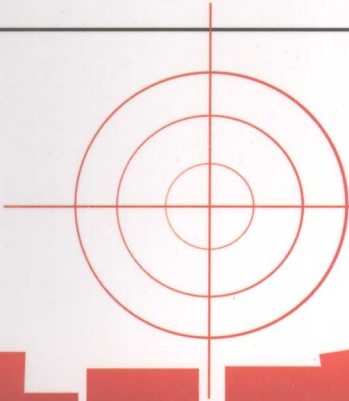




计算机 加密解密 2000例

徐 谔 黄定光 赵乘源 等编著



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

计算机加密解密 200 例

徐 谔 黄定光 赵乘源 等编著

電子工業出版社·

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书涵盖了计算机加密解密技术在日常生活中的各个领域,以 200 个计算机加密解密的精彩的案例,翔实的操作步骤,展现加密解密技术在实践中的应用。全书内容共分为 9 章,从 Windows 操作系统下常用的加密解密技巧讲起,采用案例的方式,详细讲解了 Windows 系统密码设置与破解、加密文件系统 EFS 的应用、常见的应用文件加密与解密;并介绍了 DRM 技术的加密及解密、常见的网络应用信息加密及解密、共享软件的加密及解密技巧,以及网吧的加密及解密方案;最后阐述了入侵的防范技术。本书能够帮助读者快速学会并灵活运用常见的加密及解密技巧,适合计算机初中级用户使用,也可以作为加密解密技术爱好者的参考书。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有,侵权必究。

图书在版编目(CIP)数据

计算机加密解密 200 例 / 徐谟等编著. —北京:电子工业出版社, 2008.2
ISBN 978-7-121-05754-0

I. 计… II. 徐… III. ①电子计算机—密码—加密②电子计算机—密码—解密译码 IV. TP309.7

中国版本图书馆 CIP 数据核字(2008)第 002210 号

责任编辑: 陆伯雄

印 刷: 北京市天竺颖华印刷厂

装 订: 三河市金马印装有限公司

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: 24.5 字数: 596 千字

印 次: 2008 年 2 月第 1 次印刷

印 数: 5000 册

定价: 40.00 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。

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

服务热线:(010) 88258888。

前言

随着信息化时代的到来，网络技术也日新月异地发展。网络时代的计算机信息安全越来越重要，许多对计算机知识和实用技术有一定了解的用户越来越关心计算机加密和解密技术，他们迫切需要掌握一定的知识和技术手段以保护自己的计算机和各类信息及文件的安全。

本书正是基于此目的，对常见的加密解密技术进行了全过程剖析。本书结构清晰、语言简洁，注重对实战操作步骤的解释和说明，使读者不仅能够学会加密解密的方法，同时对加密解密的原理也有所了解。

计算机的加密与解密，二者本身就是一对矛盾，它们正是在不断争斗、不断冲突、不断制约、不断发展中，演绎了计算机网络安全精彩篇章。为了知己知彼，本书在讲解计算机加密的同时，适当地展示了一些解密的案例，相信读者对此能够正确地理解和运用。

本书的一个重要特点是注重以案例、实践为核心，针对加密解密技术在日常生活中的各个领域，以翔实的实例，精彩的操作技能，展现加密解密技术在实践中的应用。全书内容共分为 9 章，从 Windows 操作系统下常用的加密解密技巧讲起，采用案例的方式，详细讲解了 Windows 系统密码设置与破解、加密文件系统 EFS 的应用、常见应用文件的加密与解密；并介绍了 DRM 技术的加密及解密、常见的网络应用信息的加密及解密、共享软件的加密及解密技巧，以及网吧的加密及解密方案；最后阐述了入侵的防范技术。本书能够帮助读者快速学会并灵活运用常见的加密和解密方法，以及安全使用计算机的实践操作技能。

本书由具有丰富的计算机加密解密专业工作经验的徐谟、黄定光、赵乘源等编著。由

电子科技大学计算机学院党委书记徐谟主编，电子科技大学陈洪彬老师参与了全书的策划、管理和技术支持。其中黄定光编写了第1、2、5、8章，赵乘源编写了第3、6、9章，李欢编写了第4、7章。另外在图书编写过程中，得到了胡霞、李晓瑜、王昕、徐义强、常政威、程曦、谢晓娜、宋庆华、李海江等同事的大力支持。

