

完全掌握

加密解密

实战
超级手册

加解密高手
技术档案

深入内涵，全盘理解，掌握精髓

· 来自安全技术一线培训师与程序员的经验之谈，从入门到实践，深入浅出地介绍最新、最实用的软件加解密技术
· 结合实战案例，详析编程思路，教你掌握方法，快速成长为加解密职业高手

DVD

7小时

多媒体视频讲解

张晓新 孙国岭 杨平等 编著



机械工业出版社
China Machine Press

完全掌握

加密解密实战

超级手册

TP309.7

2217

张晓新 孙国岭 杨平等 编著



机械工业出版社
China Machine Press

本书紧紧围绕软件的加密与解密来进行讲解,在详细讲述加密/解密技术的同时,还介绍了相应的实现原理,并配合案例分析,使读者能够系统、深入地了解加密/解密技术,能够更深层次地理解他人的编程思路,从而更好地提高自己的编程水平。全书共分为14章,包括:加密解密技术基础、常用代码分析工具、不同的加密解密算法、静态分析解密工具、动态调试解密工具、辅助工具、壳的不同应用技术、为程序打上补丁、网络验证技术、常用加密工具、不同的注册保护方式、编辑安装包程序、不同软件的保护措施、常用软件加密解密技术等。

本书讲解通俗,深入浅出,注重实践,适用于广大计算机软件加密解密技术新手、爱好者,适用于软件开发从业人员和编程爱好者,也非常适合大专院校相关专业学生,以及有志于从事安全或加解密行业的准专业人员快速掌握实用技术。

封底无防伪标均为盗版

版权所有,侵权必究

本书法律顾问 北京市展达律师事务所

图书在版编目(CIP)数据

完全掌握加密解密实战超级手册 / 张晓新 孙国岭 杨平等 编著. - 北京: 机械工业出版社, 2010.5

ISBN 978-7-111-30360-2

I. ①完… II. ①张… ②孙… ③杨… III. ①软件—密码—加密 ②软件—密码—解密译码
IV. ①TP311.56

中国版本图书馆CIP数据核字(2010)第064433号

机械工业出版社(北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑: 夏非彼 迟振春

北京科普瑞印刷有限责任公司印刷

2010年5月第1版第1次印刷

188mm×260mm • 27.75印张

标准书号: ISBN 978-7-111-30360-2

ISBN 978-7-89451-489-9 (光盘)

定价: 55.00元(附1DVD)

