看雪论坛鼎力打造

加密与解密

（第二版）

段钢 编著

電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

加密与解密

（第二版）

段　钢　编著

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

内 容 简 介

软件保护是维护软件开发人员利益的主要手段，是软件开发过程中的重要环节。为了跟上技术发展的步伐，本书在第一版的基础上，更新了第一版中的过时内容，补充了许多新技术。本书全面讲述了Windows平台下的最新软件加密与解密技术及相关解决方案，采用循序渐进的方式，从基本的跟踪调试到深层的拆解脱壳，从浅显的注册码分析到商用软件保护，几乎囊括了Windows下的软件保护的绝大多数内容。本书共分三个部分。第一部分介绍与加密和解密技术相关的基础知识。第二部分全面讲述各种最新的软件加密与解密技术及方法，如静态分析技术，动态分析技术，序列号，警告窗口，时间限制，加密算法MD5、SHA、RSA、ElGamal等。第三部分主要介绍PE文件的知识，如增加文件功能、加壳与脱壳、补丁技术等。

本书是密界一流高手的呕心之作，通过解析大量实例来展现软件加密与解密的最深处，是软件开发人员不可多得的一本专业参考书。

图书在版编目(CIP)数据

加密与解密/段钢编著. —2版—北京:电子工业出版社,2003.6
ISBN 7-5053-8648-4

Ⅰ.加… Ⅱ.段… Ⅲ.①软件—密码—加密②软件—密码—解密译码 Ⅳ.TP311.56

中国版本图书馆CIP数据核字(2003)第026106号

责任编辑:郭 立 毛兆余
印 刷:北京东光印刷厂
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
经 销:各地新华书店
开 本:787×1 092 1/16 印张:33.75 字数:861千字
印 次:2004年1月第4次印刷
印 数:5 000册 定价:49.00元(含光盘1张)

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。联系电话:(010)68279077。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。

前　言

自计算机诞生之日起，其技术的发展可谓日新月异，各种新技术、新思路不断涌现。个人计算机操作系统也经历了 DOS，Windows 3.x，Windows 9x，Windows 2000 及 Windows XP 的历程。各种应用软件从最初的几个、几十个字节发展到现在的动辄几张光盘，成千上万的共享软件和商业软件越来越庞大，技术内涵也日趋复杂。一款优秀的软件，其技术秘密往往成为他人窃取的重点。作为软件开发人员，为了保护自己辛辛苦苦开发的软件不轻易被他人“借鉴”，有必要对软件的保护（加密）和破解（解密）技术进行研究。但是，软件保护和破解方面的资料目前比较匮乏，许多软件开发人员不得不自行摸索，导致在重复劳动中走了不少弯路，耗费了大量的时间和精力。随着软件以共享方式在网络上发布这种方式的流行，软件保护和数据加密技术的迫切性被越来越突出地表现了出来。

软件加解密的发展历史

我们通常是随着操作系统的不断升级来划分相应的软件，所以划分软件加解密的发展历史就是操作系统发展的历史。

1．DOS 时期

这个时代的软件主要是正式版和功能不全的 Demo 版以及一些磁盘防拷贝保护，很少有所谓的共享软件（Shareware）。所以 DOS 时代所谓的解密通常是去掉软件中的某些限制或跳过原版磁盘检查，然后通过广大业余的 BBS 提供下载。但值得一提的是，这个时代的软件由于 16 位操作系统很容易接触到系统底层的原因，而导致个别软件保护方式异常强悍，又因为在 16 位平台上很难区分系统领空和程序领空而导致天然的破解跟踪困难，所以这个时代的软件保护机制两极分化很严重。

2．Windows 95 早期

当 Windows 95 出现的时候，很多人不适应这个平台，它上面的加解密资料奇缺，对许多人来说就像做了一场恶梦。这段时期共享软件渐渐地盛行起来，采用序列号保护的共享软件越来越多。由于当时许多程序员对刚刚出现的 Windows 95 不了解，感觉有些手足无措，编制的软件在加密部分都比较脆弱，所以那时候的序列号加密方案特别脆弱。

3．Windows 95 末期

其实这段时期应该是 Windows 95 和 Windows 98 共存的时期。在这个时期，程序员已经对 Windows 9x 这个系统了如指掌，一些需要较高编程技巧、与系统核心等底层联系紧密的软件纷纷出笼。这个时期，共享软件大多还是采用序列号加密方式，但其序列号通常经过复杂的计算，所以很难像早期的软件一样，随随便便就能被解密。