由于作者水平所限，本书难免会有所错漏，希望读者提出宝贵的意见。

作者的电子邮箱：ben_uestc@163.com。

编著者

2007年12月

全书共分10章，第1章介绍计算机病毒的基本概念、分类、传播途径、危害及防治方法；第2章介绍计算机病毒的特征、检测、清除及预防；第3章介绍计算机病毒的种类、传播途径、危害及防治方法；第4章介绍计算机病毒的种类、传播途径、危害及防治方法；第5章介绍计算机病毒的种类、传播途径、危害及防治方法；第6章介绍计算机病毒的种类、传播途径、危害及防治方法；第7章介绍计算机病毒的种类、传播途径、危害及防治方法；第8章介绍计算机病毒的种类、传播途径、危害及防治方法；第9章介绍计算机病毒的种类、传播途径、危害及防治方法；第10章介绍计算机病毒的种类、传播途径、危害及防治方法。

本书可作为高等院校计算机专业及相关专业的教材，也可供从事计算机工作的工程技术人员参考。

本书在编写过程中，参考了国内外有关文献，并得到了许多同行的帮助，在此表示衷心的感谢。

由于时间仓促，书中难免存在不足之处，恳请读者批评指正。

本书由电子科技大学计算机学院党委书记徐谟主编，电子科技大学陈洪彬老师参与了全书的策划、管理和技术支持。

目录

C O N T E N T S

第 1 章 Windows 系统及系统文件的实用加密解密技巧	1
1.1 CMOS 设置开机密码及用户密码	1
案例 1-1 Award BIOS 设置开机密码及用户密码	1
案例 1-2 AMI BIOS 设置开机密码及用户密码	4
案例 1-3 ASUS (华硕) BIOS 设置开机密码及用户密码	6
案例 1-4 Phoenix BIOS 设置开机密码及用户密码	8
1.2 CMOS 开机密码及用户密码解除及破解	9
案例 1-5 解除 Award BIOS 开机密码及用户密码	9
案例 1-6 解除 AMI BIOS 开机密码及用户密码	10
案例 1-7 解除 ASUS BIOS 开机密码及用户密码	11
案例 1-8 解除 Phoenix BIOS 开机密码及用户密码	13
案例 1-9 巧用 Debug 命令清除 CMOS 用户密码	14
案例 1-10 巧用 Copy 命令清除用户密码	15
案例 1-11 使用 CMOS 密码破解工具破解用户密码	16
案例 1-12 万能密码破解开机密码	17
案例 1-13 CMOS 放电法破解开机密码	18
案例 1-14 改变硬件配置法破解开机密码	19
1.3 系统用户密码设置及破解	19
案例 1-15 Windows 2000 用户登录密码设置	20
案例 1-16 Windows XP 用户登录密码设置	20
案例 1-17 Windows Vista 用户登录密码设置	22
案例 1-18 对于没有设置 Administrator 用户密码的破解	24
案例 1-19 ERD2003 软件破解 Windows 2000/XP/2003 用户登录密码	25
案例 1-20 NET USER 命令破解 Windows 2000/XP/2003 用户登录密码	27
案例 1-21 Windows key 破解 Windows 2000/XP/2003 用户登录密码	29
1.4 休眠和屏保的加密保护及破解	30
案例 1-22 休眠退出增加密码保护	30
案例 1-23 给 Windows XP 屏幕保护程序加上密码	32