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

客服热线: (010) 88378991; 82728184

购书热线: (010) 68326294; 88379649; 68995259

投稿热线: (010) 82728184; 88379603

读者信箱: booksaga@126.com

完全掌握

加密解密实战 超级手册

加解密高手
技术档案

多媒体教学光盘

DVD

多媒体教学光盘使用说明

32 个

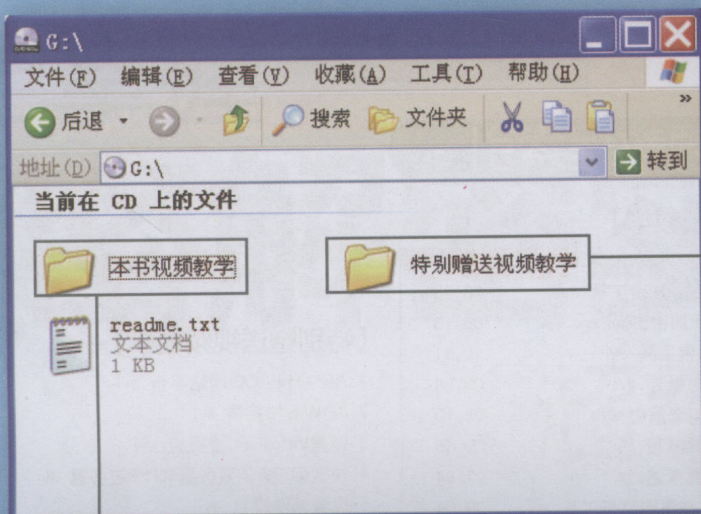
与本书配套视频教学文件

28 个

赠送与黑客技术
相关的视频教学文件

总播放
时长近 7 小时

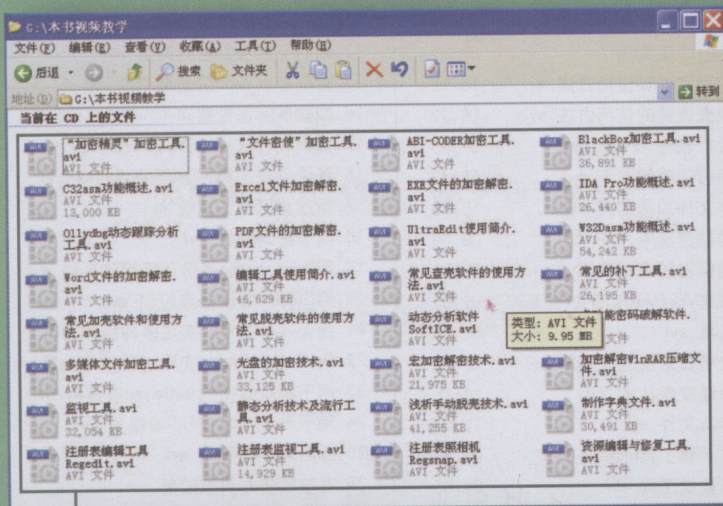
1. 本书光盘附赠作者亲自录制的多媒体音视频讲解，涵盖32个本书关键课程的视频教学，28个常用黑客工具与安全技术课程，视频教学播放总时长近7小时，超值实用。



黑客与安全工具技术视频教程

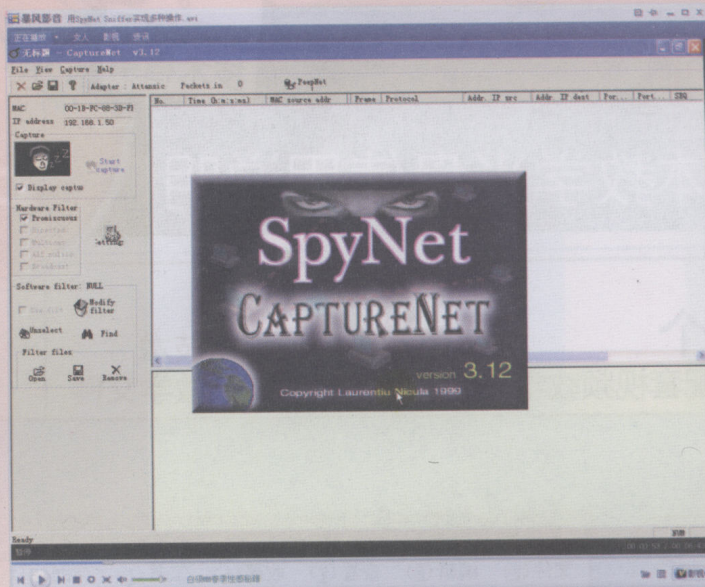
本书关键内容的视频教程

2. 视频教学存放在本光盘的两个文件夹中，打开光盘下的文件夹，即可找到视频教学文件。



视频教学文件

3. 双击光盘下的视频教学文件, 即可以使用Windows 的视频播放器Windows Media Player播放, 如果你安装了其他的视频播放软件, 如暴风影音, 同样也可以使用这些软件来播放教学视频。



