突破常规玩电脑系列丛书

智美利达

怎么样，动心了吧？如果是，请赶快翻到目录页寻找你感兴趣的内容仔细阅读。相信我们，读完之后你一定不会失望的

COMPUTER

编程语言破解秘笈

计算机技术研究组　总策划

精彩内容导读

- 加密解密技术初探
- 全面破解VB编程
- FOX解密技术面面观
- Delphi破解技术大放送
- JAVA编程与控件破解

【特别提示】

本书荟萃了众多破解名家的“不传之秘”，旨在与读者朋友进行经验交流，切勿用于其他目的

内蒙古大学出版社

突破常规玩电脑系列丛书

编程语言破解秘笈

计算机技术研究组　总策划

内蒙古大学出版社

书　　名：突破常规玩电脑系列丛书（1-7）
编　　著：武新华
出　　版：内蒙古大学出版社（呼和浩特市大学西路235号 邮编 010021）
责任编辑：赵英
封面设计：南永夫
发　　行：全国各地新华书店
印　　刷：河南省瑞光印务股份有限公司
开　　本：850×1168　1/32
印　　张：7
字　　数：215千字
版　　期：2003年9月第1版　2003年9月第1次印刷
标准书号：ISBN 7-81074-508-5/TP·27
印　　数：1—5000册
定　　价：112.00元（本册定价16.00元）

为什么购买这本书

这是一本有关计算机加密与解密问题的书籍。这本书既是写给普通电脑迷的，同时更适合那些孜孜于计算机软硬件程序的探索者——Cracker。

对于普通的电脑迷，阅读本书的意义意味着你再也不需面对日益繁多的共享软件而茫然无措。我们知道，你曾经为它们心动，因为你确实需要它们的帮助去驾御你的计算机世界；但很多时候你又非常无奈，你无奈于自己的钱财，更无奈于对加密解密技术的无知以及由此导致的对你心爱之物的不可获得。与你相似的苦恼我们也曾经历，更深知援助之手在这一时刻所具有的意义。我们无法助你钱财，但有时候知识却远比钱财重要。这本书便具有这样的作用。

我们相信，有这样一本书置于你的案头，那许许多多在你过去看来难于登天的事情，你会突然发现却原来如此简单。

而对于更高一级的电脑玩家 Cracker 来说，阅读本书的意义却另有不同。去不断地探索未知，是每一个 Cracker 心目中永远的诱惑。作为一个 Cracker，注定了你与未知的对抗，而不能掌握一些必要的软件破解技术，是你无法忍受的羞耻。

的确，有那么多的共享软件，而你却不明白它们的程序原理，这是有辱于 Cracker 的称号的。当然，Cracker 的目的不是单纯地破解软件，而是通过跟踪软件了解程序思路，从而写出更好的程序。

破解也不在于数量多寡，关键是掌握方法，弄清注册码计算原理。本书中，我们集合了数十位破解高手苦心钻研出来的心得，提供了一般加密解密书籍都无法教你的秘技与妙招，我们相信，当你翻阅完这些 Cracker“老鸟”们轻易不会示人的“私藏秘典”，你也会很快地加入他们的行列。

本书就是这样一本讲解各种破解实例的教科书，这也是我们推荐你购买与阅读本书的理由。

目 录

第 1 章　加密解密技术初探

- 初识数据加密技术
- 学会养只看家的狗

随着互联网技术的不断发展，计算机网络给广大用户的工作与生活带来了巨大的影响，但我们在享受互联网带来便利的同时，却不得不面临很多随之而来的问题。

1.1　初识数据加密技术

就拿我们大家熟悉而常用的电子邮件来说，就存在被偷看、误投和伪造的诸多安全隐患。然而，网络的安全问题又何止局限于电子邮件系统，诸如网络新闻，文件传输等，同样存在此类问题。这就更加要求大家不仅需要保护商业通信中的经济信息，而且还需要保护个人通信的隐私权。

现在，国际互联网上的各站点，几乎都有各种各样的安全措施。例如：防火墙、网络软件加密狗等。但是这些都是系统或网站层次的安全措施，对于广大用户来说，更为直接有效的办法还是使用信息加密技术。

1．什么是加密

加密技术的使用至少可以追溯到 4000 年前，从古至今，它都是在敌对环境下，尤其是战争与外交场合，更是保护通信的重要手段。在信息社会的今天，这门古老的加密技术更加具有重要的意义。