案例 1-24	给 Windows Vista 屏幕保护程序加上密码	33
案例 1-25	给 Windows 2000/XP/2003/Vista 所有的屏幕保护都加上密码	34
案例 1-26	设置 Windows XP 开机后立即运行屏幕保护程序	35
案例 1-27	解除 Windows 2000/XP/2003 屏幕保护密码	36
1.5	妙用注册表进行数据保密	36
案例 1-28	利用注册表隐藏光驱	36
案例 1-29	利用注册表隐藏文件	37
案例 1-30	防止非法编辑注册表	38
案例 1-31	防止匿名用户登录	39
案例 1-32	利用注册表屏蔽“运行”对话框	39
案例 1-33	利用注册表屏蔽“控制面板”	40
案例 1-34	禁止访问硬盘	40
案例 1-35	利用注册表屏蔽“开始”菜单	42
案例 1-36	利用注册表屏蔽“显示”属性	43
案例 1-37	禁止运行“任务管理器”	43
案例 1-38	禁用“远程管理”功能	44
案例 1-39	禁用“文件及打印共享”功能	44
案例 1-40	限制程序运行	45
1.6	第三方软件进行 Windows 系统及系统文件夹加密	45
案例 1-41	用 Syskey 命令为 Windows XP 设置启动密码	45
案例 1-42	利用回收站的特性进行加密	46
案例 1-43	利用类标识符进行加密	47
案例 1-44	“超级兔子”魔法进行系统安全设置	48
案例 1-45	Windows 安全大师进行系统安全设置	51
案例 1-46	利用 Copy 命令隐含文本文件	53
案例 1-47	更改文件后缀来加密文件	54
案例 1-48	给镜像文件添加密码保护	55
案例 1-49	速度极快的加密工具——文件夹加密器	55
案例 1-50	功能强大的加密工具——“文件夹加密超级大师”	56
案例 1-51	小巧的加密工具——“万能加密器”	59
案例 1-52	优秀的 U 盘加密工具——“高强度 U 盘文件夹加密”	60
案例 1-53	系统文件夹加密能手——PC Security	61
案例 1-54	使用“还原精灵”保护系统	65
案例 1-55	忘记“还原精灵”密码后的应急措施	66

第 2 章 微软操作系统的加密文件系统 EFS 应用

2.1	加密文件系统 EFS 基础	67
2.2	加密文件系统 EFS 的加密应用	69

案例 2-1	利用 Windows 资源管理器进行 Windows 2000/XP/2003 文件系统加密及解密	69
案例 2-2	Windows Vista 加密文件系统 EFS	70
案例 2-3	在 Windows 2000/XP/2003 中使用 cipher 命令加密	71
2.3	加密证书导入导出及加密文件共享	72
案例 2-4	在 Windows 2000/XP/2003 备份加密证书和私钥	73
案例 2-5	在不同系统中还原加密证书和私钥	74
案例 2-6	备份加密证书到远程服务器	76
案例 2-7	共享 EFS 加密文件	76
2.4	解密 EFS 加密文件	78
案例 2-8	利用 Advanced EFS Data Recovery 解密 EFS 加密文件	78
案例 2-9	EFSKey 解密 EFS 加密文件	80
案例 2-10	用 PsExec 和 IceSword 恢复 EFS 加密文件	81

第 3 章 常见应用文件的加密和解密 83

3.1	办公文档的加密和解密	83
案例 3-1	通过安全选项设置 Word 文件打开和修改密码	83
案例 3-2	对 Word 默认的通用模板进行加密	85
案例 3-3	利用宏自动加密 Word 文档	86
案例 3-4	利用 Word “版本”功能加密	90
案例 3-5	通过文档保护来保护 Word 文档	92
案例 3-6	Excel 文件的安全选项加密技巧	94
案例 3-7	隐藏 Excel 文件中的部分内容	94
案例 3-8	Excel 文件使用权限加密	96
案例 3-9	加密 Access 数据库文件	99
案例 3-10	WPS 文件加密	99
案例 3-11	Acrobat 进行 PDF 文档加密	101
案例 3-12	EncryptPDF 进行 PDF 文档加密	104
案例 3-13	永中 Office 文档加密	107
案例 3-14	Word Password Recovery 解密简单的 Word 文件	108
案例 3-15	Excel Password Recovery 解密 Excel 文件	111
案例 3-16	WKH 文件加密器进行 WPS 文件加密和解密	113
案例 3-17	PDF Password Recovery 进行 PDF 文档解密	116
案例 3-18	Solid Converter PDF 进行 PDF 文档解密	117
3.2	压缩文件的加密和解密	120
案例 3-19	WinRAR 的加密操作	120
案例 3-20	让 WinRAR 自动为压缩文件添加密码保护	121
案例 3-21	使用 WinZip 加密压缩文档	122