多媒体视频教程索引

【本书视频教学】

1. “加密精灵”加密工具.avi 06:42
2. “文件密使”加密工具.avi 08:28
3. ABI-CODER加密工具.avi 06:15
4. BlackBox加密工具.avi 10:11
5. C32asm功能概述.avi 03:58
6. Excel文件加密解密.avi 08:10
7. IDA Pro功能概述.avi 09:46
8. IDA Pro功能概述.avi 07:54
9. Ollydbg动态跟踪分析工具.avi 09:04
10. PDF文件的加密解密.avi 09:47
11. UltraEdit使用简介.avi 07:58
12. W32Dasm功能概述.avi 18:09
13. Word文件的加密解密.avi 10:32
14. 编辑工具使用简介.avi 14:45
15. 常见查壳软件的使用方法.avi 03:23
16. 常见的补丁工具.avi 08:32
17. 常见加壳软件和使用方法.avi 10:19
18. 常见脱壳软件的使用方法.avi 06:22
19. 动态分析软件SoftICE.avi 07:29
20. 多功能密码破解软件.avi 02:48
21. 多媒体文件加密工具.avi 15:48
22. 光盘的加密技术.avi 08:39
23. 宏加密解密技术.avi 06:24
24. 加密解密WinRAR压缩文件.avi 02:07
25. 监视工具.avi 08:30
26. 静态分析技术及流行工具.avi 12:23
27. 浅析手动脱壳技术.avi 14:15
28. 制作字典文件.avi 10:01
29. 注册表编辑工具Regedit.avi 09:39
30. 注册表监视工具.avi 04:35
31. 注册表照相机Regsnap.avi 04:12
32. 资源编辑与修复工具.avi 09:34

【特别赠送视频教学】

1. ASP+PHP+CGI网站平台.avi 09:58
2. X-Way扫描器.avi 05:20
3. 创建Virtual PC虚拟机.avi 06:18
4. 快速架设ASP服务器和PHP服务器.avi 04:54
5. 设置系统项目.avi 04:57
6. 设置邮箱的反垃圾功能.avi 01:52
7. 设置桌面项目.avi 03:39
8. 生成木马服务器.avi 03:21
9. 使用FinaData恢复数据.avi 08:08
10. 使用驱动精灵备份硬件驱动.avi 01:47
11. 顺利下载被保护的图片.avi 04:09
12. 顺利下载被加密的网页.avi 05:32
13. 完美卸载2008的杀毒功能.avi 03:02
14. 微软反间谍专家.avi 11:09
15. 伪装成可执行文件.avi 04:53
16. 系统监控工具: RealSpyMonitor.avi 04:21
17. 新建虚拟操作系统.avi 05:17
18. 星号密码查看.avi 05:12
19. 用Drive Image备份还原操作系统.avi 05:31
20. 用QuickIP实现多点控制.avi 10:44
21. 用SpyNet Sniffer实现多种操作.avi 06:43
22. 用URL Warning实现远程信息监控.avi 03:55
23. 用于捕获数据的snifferpro嗅探器.avi 04:15
24. 用于局域网嗅探IRIS嗅探器.avi 08:29
25. 邮箱炸弹的防范.avi 04:24
26. 有效预防网页被破解.avi 09:13
27. 预防远程控制的“QQ远控精灵”.avi 04:06
28. 运行组策略.avi 03:23

随着网络技术的发展,在互联网上进行文件传输、电子邮件商务往来存在着许多不安全因素,特别是在网络上传输的一些大公司的机密文件。因此,数据安全已成为不可回避的话题。

加密与解密技术可有效确保用户的数据信息不被别人拦截和窃取,但加密与解密是一种辩证的关系,两者相互矛盾、相互依存、缺一不可,解密可以促进软件加密水平的进一步提高,加密水平的提高又需要解密技术的验证。

本书内容

本书以图释、标注、指引线框等丰富的图解手段,再辅以最易懂的语言,不但介绍了加密解密技术的一般方法、步骤,而且可使读者在了解日常加密解密技术的前提下,注重对操作技巧的剖析,使读者在遇到不同的疑难时,能够尽可能的心中有数,采取相关的方法来制定相应措施。全书共分为14章,主要内容包括:常用代码分析工具、加密解密算法、静态分析工具、动态调试工具、辅助工具、壳、补丁、网络验证、常用加密工具、注册保护方式、安装包程序、不同软件的保护措施以及常用软件加密解密技术等。