计算机密码学是研究计算机的加密和解密以及变换的科学，尽管其背后的数学理论相当高深，但加密的概念却十分简单。

所谓加密就是指把数据和信息转换为不可辩识的密文的过程，使不应该了解该数据和信息的人不能够识别，欲知密文的内容，需将其转换为明文，这就是解密过程。

2．加密系统的组成

加密和解密过程组成了加密系统，明文与密文总称为报文，其实任何加密系统，不管形式多么复杂，至少都包括以下 4 个组成部分：

① 待加密的报文，也称明文；

② 加密后的报文，也称密文；

③ 加密、解密装置或算法；

④ 用于加密和解密的钥匙，它可以是数字、词汇或语句。

加密是在不安全的环境中实现信息安全传输的重要方法。例如：当你要发送一份文件给别人时，先用密钥将其加密成密文，当对方收到带有密文的信息后，也要用钥匙将密文恢复成明文。即使说发送的过程中有人窃取了，得到的也是一些无法理解的密文信息。

3. 加密方法

传统的加密方法有4种：代码加密、替换加密、变位加密和一次性密码簿加密。

① 代码加密

发送秘密消息的最简单方法，就是使用通信双方预先设定的一组代码，它简单而有效，得到了广泛的应用。例如：

密文：老鼠已经出洞了

明文：歹徒已经出现在目标区

② 替换加密

明文中的每个字母或每组字母被替换成另一个或一组字母，例如：

明文字母：A B C D ……

密文字母：L K J L ……

上面的这组字母之间的对应关系就构成了一个替换加密器。

③ 变位加密

变位加密不隐藏原明文的字符，但却将字符重新排列。例如：

密钥：3　1　4　5　2　6　0

明文：火 车 已 安 全 发 出

密文：出 车 全 火 已 安 发

④ 一次性密码簿加密

如果要既保持代码加密的可靠性，又保持替换加密器的灵活性，可采用一次性密码簿进行加密。

密码簿的每一页都是不同的代码表，可以用一页上的代码来加密一些词，用后将其毁掉；再用另一页的代码加密另一些词，直到全部的明文都被加密，破译该密文的惟一方法就是获得一份相同的密码簿。

随着密码学的不断地发展与进步，新的技术也不断涌现，如公开密钥加密技术，它与传统加密方法不同，它使用两把钥匙：一把公开钥匙、一把秘密钥匙。前者用于加密，后者用于解密，它也称为“非对称式”加密方法。

公开密钥加密技术解决了传统加密方法的局限性问题，极大地简化了钥匙分发的过程，它如果与传统加密方法相结合，可以进一步增加传统加密方法的可靠性，在许多重要的场所，已得到了广泛的应用。

1.1.1　提高加密强度的基本原则

为了提高软件加密的强度，下面我们就来看一下提高加密强度的一些基本原则：

1．加密点多且分散

软件的加密部分由多个加密点组成，每个加密点是一次对密钥的访问和校验过程，这个过程通常是被分成几步处理，然后分散在程序运行中，而不是集中在一起，因为这样可以增加解密者分析加密点的难度。

2．密钥的返回数据不能固定不变

对解密的分析有助于进行加密设计。解密的思路很多，一般来讲，从硬件角度主要是仿制、模拟密钥；从软件角度主要是先定位、分析加密点，然后寻找突破口。除非特殊需要，解密者一般不理会与加密无关的部分。

由于密钥的设计越来越完善，包括使用特殊的单片机、保密的通讯协议等，基于硬件的解密已经越来越少了，加密点的各个环节成为解密者的主要攻击目标。

【注意】

只要解密者发现了加密点中的一个漏洞，就可以直接解密，而不必分析加密点的其它部分。

举个常见的例子：

假设某个加密点在使用密钥时，密钥的返回数据是固定不变的，解密者就可以通过修改软件，去掉访问密钥的代码，将这个数据直接返回，而不必理会软件中是如何校验这个数据的。

3．加密复杂程度要高

通常用加密强度来综合评价软件的抗解密能力，在进行加密强度的分析时，习惯于从解密的角度出发，比如考虑解密复杂度（即解密难点）、解密工作量等。其中，

解密复杂度是最主要的因素，它是软件所有的加密点中最难解密的一个决定。

如果解密复杂度很低，即所有加密点都很容易攻破，就需要通过提高解密工作量来提高加密强度；反之，哪怕只有一个加密点，但是解密复杂度很高，加密强度还是很高的。

4. 设计加密点的3个基本要求

在设计加密点时，只有从以下3个方面着手，才能有效地提高解密复杂度：

① 入口数据随机对应加密点的起始环节

准备数据要求软件发送给加密锁的数据有很强的随机性；否则的话，解密者就可以统计出所有可能的输入输出，然后用软件仿真加密锁。

② 出口数据随机

对应加密点的中间环节：访问。密钥要求加密锁返回给软件的数据有很强的随机性，这个要求也等价于加密锁内的程序不可从外部求解，否则，解密者可以解析出加密锁内部的处理方法，进而用软件来取代锁。