案例 3-22	使用 Winace 加密压缩文件.....	124
案例 3-23	用 Advanced RAR Password Recovery 解密 RAR 文件.....	126
案例 3-24	用 Advanced ZIP Password Recovery 解密 ZIP 文件.....	127
案例 3-25	RAR 文件解密工具进行 RAR 文件解密.....	129
3.3	图片的加密和解密.....	130
案例 3-26	用 PhotoEncryp 加密及解密图片.....	130
案例 3-27	用图片加密器加密图片.....	132
案例 3-28	图片加密大师给图片加把锁.....	136
3.4	光盘文件的加密和解密.....	138
案例 3-29	光盘加密大师加密光盘文件.....	138
案例 3-30	CD-Protector 保护光盘版权.....	142
案例 3-31	用 CryptCD 进行加密光盘制作.....	145
案例 3-32	用 CloneCD 进行加密光盘数据的拷贝.....	147
案例 3-33	File Monitor 查找目录的加密光盘.....	149
案例 3-34	用 IsoBuster 浏览光盘上的隐藏文件.....	151

第 4 章 DRM 技术的加密和解密 153

4.1	DRM (数字版权管理) 技术基础.....	153
4.2	DRM 技术的加密应用.....	156
案例 4-1	DRM 音频视频加密器进行音视频加密.....	156
案例 4-2	多媒体文件加密器——全方位的加密音频视频文件.....	159
案例 4-3	eBook Studio 制作加密电子书.....	161
案例 4-4	eBook Workshop 制作加密电子书.....	168
案例 4-5	SignRobot 图片数字水印制作.....	173
案例 4-6	图片加数字水印进行数字水印制作.....	176
案例 4-7	会声会影加入视频数字水印.....	178
案例 4-8	PDF 文本中添加数字水印.....	179
案例 4-9	Word 文档添加数字水印.....	181
案例 4-10	利用 Photoshop 添加图片水印.....	184
4.3	多媒体音频、视频 Flash 的 DRM 技术解密.....	186
案例 4-11	解密播放 DRM 加密的音视频文件.....	186
案例 4-12	FairUse4WM 破解微软 DRM 加密音视频文件.....	187
案例 4-13	修复系统“数字版权管理”DRM.....	188
案例 4-14	利用 CHM 电子书批量反编译器来解密电子书.....	190
案例 4-15	E 书伴侣解密 Web Compiler 制作的 EXE 电子书.....	192
案例 4-16	去除图片的水印.....	194

第5章 网络应用信息的加密 197

5.1 网页加密	197
案例 5-1 利用 JavaScript 密码锁进行加密	197
案例 5-2 使用 IIS 的密码锁进行网页加密	199
案例 5-3 使用 ASP 程序密码锁进行网页加密	201
案例 5-4 使用网页加密精灵进行网页加密	202
案例 5-5 使用网页加密器进行网页的加密	204
案例 5-6 网页 HTML 加密器进行网页加密	205
5.2 电子邮件加密	207
案例 5-7 电子证书的申请及安装	207
案例 5-8 Foxmail 电子签名技术进行邮件加密设置	208
案例 5-9 使用 Outlook 数字签名技术进行邮件加密设置	211
案例 5-10 用 A-Lock 来加密文本内容的电子邮件	212
案例 5-11 用 zMailGuard 加密邮件系统	213
案例 5-12 利用 Puffer 加密邮件	215
5.3 聊天工具加密	217
案例 5-13 QQ 聊天记录的加密	217
案例 5-14 QQ 密码保护方案	218
案例 5-15 QQ 空间加密	220
案例 5-16 用 Windows live messenger 进行 MSN 聊天记录加密	220
5.4 其他网络应用信息的加密	225
案例 5-17 无线路由器的加密设置	225
案例 5-18 FTP 服务器软件 Serv-U 的安全加密设置	230
案例 5-19 IIS 中 FTP 加密设置	232
案例 5-20 个人网上银行证书认证版加密设置	234

第6章 网络应用信息的解密与安全防范 237

6.1 网页的监控、漏洞扫描及解密	237
案例 6-1 破解网页鼠标右键被禁用	237
案例 6-2 破解网页不能被复制	239
案例 6-3 查找真实的下载地址	240
案例 6-4 使用 Pwsniffer 获取密码信息	242
案例 6-5 使用“艾菲网页侦探”监听网络 HTTP 数据	244
案例 6-6 使用 IRIS 进行网络监听和网络性能分析	245
案例 6-7 利用 N-Stealth 进行网页漏洞扫描	249
案例 6-8 使用“流光”进行网页漏洞扫描	252