本书特色

本书以情景教学、案例驱动与任务进阶为鲜明特色,在书中可以看到一个个生动的情景案例。通过完成一个个实践任务,读者可以轻松掌握各个知识点,在不知不觉中快速提升实战技能。

- 从基础到实践,完全站在实用的角度,介绍加密解密技术。与大量传统教材不同的是,突出了实用性和案例分析,所举实例来自于实际应用,学以致用,真正解决问题。
- 通俗易懂,结合图解、标注和多媒体教学,使神秘、高深、难以掌握的加密解密技术学习起来省时、省力,易于上手,非常适合新手、大专院校学生,以及有志于从事安全或加密解密行业的准专业人员快速掌握实用技术。
- 紧扣“理论+实战+图文+视频=全面提升学习效率!”的主导思想,详细分析每一个操作案例,以实现读者用更少的时间尽快掌握加密解密技术的操作,并对实战过程中常见问题作必要的说明与解答。
- 当前最新技术、热点技术、常用相关工具软件都在本书有所涉及,对加密解密的编程技术、方法与思路也做了重要讲解,并通过实例介绍综合技术的运用手段,能够达到举一反三的效果。

- 超值的多媒体配套教学光盘。在随书多媒体配套教学光盘中，尽可能使读者在阅读时参考光盘中的视频教程，轻松、快速地实现自己的网络化办公需求。

读者对象

本书面对的读者可分为 3 个层次：

- 入门读者。这类读者往往需要为自己的日常文档、邮箱等加密，或简单破解忘了密码的文件。本书注重实用，可以满足这类读者的需要。
- 进阶读者。这类读者对诸多专业软件和技术原理一知半解，达不到系统掌握的阶段，所以他们的实践运用能力也就总停滞不前。本书注重学好理论基础并举一反三，达到各种技术的综合运用，完全适合这类读者。
- 从业人员。这类读者需要各种技术的灵活运用和丰富的临场发挥，成功的实例是该类读者不断提高自己的阶梯，并有助于拓展视野，直接获得实践经验。

本书由多名经验丰富的高校教师及安全专家编写，其中大多数长期从事安全技术教学软件开发和培训工作，同时也得到了众多网友的支持，在此一并表示衷心的感谢。参与本书编写的老师有：刘双红负责第 1 章，陈艳艳负责第 2 章，段玲华负责第 3 章，杨平负责第 4 章，余建国负责第 5 章，张晓新负责第 6、7、8 章，李防负责第 9 章，李伟负责第 10 章，孙国岭负责第 11、12 章，安向东负责第 13、14 章，最后由武新华统审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有失误、遗漏之处，因此，还望大家以宽容为本，本着共同探讨、共同进步的平和心态来阅读本书。作者心存谨敬，随时恭候您提出宝贵意见，联系邮箱：lly69@vip.sina.com。

编者

2010 年 3 月

目录

前言

第 1 章 初识加密解密技术.....	1
1.1 加密解密技术基础.....	2
1.1.1 密码学简述.....	2
1.1.2 常用汇编语言命令.....	2
1.1.3 破解密码的常用方式.....	4
1.1.4 壳的作用和分类.....	5
1.2 文件读写与动态链接库文件.....	6
1.2.1 INI 文件与自定义文件的读写.....	6
1.2.2 在 Delphi 中建立和使用 DLL 文件.....	10
1.2.3 DLL 文件的调用方法.....	12
1.3 设计与发布包组件.....	14
1.3.1 包组件概述.....	14
1.3.2 设计与发布包组件.....	15
1.3.3 安装与卸载包组件.....	17
1.4 解密与注册保护.....	19
1.4.1 解密方式.....	19
1.4.2 注册保护方式.....	19
1.5 试用期限限制功能.....	21
1.5.1 试用次数限制功能.....	21
1.5.2 试用天数限制功能.....	25
1.5.3 试用日期限制功能.....	31
1.5.4 执行时间限制功能.....	36
1.5.5 NAG 窗口提示限制.....	37
1.6 专家点拨：常见问题解答.....	42
第 2 章 常用代码分析工具.....	43
2.1 初识 PE 格式文件.....	44
2.1.1 PE 格式文件概述.....	44
2.1.2 检验 PE 格式文件.....	46
2.1.3 PE 文件格式的头结构.....	46
2.1.4 设置 Optional Header 可执行信息.....	49
2.1.5 Section Table 结构数组.....	51