4．Windows 2000/XP 时期

这段时期就是 Windows 9x 和 Windows 2000/XP 共存的时期。这时，各种软件的加密外壳泛滥，特别是各种专用加壳软件的出现，大大地提高了软件的保护质量；同时，解密技术也不断提高，各种新式的解密工具随即出现。此时的序列号加密越来越多地采用密码学中不可逆的加密算法，使得解密的过程越来越像高等数学的研究。软件解密者要想得到正确的序列号就必须对各种成熟加密算法有很深的了解，或者找出软件加密算法的漏洞（像 WinRAR，CloneCD 等软件的 Keygen 就是利用 ECC 椭圆算法的加密漏洞而编制出来的）。

关于本书

2000 年初，作者想找一些研究加解密的朋友交流一下，但十分令人遗憾的是，那时国内这方面的技术资料很缺乏，不成系统，大家的交流也有限，因此就建了一个主页“看雪学院”，与大家共同探讨加密与解密的知识。这个主页是当时国内惟一一个从技术角度研究加解密的站点，并在广大网友的支持下，健康地成长了起来。后来，主页提供的软件调试论坛成了国内知名的加解密技术论坛，吸引了密界众多高手。大家以知识共享的精神，无私地将自己所知的技术奉献出来了，至今为止原创了 2500 余篇文章，极大地推动了国内加解密技术的发展。

这是一本很难写的书，因为当时这是一个全新的领域。从 Windows 95 面世以来的 6 年内，市面上没有一本这方面的书，网上也缺乏相关资料。为了填补国内 Windows 平台上加密与解密书籍的空白，作者与软件调试论坛的密界一流好手努力合作，克服种种困难，于 2001 年 9 月推出了国内第一本全面介绍 Windows 平台下软件加密与解密技术的书籍，这就是本书的第一版《加密与解密——软件保护技术及完全解决方案》。

在第一版中，我们试图从软件加密和解密这两个方面对当今流行的软件保护技术进行了分析。希望读者看过本书之后，能够对各种流行的软件保护与破解技术有所了解。

第一版一面世就得到了广大读者的喜爱和认可，获得了 2002 年全国优秀畅销书奖（科技类）！在全国很多计算机专业书店获得了名列前茅的销售业绩，而且一年来在著名的华储网销售排行中都被排在前几名内。次年，本书在台湾发行了繁体版，得到了台湾读者的热烈欢迎。

为了跟上技术发展的步伐，作者花费了 6 个月时间做准备，6 个月时间进行写作，汇集了国内顶尖软件调试论坛（看雪论坛）的众多密界一流好手，以本书第一版为基础，更新了第一版的大部分内容，最后完成了本书的第二版《加密与解密》。这本 500 多页的图书，几乎囊括了 Windows 下软件保护的绝大多数内容，从基本的跟踪调试到深层的拆解脱壳、从浅显的分析注册到商用的软件保护，其跨度之广、内容之深，国内至今尚无同类出版物能与之比肩。

内容导读

第二版是在第一版基础上写成的，删除了第一版中的过时内容，补充了许多新技术。全书有一半的内容与第一版不同，结构更加合理。补充和加强了 Windows 与 Unicode、代码逆

向分析、IDA 详细操作、SoftICE 符号调试技术、OllyDbg 操作、密码学算法应用、VB 的 Pcode 跟踪、增加 PE 文件的功能、SEH 技术、脱壳技术等。

什么是 API？什么是 Unicode？什么是逆向分析？Winodws 9x 与 Windows 2000/XP 上的加解密究竟有什么不同？只有了解这些基础知识，在加密与解密过程中才能有的放矢地处理各种问题。本书的基础篇（第 1 章“基础知识”和第 2 章“代码分析技术”） 将系统地解答这些问题。

在进行软件解密的过程中，一个首要问题是对被解密的软件进行分析，这部分就是静态分析与动态分析技术。本书以极大的篇幅讲述了这两种分析技巧，包括逆向工程必备工具 IDA 的详细操作，最新 SoftICE 和 OllyDbg 的操作等。这些内容可以在第 3 章“静态分析技术”与第 4 章“动态分析技术”中找到。

一些软件作者对软件保护方案的策划与实施很不以为然，他们往往自以为是的保护在解密者眼中不堪一击。希望本部分能让这些软件作者了解一些软件攻击的方法，以便更好地保护自己的作品。在这个年代，研究加解密不掌握点密码学的知识是不可思议的。第二版详细讲解了 MD5, SHA, CRC, RSA, ElGamal 等算法在软件保护方面的应用，并且光盘上提供了实例的源码！这些内容可以在第 5 章“软件保护及其弱点”与第 6 章“加密算法”中找到。