案例 6-9	从网页代码中进行加密网页源码破解	255
案例 6-10	探索“流光”解密已加密的网页	257
6.2	电子邮件的解密与防范	260
案例 6-11	探索利用 NoPassword 破解 POP3 邮箱密码	260
案例 6-12	探索使用“溯雪”进行 Web 邮箱破解	261
案例 6-13	使用 Outlook Express 的邮件过滤	264
案例 6-14	设置 Foxmail 的访问口令	266
案例 6-15	电子邮件的破解防范	268
6.3	聊天密码的破解与防范	271
案例 6-16	探索利用 Keymake 密码破解器进行 QQ 密码破解	271
案例 6-17	破解 QQ 相册空间方法揭密	273
案例 6-18	使用聊天记录器查看 QQ 聊天记录揭密	275
案例 6-19	破解 MSN 账户方法揭密	278
案例 6-20	如何防范聊天密码被破解	278

第 7 章 共享软件的加密和解密 281

7.1	软件的加密和解密基础	281
7.2	共享软件的加密	284
案例 7-1	给软件加壳保护共享软件	284
案例 7-2	用“软件保护神”添加反跟踪保护共享软件	286
案例 7-3	增加注册认证保护共享软件	288
案例 7-4	Codefantasy 软件加密解决方案进行软件加密	292
案例 7-5	共享软件加密算法库给共享软件加锁	296
7.3	共享软件的解密	300
案例 7-6	W32Dasm 的反汇编解密	301
案例 7-7	C32asm 的反汇编解密	304

第 8 章 网吧的加密和解密 307

8.1	网吧计算机的加密	307
案例 8-1	禁止 IE 下载	307
案例 8-2	禁止 IE 地址栏	308
案例 8-3	禁止任务栏上的右键	308
案例 8-4	禁止使用菜单条上的右键	309
案例 8-5	不提供 TE（只提供去掉 TE 的 QQ）	309
案例 8-6	屏蔽本地硬盘（通过修改注册表）	310
案例 8-7	禁止使用 WinZip	310
案例 8-8	禁止使用实核 DOS	311

案例 8-9	禁止导入 REG 文件	311
案例 8-10	禁止导入 INF 文件	312
案例 8-11	屏蔽 IE 中的文件菜单	312
案例 8-12	屏蔽 IE 的 Internet 属性	313
案例 8-13	屏蔽鼠标右键	313
案例 8-14	屏蔽 MS-DOS 方式	314
案例 8-15	禁止使用 Regedit	314
8.2	网吧计算机的解密	315
案例 8-16	利用 IE 菜单漏洞找回菜单	315
案例 8-17	利用本地硬盘漏洞找回硬盘	315
案例 8-18	修改注册表恢复“运行”程序	316
案例 8-19	利用资源管理器漏洞解放管理器	317
案例 8-20	利用鼠标右键漏洞挡住右键菜单	317
案例 8-21	利用下载漏洞突破下载封锁	318
案例 8-22	利用输入法漏洞删除文件	318
案例 8-23	注册表漏洞突破封锁注册表	319
案例 8-24	禁用软件漏洞恢复“WinZip”本色	319
案例 8-25	定制 IE 浏览器漏洞定制 IE 浏览器	319
8.3	网吧密码解密工具应用	320
案例 8-26	“小哨兵密码清除器”破解忘记还原卡密码	320
案例 8-27	“解锁安全器 2.0”破解网吧软件	321
案例 8-28	“注册表解锁器”破解网吧注册表	322
案例 8-29	“网上邻居密码破解器”破解共享密码	323

第 9 章 防范入侵的方法 325

9.1	清除网络秘密	325
案例 9-1	IE 缓存记录清除	325
案例 9-2	Cookie 记录清除	326
案例 9-3	History 文件夹记录清除	326
案例 9-4	拨号记录清除	327
案例 9-5	密码记录清除	327
案例 9-6	网页收藏记录清除	328
案例 9-7	消除已访问 IE 地址的颜色变化	329
案例 9-8	关闭 IE 自动填写表单功能	330
案例 9-9	删除 IE 的临时文件	331
案例 9-10	设置 IE 分级审查	331
案例 9-11	设置 IE 的安全区域	333
案例 9-12	安装身份证	334