2.1.6	Import Table 输入表	52
2.1.7	Export Table 输出表	53
2.1.8	重定位表	54
2.2	简述代码分析实战	55
2.2.1	虚拟地址与偏移地址	55
2.2.2	搜索程序入口点 OEP	58
2.2.3	转储程序与修复输入表	58
2.2.4	用增加重定位项调用引入表函数	62
2.3	常见静态分析工具	63
2.3.1	常见程序类型分析工具	63
2.3.2	常见资源编辑器工具	64
2.3.3	常见反汇编分析工具	66
2.4	常见动态分析工具	67
2.5	常见注册表分析工具	68
2.5.1	注册表编辑器 Regedit	68
2.5.2	注册表监控工具 Regsnap	71
2.5.3	注册表数据库监视软件 Regmon	73
2.5.4	注册表静态比较工具 RegShot	74
2.6	专家点拨：常见问题解答	75
第 3 章	不同的加密解密算法	76
3.1	数据加密的缘由	77
3.1.1	数据加密技术概述	77
3.1.2	为什么要进行数据加密	77
3.1.3	数据加密的原理	77
3.1.4	加密技术与密码分析	79
3.2	Hash 算法基础	81
3.2.1	CRC32 算法	81
3.2.2	MD5 算法	82
3.2.3	SHA 算法	85
3.3	对称密码算法基础	87
3.3.1	对称密码算法概述	88
3.3.2	BlowFish 算法概述	88
3.3.3	DES 算法概述	90
3.3.4	IDEA 算法概述	94
3.4	非对称密码算法基础	95
3.4.1	非对称密钥密码概述	95
3.4.2	RSA 非对称密钥密码概述	95
3.4.3	DSA 数据签名技术	96

3.4.4	Diffie-Hellman 密钥交换系统概述	97
3.5	专家点拨：常见问题解答	97
第 4 章	静态分析解密工具.....	98
4.1	程序源代码概述	99
4.1.1	基本程序信息	99
4.1.2	反汇编源代码部分	101
4.2	常用反汇编工具	103
4.2.1	反汇编和调试工具 W32Dasm	103
4.2.2	国产静态反编译工具 C32asm	114
4.2.3	反汇编工具 IDA Pro	116
4.3	实战静态分析解密	127
4.3.1	如何实现静态分析解密	127
4.3.2	汇编指令及其机器码值	128
4.3.3	判断真假注册码的方法	128
4.3.4	实例分析：静态破解 Crackme3 软件	129
4.4	注册机编写器 keymake	131
4.4.1	为破解文件打个补丁	132
4.4.2	制作内存补丁	132
4.5	专家点拨：常见问题解答	133
第 5 章	动态调试解密工具.....	135
5.1	动态调试工具 Ollydbg	136
5.1.1	初识 Ollydbg	136
5.1.2	不同的配置选项	138
5.1.3	快速掌握常用功能	138
5.1.4	熟悉必要的插件	141
5.1.5	实现动态调试解密	141
5.1.6	实例 1：解密加过 UPX 壳的 Crackme 程序	142
5.1.7	实例 2：找出真的注册码	143
5.2	内核模式调试器 SoftICE	144
5.2.1	配置 SoftICE 工具	144
5.2.2	实现 SoftICE 调用	148
5.2.3	激活 SoftICE 主窗口	148
5.2.4	快捷键与常用命令	150
5.2.5	快速找到程序入口处	157
5.2.6	多次跟踪的设置	158
5.2.7	用 PE 修改代码属性	158
5.3	动态反汇编调试器 TRW2000	159