现在所使用的语言无非是两种：一种是解释执行的语言，另一种就是编译后才能够执行的语言。解释语言的最大弱点之一就是能被反编译，因此其保护的重点应放在如何防止反编译上。这些内容可以在第 7 章“反编译语言”中找到。

PE 是 Windows 上可执行文件的格式，熟知 PE 文件将有助于对操作系统的深刻理解。如果你知道 EXE 和 DLL 里面的奥秘，将成为一名知识更加渊博的程序员。本书用大量篇幅，图文并貌地详细讲解了 PE 格式（第 8 章“PE 文件格式”）。

在掌握 PE 格式后，就可随心所欲地对 PE 文件做“手术”，进行二次开发，如增加菜单、按钮等功能。这部分将带你走进另一个计算机的世界里去（第 9 章“增加 PE 文件功能”）。

SEH 的出现已非一日，但有关 SEH 的知识资料却不是很多。SEH 不仅可以简化程序的错误处理，使程序更加健壮，还被广泛应用于反跟踪和加密中。本书从解密角度讲述了 SEH 的机理，同时讲述了其他各种反跟踪技术，如 Anti-Debug、花指令等。软件作者可以将这些技术应用到自己的软件中去，以加强软件的反跟踪能力（第 10 章“反跟踪技术”）。

现在，越来越多的软件都采用了加壳保护。当在软件分析和汉化过程中，脱壳是必不可少的一步。第 11 章“加壳与脱壳”详细介绍了各种壳的脱壳技巧，读者可以在自己的软件中运用这些壳中的先进反跟踪技术。

第 12 章“补丁技术”介绍了文件补丁和内存补丁技术，同时重点讲解了 SMC 技术在补丁方面的应用。学习补丁是一件很有意思的事情。

商用软件保护技术实际就是对商业软件加密的技术，真正有价值的商业软件一般都会采用这些技术来保护。第 13 章“商用软件保护技术”讲解了常见的商业保护技术，如软件狗，Vbox，SalesAgent，Flexlm 等保护，而且对这些保护的优缺点进行了分析。

对读者的要求

本书适合以下读者。

- 对软件加密与解密感兴趣的读者
- 对软件保护感兴趣的软件开发人员
- 对逆向工程感兴趣的读者
- 对调试技术感兴趣的读者

使用本书需要具备以下知识。

- 汇编基础知识。此类书籍市面上很多，如《IBM PC 汇编语言程序设计》等。
- 应了解 C 语言。了解 C 语言的某些知识是有帮助的，但不是必须了解。
- Win32 编程。不管研究加密与解密，还是编程，都必须了解 Win32 编程。Win32 编程就是 API 方式的 Windows 程序设计，学习 Windows API 能使你更深入地了解 Windows 工作方式。此类书籍有 Charles Petzold 所著的《Windows 程序设计》，该书堪称经典之作，它以 C 语言为讲解平台。另一本书是罗云彬所编著的《Windows 环境下 32 位汇编语言程序设计》，它以 Win32 汇编为讲解平台。

到此为止，作者将不再假设你已经具有任何加解密的经验了。

致谢

感谢我的母校同济大学，她的“同舟共济、自强不息”的同济精神一直指导着我的工作和学习！

感谢电子工业出版社计算机图书事业部（http://jsj.phei.com.cn）对本书的大力支持！感谢本书责任编辑郭立女士和毛兆余老师所做的大量工作。

同时，也要感谢那些共同参与第一版组稿的软件调试论坛的众多密界一流好手，是他们的参与才让此书得以完成。这次的第二版改动较大，参考引用了如下朋友在第一版中参与的文章：

1．Blowfish（http://www.shieldsoftware.com/）参与的“软件保护技术”、“Anti-Debug”、“Java 程序反编译”；

2．DREAMtHEATE 参与的“Windows 消息机制”；

3．DDXia[CCG]参与的“远程调试技术”，“补丁技术”；

4．Passion 参与的“FileMon 的使用”、“TimeLOCK 保护”；

5．Ljtt 参与的“花指令”；

6．Arbiter 参与的“FrogsICE 使用简介”、“CRC 原理篇”；

7．Ajj（http://ajj.126.com/）参与的“IceDump 和 NticeDump 的使用”；

8．Fisheep（fisheep@sohu.com）参与的“VBOX4.3”、“SalesAgent 保护技术”、“FlexGen 工具用法”、“利用 FlexLm SDK 解密”、“浮点指令小结”；