9.2 清除系统秘密	335
案例 9-13 “文档”记录清除	335
案例 9-14 “运行”记录清除	336
案例 9-15 “查找”记录清除	338
案例 9-16 计划任务记录清除	338
案例 9-17 TEMP 文件夹记录清除	339
案例 9-18 剪贴内容清除	340
案例 9-19 “回收站”内容清除	340
9.3 软件记录清除	341
案例 9-20 Word 记录清除	341
案例 9-21 Excel 记录清除	342
案例 9-22 WPS 记录清除	343
案例 9-23 “被挽救的文档”清除	343
案例 9-24 网络蚂蚁记录清除	343
案例 9-25 清除网际快车“添加新任务\另存到”下的目录列表	345
案例 9-26 清除 WinZip “文件”菜单中的历史文件	346
案例 9-27 清除 WinRAR 访问的历史记录	347
案例 9-28 Windows Media Player 播放记录清除	348
案例 9-29 RealOne Player 文件记录清除	348
案例 9-30 让 ACDSee 自动清除历史记录	349
案例 9-31 删除输入法自动记忆的信息	350
9.4 漏洞扫描、木马清除及查杀病毒	351
案例 9-32 漏洞扫描	351
案例 9-33 补丁的安装	354
案例 9-34 Iparmor 木马克星清除木马	355
案例 9-35 杀毒软件杀木马	356
案例 9-36 手动清除木马可用方法总结	358
案例 9-37 防火墙安装及分析	360
案例 9-38 用卡巴斯基 6.0 杀毒软件清除病毒	363
案例 9-39 利用网络资源查找病毒的详细资料	364
案例 9-40 用 Ad-Aware 彻底清查广告与间谍软件	365
案例 9-41 如果没有防毒软件, 在线杀毒帮助你	368
案例 9-42 用 Windows Defender 找出潜藏的恶意软件	370
案例 9-43 手动清除病毒	373
9.5 密码安全恢复新策略	376
案例 9-44 密码设置技巧分析	376
案例 9-45 密码保护应用	377
案例 9-46 密码管理软件保存密码	378

第1章

Windows系统及 系统文件的实用加密解密技巧

世界已经进入信息时代，保护隐私已经成为一个非常敏感的话题。加密离我们并不遥远，从小小的个人密码，到重要的机密文件，无一不是经过加密后的产物。加密技术已经渗透进了整个信息时代，任何人都不可避免地接触到——即使你根本不知道“加密”是什么。如何在计算机上有效地保护自己的信息？怎样才能最大限度地计算机上保护自己的隐私？或许，你可以在本章找到答案。

1.1 CMOS 设置开机密码及用户密码

BIOS(Basic Input Output System, 基本输入输出系统)是被固化到计算机主板上的 ROM 芯片中的一组程序，其主要作用是给计算机提供最低层的、最直接的硬件设置和控制。由于 BIOS 设置程序是储存在 BIOS 芯片中的，因此只有在开机时才可以进行设置。

CMOS 主要用于存储 BIOS 设置程序所设置的参数与数据，而 BIOS 设置程序主要对基本输入输出系统进行管理和设置，使系统运行在最好状态下。使用 BIOS 设置程序还可以排除系统故障或者诊断系统问题。

在计算机上使用的 BIOS 程序，根据制造厂商的不同，分为：Award BIOS 程序、AMI BIOS 程序、Phoenix BIOS 程序，以及其他的免跳线 BIOS 程序和品牌机特有的 BIOS 程序，如 IBM 等等。

目前主板 BIOS 有三大类型，即 Award、AMI 和 Phoenix 三种。不过，Phoenix 已经与 Award 合并了，因此有些台式机主板上虽然标有 Award-Phoenix，其实还是 Award 的 BIOS。Phoenix BIOS 多用于高档的 586 原装品牌机和笔记本电脑上，其画面简洁，便于操作。