③ 软件依赖于锁内程序的算法（而不是数据）

对应加密点的最后环节：校验返回，即软件如何使用加密锁返回的数据。从理论上的要求是：加密锁内的程序是软件不可分割的部分，且在软件中没有副本（即锁内的程序是从加密前的软件中移植过来的）。这是为了防止解密者通过跟踪返回数据的使用过程而推测出锁的功能。

以上每一点都是必需的，解密者只要攻破其中一个环节，整个加密点就被解了。由于加密锁的资源限制及软件的固有特征限制，真正达到这3点并不容易，但可以作为提高加密强度的基本依据。

1.1.2 软盘加密技术

如果您的软件是低价格通用软件，那您的保护模式可以考虑使用软盘加密。由于采用特别加密技术，其加密强度可与各种加密狗等媲美，能抵抗各种密钥盘拷贝工具，有效防止密钥盘被硬解密。同时具有价格低廉，使用方便等优点。

当然了，在采用光盘（CD-ROM）、网络等方式发布软件的时候，也可采用软盘加密这一方案。

该加密技术提供的软件及服务如下：

① 密钥盘制作软件 Keymaker.exe 限定了能制作密钥盘的数量（与该授权数量有关）。

② 密钥盘制作软件 Keymaker.exe 中可提供选择制作的密钥盘能在几台计算机上安装使用。如果没有特别指出，制作的密钥盘只能在一台计算机上安装使用。如果有该要求，可以在订做密钥盘时提出，可提供该功能。

密钥盘能安装计算机的选择范围是 1～100（如果要求密钥盘可安装计算机数量少于 5 台，不收费。多于 5 台，将按每 5 台算一个授权，加收部分费用）供软件调用的 DLL 动态连接库，如果您的编程语言是 VC，可提供 LIB 静态连接库；如果是 DOS 软件，可提供 OBJ 模块等。

1.1.3　自己动手编制加密软件

目前，绝大多数商业软件采用加密技术，其目的主要是为了保护软件开发者的利益和防止软件的非法扩散。不同的商业软件采用的加密技术是不同的，向开发商购买现成的商业加密软件，或自己动手开发加密软件已成为现阶段软件开发商的两大选择。商业加密软件保密系数固然很高，然而当这种加密软件被他人解密后，所有被这种加密软件加密的程序全都变得不攻自破。而自己编制的加密软件灵活性好，随时能够修改扩充，还可与商业加密软件结合使用。

下面将开始论述加密软件是如何编制的：

1．构造加密壳

构造加密壳是编制加密软件的核心部分之一，其工作原理是把一段用户编制的加密代码附加到可执行程序上，并通过修改原可执行程序的文件头，使原可执行程序入口指向附加程序。

当加密程序装入内存时，附加的加密程序首先执行，并且根据用户的不同需要，附加程序来完成不同的功能。

如判断是否有跟踪程序存在，识别用户口令，识别密钥盘、加密狗或加密卡等，如果满足一定条件则转入原可执行程序中执行。

由于附加的加密程序本身要进行二进制变换以及对原可执行程序进行解密还原，所以笔者建议最好还是使用汇编语言来编写附加的加密程序。

2．反跟踪技术

反跟踪技术是编制加密软件最关键的问题。评价一个加密软件的好坏，主要看其反跟踪技术是否过硬，如果加密软件没有强有力的反跟踪技术，软件内部的密钥就会暴露，以至于加密软件可能会在很短的时间内被破解。