9．吴朝相（http://www.souxin.com/）参与的“常用断点设置技巧”及“认识壳”；

10．mr.wei 参与的“DeDe 用法”；

11．邹丹（http://www.zoudan.com）的论文“关于 Windows 95 下的可执行文件的加密研究”；

12．TiANWEi（http://winice.yeah.net）参与的“SoftICE 指令手册”。

在第二版的编写过程中特别感谢：

1．Hume（http://humeasm.yeah.net/）提供的“指令优化一文”；

2．老罗的缤纷天地（http://www.luocong.com/）提供的“CRC32 实践篇”与“奇妙的Base64 编码”两篇文章及实例；

3．夜月提供“Blowfish 算法解密”一文；

4．娃娃（王凌迪）提供的“MD5 算法”资料；

5．Blowfish 的“ReVirgin 使用指南”，“挫败隐藏在 SEH handler 中的保护”。

同时，也要感谢 Sun Bird，Hying，Spring，pll621，Ajj，小楼，Ljtt，Arbiter，Aming，Cooljiang，洋白菜，WinDos2K，小牧童等软件调试论坛的众多朋友的支持和帮助！论坛网友的一言一行都已融进了本书的文字里，实在无法一一列举。另外，特别感谢 CCG 团体给予的技术支持！

关于配套光盘

本书所有实例及源码均在配套光盘里提供，大部分实例是使用 Microsoft Visual C++ 6.0 开发和测试的。

由于版权问题，配套光盘仅提供书中提到的免费软件或共享软件。如果从学习角度需要使用那些有版权的软件，建议用搜索引擎查找（如 www.google.com）。

光盘提供的软件经过多方面检查测试，绝无病毒。但一些加解密工具采用了某些病毒技术，因此部分代码与某些病毒的特征码类似，会造成查毒软件的误报。

请勿将光盘的文件做成虚拟光驱，并跟踪调试虚拟光驱上的实例，以免出现一些无法解释的错误。建议将文件拷贝到硬盘，并去除只读属性再调试。

反馈信息

我们非常希望能够了解读者对本书的看法。如果有什么问题或有自己的加、解密故事，欢迎发到作者主页的论坛里，我乐意回答朋友们提出的任何合理的问题，因为当我努力回答这些问题时，也会从中获益匪浅。

作者主页　　http://www.pediy.com

　　http://toye.yeah.net

段　钢

目　录

第1章 基础知识

研究软件加密与解密，必须要了解一些 Windows 系统的基础知识。比如不同版本的 Windows 对 ASCII 码与 Unicode 码支持情况，什么是 API 函数，注册表结构等知识。掌握这些后，在加密与解密过程中才能有的放矢地处理各种问题。

1.1 文本编码方式

美国信息交换标准码（ASCII：American Standard Code for Information Interchange）起始于 20 世纪 50 年代后期，并最终在 1967 年定案。现代的 ASCII 是一个七位的编码标准，包括 26 个小写字母、26 个大写字母、10 个数字、32 个符号、33 个控制代码和一个空格，总共 128 个代码。由于计算机通常用“字节（byte）”这个八位的存储单位来进行信息交换，因此不同的计算机厂家对 ASCII 进行了扩充，增加了 128 个附加的字符来补充 ASCII，它们的值在 127 以上的部分是不统一的。例如 ANSI、Symbol、OEM 等字符集，其中 ANSI 是系统预设的标准文字存储格式。表 1-1 列出了用十六进制（Hex）与十进制数（Dec）表示的部分常用字符的 ASCII 值。

Unicode 是 ASCII 字符编码的一个扩展。Unicode 据称是使用“宽字符集”，所以本书把宽字符（Widechars）和 Unicode 作为同义语。为了将成千上万的文字统一到同一个编码机制之下，不管是东方文字还是西方文字，在 Unicode 中一律用两个字节来表示。也就是说，Unicode 是一种双字节编码机制的字符集，使用 0～65 535 之间的双字节无符号整数对每个字符进行编码。Unicode 中，所有的字符都是 16 位，包括所有的 7 位 ASCII 码都被扩充为 16 位（注意，高位扩充的是零\x0）。如英文字串“pediy”，它的 ASCII 码是：

0x70 0x65 0x64 0x69 0x79

其 Unicode 码的十六进制是：

0x0070 0x0065 0x0064 0x0069 0x0079

Intel 处理器在内存中将以如图 1.1 所示的形式存放。存放时，低位字节存入低地址，高位字节存入高地址，也就是说，是以相反的次序存入的。

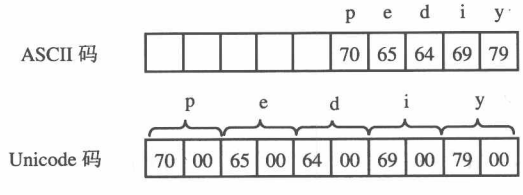

图 1.1 内存中的 ASCII 码与 Unicode 码