案例 1-1 Award BIOS 设置开机密码及用户密码

保护自己的计算机的第一步，通常是设置一个开机密码。在 CMOS 中，可以分别设置系统密码和用户密码。

1. Award BIOS 介绍

Award BIOS 是 Award Software 公司开发的 BIOS 产品，在目前的计算机中非常流行。许多主板都采用 Award BIOS，它的功能比较齐全，对各种操作系统都能提供良好的支持。Award BIOS 主要由如表 1-1 所示的选项组成。

表 1-1 Award BIOS 选项列表

选 项	含 义
STANDARD CMOS SETUP	标准 CMOS 设定
ADVANCED BIOS FEATURES	高级 BIOS 特性设定
CHIPSET FEATURES SETUP	芯片组特性设定
POWER MANAGEMENT SETUP	省电功能设定
PNP/PCI CONFIGURATION	即插即用设备与 PCI 组态设定
LOAD BIOS DEFAULTS	载入 BIOS 预设值
LOAD OPTIMIEZED Defaults	载入主板 BIOS 出厂设置
INTEGRATED PERIPHERALS	整合设备周边设定
SUPERVISOR PASSWORD	管理者密码
USER PASSWORD	用户密码
IDE HDD AUTO DETECTION	自动检测 IDE 硬盘类型
SAVE&EXIT SETUP	储存并退出设置
EXIT WITHOUT SAVE	沿用原有设置并退出 BIOS 设置)

2. 设置开机密码和用户密码

开启计算机或重新启动计算机后，在屏幕显示“Press to enter setup”提示时，按下【Del】键，就可以进入 BIOS 设定程序 CMOS 的设置界面，如图 1-1 所示。

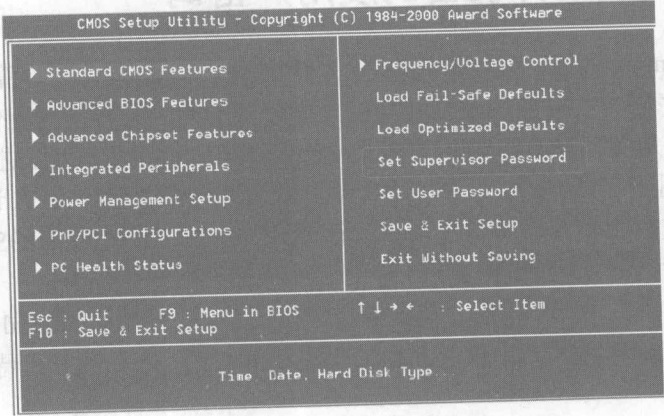


图 1-1 CMOS 主界面

小 知 识

先了解一下在这里可能用得上的功能键。Esc: 按下此键可以退出 BIOS Setup。方向键↑ ↓ ← →: 在主选菜单内按下这些键可以选择需要确认或修改的选项。F10: 当完成 BIOS 的各项设定之后，按下此键可以保存这些参数并退出 BIOS Setup。

管理者密码与用户密码所控制的层次不同，它们的区别如表 1-2 所示。

表 1-2 管理者密码与用户密码的区别

密 码	功 能
管理者密码	此密码可以正常开机，进入 CMOS 并设定和更改 BIOS 设定
用户密码	可正常开机，进入 CMOS，仅能更改时间日期，无法更改 BIOS 设定

★ 设置开机密码的步骤

- 1 使用方向键移动到“Set Supervisor Password”项，按下【回车】键。
- 2 弹出“Enter new supervisor Password”对话框，提示输入密码，输入欲设置的密码，可以是六个字节的英文、数字，或符号。输入完毕后，按下【回车】键，如图 1-2 所示。
- 3 按下【回车】键后，再输一次密码以确保密码正确。当两次密码确认无误后，密码设置完成。
- 4 使用方向键移动到“Advance BIOS FEATURES”项，按【回车】键，弹出如图 1-3 界面。使用方向键移动到“Security Option”的选项，按【回车】键。如果设为“System”，即开机需要密码才能启动；如果设为“Setup”时，即进入 CMOS 时才需要密码。这里我们设为“System”，如图 1-3 所示。