下面将从常规反跟踪技术、反动态跟踪技术和反脱壳软件技术3方面来介绍加密软件的反跟踪技术。

① 常规反跟踪技术

常规反跟踪技术主要通过设置各种陷阱，自身做大量变形和跳转来迷惑和拖垮解密者，也是通常加密软件所采用的方法。

对于编制加密软件的初学者来说，掌握以下几种反跟踪技术是必不可少的：

● 破坏单步跟踪中断和断点中断

向int1和int3的中断向量地址写入无用数据，将堆栈设置在int1和int3的中断向量地址中或把对自身进行解密还原程序挂到int 3上。

● 封锁键盘输入

通过修改中断屏蔽寄存器21h的第一位或中断屏蔽寄存器61h的第七位来实现封锁键盘输入。

● 利用零类中断、溢出中断（int4）和时钟中断（int8）来实现隐蔽跳转

先将跳转的目标地址挂到以上中断上，然后当程序执行到需要跳转的地方时，人为地制造一个假象比如被零除或溢出，即可实现隐蔽跳转。

● 隐藏代码技术

在程序中一步一跳转，即第一条语句执行完后跳到第二条语句上。在第一条语句和第二条语句间加入汇编语言编译后的关键字如0ebh。

这样，程序执行时还会按照原来语句执行，但用反汇编工具只会看到一连串的跳转语句而看不到原程序，从而提高了加密程序的保密系数。

以上所介绍的反常规跟踪技术应结合使用，比如破坏单步跟踪中断和断点中断和封锁键盘输入技术就是结合隐藏代码技术，使加密程序的可读性降低。

笔者在这里强烈推荐隐藏代码技术，使用隐藏代码技术的加密程序，如用Gametool或其他调试程序跟踪，调试程序将无法对下一条语句进行正确定位。

② 反动态跟踪

“道高一尺，魔高一丈”，随着加密技术的不断进步，动态跟踪解密软件也在不断地推陈出新，而国人编制的解密软件更是层出不穷。

新版的动态跟踪软件如Gametool，Soft－ice都具有内存断点、中断断点及硬件断

点等强大功能。

在 1995 年 11 月，四川重庆的谢军先生曾经对 Soft－ice 进行了改进，使得改进后的 Soft－ice 可以在几秒钟内解密没有密钥盘的 Lock95。笔者也曾在没有密钥盘的情况下，用 Gametool 成功地解开 KV300、VRVNT 和 RAV 等软件。

动态跟踪软件可以轻松地越过前面所涉及的常规反跟踪步骤，直接从加密软件内部的某个中断开始跟踪。由此可见，反动态跟踪技术也是编制加密软件重要的一环。

下面将着重介绍检测 Gametool 和 Soft－ice 存在的方法。因为任何驻留内存的解密软件都会在内存中留下一些蛛丝马迹，以便检测自己是否重复驻留，由此便可以检测上述动态跟踪软件是否存在。

● 检测 Gametool 的存在

如果在 0：40h 到 0：0380h 之间的某一个双字为 00abcdefh 则说明检测到 Gametool 的存在。

● 检测 Soft－ice 及其改进版的存在

首先重置 int3 使其只含有一个返回语句（iret），然后用 ax K0，si K4647h（改进版为 4747h），di K4a4dh 调用 int3，如返回 si 不等于 4647h（改进版为 4747h）且 si 大于 0210h 则说明检测到 Soft－ice 存在。

【注意】

在检测到上述软件存在时，加密软件在做出反应（通常为退出或重启动）前，一定别忘记清内存以防止加密软件的内存映象被解密者发现。

③ 反脱壳软件

自 1995 年夏天《九五反加密工具箱》的问世，各类脱壳软件就层出不穷。按其工作方式大致可分为 2 类：

● 一类是以 MSCopy，Magickey，UNkey，RCopy，LLgz 和 UNall 为代表的以利用加密程序调用的系统中断为导线进行脱壳的解密软件；

● 另一类以 UNShell 为代表的以识别高级语言特定的文件头为导线进行脱壳的解密软件。

第 1 类解密软件不仅用来还原被加密程序，还被某些解密高手用来分析加密壳，使加密软件编制者们辛苦编制的十几 K 的加密代码赤裸裸地呈现在解密者面前。

对付第 1 类解密软件的方法是：

首先，在不调用任何中断的情况下记录下当前程序的 psp，然后，加密程序可以在任何时候读取当前 psp 并与所记录的 psp 相比较。如果相同，则说明程序没有被脱

壳，反之，加密程序做出反应（退出、重启动或陷入死循环）。

对付第2类解密软件的方法是：

在加密前，修改可执行程序的头部语句，下图为一个由C语言编译的可执行文件头部语句，将标号（2）与标号（3）的语句互换即可防止UNShell的脱壳，其他语言编译出的可执行文件与之大同小异，读者可做参考。