5.3.1	安装与配置 TRW2000	160
5.3.2	呼出 TRW2000 调试窗口	162
5.3.3	常用命令和功能键	164
5.4	专家点拨: 常见问题解答	169
第 6 章	各显其能的辅助工具	171
6.1	不同的编辑修改工具	172
6.1.1	十六进制编辑工具 WinHex	172
6.1.2	十六进制查看器 Hiew	175
6.1.3	十六进制编辑器 HexWorkshop	179
6.1.4	文本编辑器 UltraEdit	182
6.2	不同功效的监视工具	187
6.2.1	文件系统监视工具 Filemon	187
6.2.2	API 函数监视工具	188
6.2.3	MFC (微软库类) 监视工具 Mfcspy	190
6.3	编辑程序内部资源工具	191
6.3.1	用 FreeRes 工具修复资源	191
6.3.2	用工具 eXeScope 编辑程序内资源	192
6.3.3	用工具 Festools 管理系统资源	194
6.4	制作破解补丁工具	196
6.4.1	补丁制作工具 dUP	196
6.4.2	绿色工具 XCell	199
6.5	专家点拨: 常见问题解答	200
第 7 章	揭秘壳的不同应用技术	201
7.1	不同的加壳压缩软件	202
7.1.1	DOS 窗口下的文件压缩壳软件 UPX	202
7.1.2	压缩各种可执行程序的 ASPack	203
7.1.3	软件保护压缩工具 Armadillo	204
7.1.4	国产外壳保护工具 EncryptPE	207
7.2	查壳工具大放送	208
7.2.1	用 Language2000 查看加壳情况	208
7.2.2	功能强大的 PEiDentifier	209
7.3	各具神通的脱壳工具	210
7.3.1	常用 ASPack 脱壳软件简介	210
7.3.2	通用脱壳工具 UnPECompact	211
7.3.3	通用脱壳工具 ProcDump	212
7.3.4	脱壳工具大集合 UN-PACK	214
7.4	轻松实现手动脱壳	215



7.4.1	用 ImportREC 实现手动脱壳	216
7.4.2	重建可编辑资源	220
7.5	专家点拨: 常见问题解答	220
第 8 章	别出心裁: 为程序打上补丁	222
8.1	常用补丁制作工具	223
8.1.1	专业补丁制作工具 CodeFusion	223
8.1.2	内存动态补丁工具 Process Patcher	226
8.2	实例: 网络客户端程序补丁	228
8.2.1	程序拦截的验证代码	228
8.2.2	增加自动修改机器号功能	229
8.2.3	用补丁修改程序	232
8.2.4	为程序附带一个动态链接库	234
8.2.5	用补丁加密可执行文件	235
8.3	代码自修改 SMC 技术	238
8.3.1	SMC 函数定义	238
8.3.2	实例: SMC 补丁技术应用	239
8.4	用 CrackCode2000 制作注册机	241
8.4.1	快速找到注册码	241
8.4.2	实现内存直接寻址	242
8.4.3	实现寄存器间接寻址	243
8.4.4	为 Decompile Winhelp 制作注册机	243
8.4.5	实例: CrackCode 的加强模式	245
8.5	专家点拨: 常见问题解答	247
第 9 章	网络验证技术大放送	248
9.1	实现 Web 服务器网络验证	249
9.1.1	加密客户端	249
9.1.2	控制本地计算机	252
9.2	实现本地服务器验证	256
9.2.1	加密客户端	257
9.2.2	加密服务器端	259
9.3	在线升级验证加密技术	261
9.3.1	在线升级验证实现	261
9.3.2	实例分析: 在线升级验证	262
9.4	专家点拨: 常见问题解答	268
第 10 章	各种常用加密软件工具的使用	269
10.1	多媒体文件加密工具	270