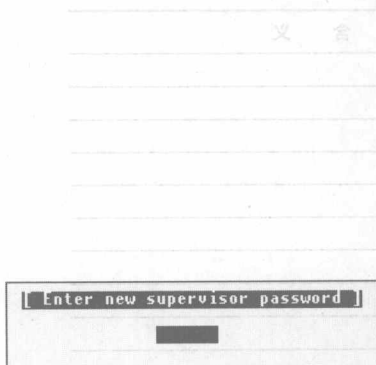


图 1-2 设置新管理员密码

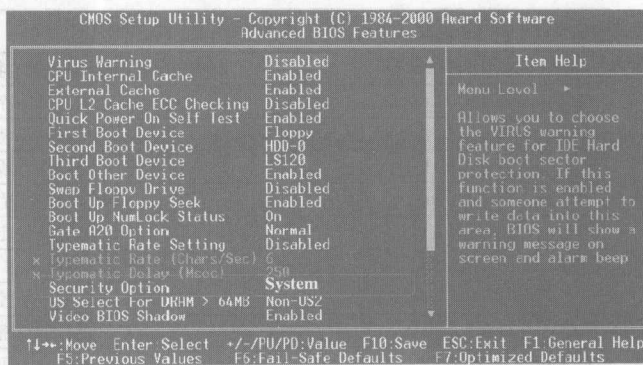


图 1-3 设置 Security Option 项

- 5 按【F10】键保存并退出。

重启计算机，你会发现提示“Enter your password”，只有当输入正确的密码时，才能启动系统。

★ 设置用户密码的步骤

- 1 使用方向键移动到“Set User Password”项，按下【回车】键。
- 2 弹出“Enter Password”对话框，提示输入密码，输入欲设置的密码，可以是六个字节的英文、数字，或符号。输入完毕后，按下【回车】键。
- 3 按下回车键后，再一次输入密码以确保密码正确。当两次密码确认无误后，系统表示密码设置完成。若出现“Password not match”信息，表示密码确认时输入错误，请重新输入一次。
- 4 按【F10】键保存退出。

! 注意

如果开机按得太晚，计算机将会启动系统，这时只有重新启动计算机了。大家可在开机后立刻按住【Del】键直到进入CMOS。在CMOS主界面，可以用方向键移动光标选择CMOS设置界面上的选项，然后按【回车】键进入选项，用【ESC】键来返回父菜单，按【F10】键保留并退出BIOS设置。

▶ 案例 1-2 AMI BIOS 设置开机密码及用户密码

1. AMI BIOS 介绍

AMI BIOS 是与 Award BIOS 齐名的 BIOS 系统。但现在的主板 BIOS 中使用 AMI BIOS 的并不多，只是有一些著名的主板厂商还在采用它，例如著名的微星（MSI）主板产品就是如此。

AMI BIOS 主要由如表 1-3 所示的选项组成。

表 1-3 AMI BIOS 选项列表

选 项	含 义
Standard CMOS Features	标准 CMOS 特性
Advanced BIOS Features	高级 BIOS 特性
Advanced Chipset Features	高级芯片组特性)
Power Management Features	(电源管理设定)
PNP/PCI Configurations	PnP/PCI 配置
Integrated Peripherals	周边设备设定
PC Health Status	PC 健康状态
Frequency/Voltage Control	频率和电压控制
Set Supervisor Password	设置管理员密码
Set User Password	设置用户密码
Load Optimal Defaults	载入优化默认值
Load Fail Safe Defaults	载入故障保护默认值
Save & Exit Setup	保存后退出
Exit Without Saving	不保存退出

2. 设置开机密码和用户密码

开启计算机或重新启动计算机后，在屏幕显示“Press to enter setup”提示时，按下【Del】键，就可以进入 BIOS 设定程序 CMOS 的设置界面，如图 1-4 所示。

★ 设置开机密码的步骤

- ① 使用方向键移动到“Set Supervisor Password”项，按下【回车】键。
- ② 弹出“Enter new supervisor Password”对话框，提示输入密码，输入欲设置的密码，可以是六个字节的英文、数字，或符号。输入完毕后，按下【回车】键，如图 1-5 所示。
- ③ 按下【回车】键后，再输一次密码以确保密码正确。当两次密码确认无误后，密码设置完成。
- ④ 使用方向键移动到“Advance BIOS FEATURES”项，按下【回车】键。再用方向