊伟

本书技术覆盖面广、可操作性强，称得上国内最完整、最实用的底层安全技术书籍，曾指引众多热爱技术的人进入安全行业，而其中的许多人已经成为相关企业的技术骨干。看雪论坛有着深厚的技术积淀和人才积累，这本书中介绍的所有技术均有相关资深安全从业者活跃于论坛，可为安全技术爱好者及想进入安全行业的人提供交流互动和提升技术能力的平台。

本书详细而透彻地讲解了系统底层的基础知识和安全核心技术的实践技能，基础知识的介绍包括 Windows 异常机制、内核基础、调试器、加密算法等，核心技术方面则有反汇编技术、静态分析技术、动态分析技术、代码注入技术、Hook 技术、漏洞分析技术、脱壳技术等，这些知识都是底层安全从业人员和高级黑客必须掌握的。

启明星辰 ADLab 高级安全研究员，看雪论坛“智能设备”版块版主　甘杰（gjden）

在从事反病毒工作的前几年里，《加密与解密》是少数几本对我和同事们帮助极大的书籍之一。相信《加密与解密（第 4 版）》依然会是反病毒、系统安全、软件保护等方向的权威参考和案头必备工具书。

Palo Alto Networks 安全研究员，看雪论坛“Android 安全”版块版主　Claud Xiao

编辑寄语

手握即将付梓的《加密与解密（第 4 版）》清样，默念着与看雪相伴十几年的专家朋友们的新版致辞，作为看雪图书的出版者，心中感慨油然而生。

近 20 年前的我刚走出工科院校不久，是个出版行业的新兵。出于对硬件技术的专业兴趣，我经常在底层相关的网站上浏览内容。当发现看雪论坛时，真仿佛见到大学里对技术痴迷的大神，顿时眼前一亮！从第一次与看雪取得联系到《加密与解密》（第 1 版）面世，经历了几百个日夜的努力。在那个计算机普及类图书铺满书店货架的年代，这本书看似另类，实则卓尔不群，很快引起了专业出版领域的强烈关注。

18 年光阴逝去，沧海桑田间，《加密与解密》的前 3 版已经成为几代人在安全领域的领路者。今天的看雪，人并没有老去，他更加执着于技术，也更加精进于每一个技术要点；看雪论坛也已升级为公司化运作模式，并成为国内该领域的翘楚；《加密与解密（第 4 版）》则将技术的沉淀与知识的更新进行了高度融合，不仅充分增量扩容，更实现了进化般的质变。

学习本书无疑是软件安全相关工作者提升专业水准的必行通道。不积跬步，无以至千里。看雪这种对技术探索 20 年矢志不渝的精神，体现在书中的字里行间。相信读者在阅读这本经典之作的同时，也能够被这种精神所激励，更好地走出属于每个人的技术之路。

《加密与解密》策划编辑　郭立

15 年前，初入职场，便闻《加密与解密》大名。15 年后，有幸成为《加密与解密（第 4 版）》的责任编辑，细读书中一字一句，深刻理解了这本书为什么会成为软件安全领域图书的里程碑。

写作这么厚的一本书，不仅需要执着和坚韧，更需要纯粹的专注和平静。在与段钢老师一起讨论和修改书稿的近两年中，我获益良多，这段与二进制相伴的有趣日子，也是我职业生涯中极具价值的一课。

愿这本凝聚众多高手智慧的厚重的书，能一如既往，帮助它的读者迎接来自技术的“暴击”，成为新一代的行业中坚。

《加密与解密（第 4 版）》责任编辑　潘昕