10.1.1	多媒体加密工具 Private Pix	270
10.1.2	图片软件加密工具 CryptaPix	272
10.1.3	图片文件专业加密工具 WinXFiles	273
10.2	多功能文件加密工具	276
10.2.1	数据加密和安全通讯工具“文件密使”	276
10.2.2	可加密各种格式文件的 BlackBox	281
10.2.3	对称加密算法工具 ABI-CODER	286
10.2.4	国产加密工具“加密精灵”	288
10.3	专家点拨：常见问题解答	291
第 11 章	分析软件的不同注册方式	292
11.1	简单的注册码保护方式	293
11.1.1	追踪简单算法	293
11.1.2	简单注册码的破解	294
11.1.3	API 函数常用断点及实例	298
11.2	按钮功能限制	308
11.2.1	按钮功能限制概述	308
11.2.2	突破按钮限制	309
11.2.3	按钮限制解密实例	311
11.3	NAG 窗口	312
11.3.1	NAG 窗口实例 1	313
11.3.2	NAG 窗口实例 2	317
11.4	加密狗解密	319
11.4.1	判断加密狗类型	319
11.4.2	加密狗解密实例	320
11.5	专家点拨：常见问题解答	325
第 12 章	编辑安装包程序	326
12.1	InstallShield	327
12.1.1	InstallShield 使用介绍	327
12.1.2	编辑 CAB 压缩包	341
12.2	Wise 安装包软件	343
12.3	Setup Factory 安装包制作工具	343
12.4	Inno Setup 安装制作软件	352
12.4.1	Inno Setup 的使用介绍	352
12.4.2	Inno Setup 的脚本语法介绍	357
12.4.3	压缩包的编辑	360
12.5	微软 MSI 安装包	360
12.6	专家点拨：常见问题解答	362

第 13 章 不同软件的保护措施	363
13.1 对抗不同的破解手段	364
13.1.1 对抗 DeDe 和动态调试	364
13.1.2 对抗 SoftICE	365
13.1.3 对抗静态调试	367
13.1.4 实现磁盘文件自校验	368
13.2 不同软件的保护实现	369
13.2.1 把 ASP 编写成 DLL	370
13.2.2 COM 组件的 Delphi 实现	372
13.2.3 实现软件注册保护的 VCL 组件	377
13.2.4 利用伪装壳制造虚假信息	379
13.2.5 利用加密锁保护程序	380
13.3 邮件加密软件 PGP	384
13.3.1 PGP 概述	384
13.3.2 PGP 的安全问题	385
13.4 专家点拨: 常见问题解答	390
第 14 章 常用软件加密解密技术	391
14.1 加密解密 Word 文件	392
14.1.1 Word 自身功能加密	392
14.1.2 利用 AOPR 解密 Word 文档	393
14.1.3 风语文件加密工具	395
14.1.4 Word Password Recovery 破解工具	395
14.1.5 Word 密码查看器	396
14.2 Excel 文件加密解密	397
14.2.1 实现 Excel 自加密	397
14.2.2 办公文件密码恢复程序	398
14.2.3 Excel 加密文档解密工具 Excel Key	399
14.3 PDF 文件的加密解密	400
14.3.1 加密 PDF 文件	400
14.3.2 使用 PDF 文件加密器	402
14.3.3 Advanced PDF Password Recovery	404
14.3.4 用 PDF Password Remover 解除 PDF 文件口令	406
14.4 宏加密解密技术	408
14.4.1 实现宏技术加密	408
14.4.2 宏解密工具 VBA Key	411
14.5 对压缩文件实施加密解密	411
14.5.1 实现 WinZip 自加密	412

14.5.2	解除 ZIP 文件口令	413
14.5.3	实现 WinRAR 自加密	413
14.5.4	解除 RAR 文件密码	414
14.6	加密解密 EXE 文件	415
14.6.1	用 ASPack 加密 EXE 文件	415
14.6.2	用 tElock 加密 EXE 文件	417
14.6.3	为 EXE 文件加口令	419
14.7	解密 MS SQL Server 保护	420
14.7.1	实现本地用户的帐户登录	420
14.7.2	查询分析器的使用	420
14.7.3	多功能密码破解软件	421
14.8	加密解密网页与脚本文件	423
14.8.1	网页与脚本的加密	423
14.8.2	网页与脚本的解密	428
14.9	专家点拨: 常见问题解答	430

第 1 章

初识加密解密技术

重点提示

- 加密解密技术基础
- 动态链接库 (DLL) 文件
- 设计与发布 BPL 组件
- 解密与注册保护
- 试用期限限制功能

本章精粹

本章主要介绍了关于加密解密的基础知识,其中包括加密基础技术、文件读写、BPL 组件设计、软件试用期,以及几种常用软件解密方法和软件注册保护方式,展现了比较全面的加密解密技术知识。

1.1 加密解密技术基础

加密解密技术长期以来只应用在很小的范围内,如军事、外交、情报等部门使用。计算机加密技术是研究计算机信息加密、解密及其变换的科学,是数学和计算机的交叉学科,也是一门新兴的学科。

很多人都曾不止一次地面对过网络上的安全问题,黑客程序、病毒、邮件炸弹、远程侦听等安全问题,让人一听就胆战心惊。病毒、黑客的肆意猖獗,更是使人时刻感觉到危险无处不在。因此,人们就想到了要对自己的数据进行加密。

对数据进行加密,在国外已成为计算机安全主要的研究方向,也是计算机安全课程教学中的主要内容。一个密码系统的安全性只在于密钥的保密性,而不在于算法的保密性。

1.1.1 密码学简述

密码学可细分为编码学和破译学两个方面,编码学主要研究密码变化的客观规律,一般应用于编制密码,以确保通信过程中的信息安全;破译学主要用于破译密码,以获取通信过程中的情报。

随着先进科学技术的应用,密码学已成为隐藏通信信息内容的重要保密手段。通信双方按一些约定的准则对信息进行特殊变换,其中若是变明文为密文,则称加密变换;若是变密文为明文,则称脱密变换;而进行明密变换的准则,被称为密码的体制;指示这种变换的参数,就是所谓的密钥。密码的体制和密钥均是密码编制过程中的重要组成部分,而密码体制的基本类型一般有4种:错乱、代替、密本和加乱。

- 错乱:按照规定的图形和线路,改变明文字母或数码等的位置成为密文。
- 代替:用一个或多个代替表将明文字母或数码等代替为密文。
- 密本:用预先编定的字母或数字密码组,代替一定的词组单词,从而变明文为密文。
- 加乱:用有限元素组成的一串序列作为乱数,按照一定的算法,同明文序列相结合后变成密文。

对于上述4种密码体制,为编制出各种复杂度很高的实用密码,既可对其单独使用,也可将它们混合使用。密码破译是随着密码的使用而逐步产生和发展的。它利用文字和密码的规律,通过采取各种技术手段对密文进行认真而细致地分析,以还原密码编制并最终获得加密前的明文信息。

1.1.2 常用汇编语言命令

汇编语言是面向机器的程序设计语言,描述了机器最终要执行的指令序列,是人和计算机沟通的最直接方式。它主要由三部分内容组成:汇编指令、伪指令和其他符号。其中,汇编指令即机器码的助记符,汇编后直接由机器执行;而伪指令或其他符号均由编译器识别。

由于在加密解密过程中,往往会遇到或用到一些常见的汇编语言的概念或命令,为了便于