注：由于标号（1）的语句需重定向，所以不可改变标号（1）的语句。

1360：0000ba8d15movdx，158d（1）

1360：00032ecs：

1360：00048916be02mov［02be］，dx（2）

1360：0008b430movah，30（3）

1360：000acd21int21

1360：000c8b2e0200movbp，［0002］

以上笔者从两大方面谈及加密软件编写的方法，其核心问题为反跟踪技术，它直接关系到能否有效地保护加密软件的加密算法，如果算法暴露，加密软件将会被解得干干净净。

总之，加密技术既不是深不可测，也不是停止不前，加密技术的进步也带动着解密技术的进步，二者相互对立又相互联系。

1.1.4 软件的演示版、试用版

一套软件经常需要有供演示或者供试用的版本，这时可以不必修改软件，仅需要通过在加密锁中增加“倒计数”和“远程升级”功能，就可以实现从演示版、试用版到正式版的升级。

① 倒计数功能

加密锁利用倒计数功能来限制软件的使用次数。设计时，首先在数据区中设置一个倒计数单元然后修改锁内程序的返回部分：检查倒计数单元，如果为零则不返回数据；如为-1则先将倒计数单元减1，再正常返回数据。

【注意】

原来的锁内程序中不能有写数据区的指令，否则就会出现双写。使用时，将软件的可用次数预先写入倒计数单元。

加密软件每次运行时访问加密锁，倒计数单元会自动递减，当减到零时，锁就不返回数据，软件就被停止使用。

② 远程升级功能

远程升级功能就是在锁内的倒计数功能基础之上增加一个功能，专门用来重新设置倒计数单元。

所谓升级就是把倒计数单元由零改成-1，使软件由不可用变成可用，升级时必须修改锁的设置，但厂家只需给用户一组数据（或者给用户一个升级程序），而不必更换加密锁，故称“远程”。

每个用户的升级密码都不能一样，因此可以采用如下的方法：

加密锁内的程序在修改倒计数单元之前，先校验输入的密码与锁内保存的密码是否一致，不一致时马上返回。

每个锁都有一个公开的序列号，厂家保存与这个序列号相对应的密码，当用户需要升级时，厂家再通知给用户。

只要对锁进行设置就可以实现软件的演示、试用等，这种方法对用户和厂家都有好处。

对用户来讲，试用的不是简化版，而是与标准版完全一样，而且当决定购买时，升级也很方便。对厂家来讲，软件只有一个版本，销售方式却更灵活了，而且对加密的安全性也没有什么影响。

笔者采用了计次的方法（倒计数功能）来限制用户试用软件，没有使用计时或者限制日期，这是因为加密锁没有内置时钟，难以保证安全性。

当然，可以利用计算机的时钟，但是对于如何提高这种方式的安全性还有待研究。

【注意】

这里的升级功能是将软件升级为永远可用，如果想让软件反复升级，那么远程升级功能就必须用新的方法实现。

1.1.5　什么是反共享器技术

目前有许多人利用针对软件加密锁设计的共享器来达到盗用软件的目的。对此笔者设计的反共享原理是这样的：软件访问加密锁，必须首先通过初始化（Init）功能来获得加密锁的控制权，并且把相关的数据保存在参数表中的保留区中，以后每次访

间加密锁都必须使用这个参数表，参数表中的数据是次次更新的，所以每次都只能使用上次返回的，否则加密锁不工作。反共享机制是专门用来限制一把锁只能支持一套软件运行。

但有些共享器可以自动初始化端口，这样加密锁也被初始化，使锁的反共享机制失效如果加密设计时需要彻底避免软件被共享，则可以在软件启动时往锁的一个特定数据单元内写入一个随机数，然后在软件运行时检查这个数据是否被修改了，如果被修改了则出现了共享的软件，此时软件可以采取一些适当的反击措施。

1.2 学会养只看家的狗

现在很多家庭都拥有了电脑，如果电脑能按照事先的设定时间自动关机，则既可以控制孩子花费在电脑上的时间，同时也给大家的远程工作带来很大方便。在本章节中我们就将推荐这样一款小巧玲珑、使用简单、功能够用的中文软件狗。

1.2.1 “微型软件狗”试用小记

现在终于找到了这样一种“微型软件狗”，它是由西安“笨蛋”软件工作室的杨伟宁朋友编写的，大小仅为169K，试用后感觉很好。

“微型电脑狗”是一只微型的、“绿色”的、中文界面的软件狗，使用起来极其方便，而且它是完全免费的，可以随意使用，免费拷贝，但在拷贝时必须保持文件的完整性，最好连带目录一起拷贝。

软件运行时需要Msvbvm50.dll文件来支持运行。在“微型电脑狗”运行时，如果断电、死机，在下次开机后可以保持计时的自动接续。

启动后，如果要关闭它，必须首先输入密码，以避免孩子自作主张地改变事先设置的电脑运行时间。

当“微型电脑狗”进入关闭电脑的倒计时时，可发出相应声音进行提示。如果不想关闭电脑，可输入密码后进行改变。

同时为安全起见，在进行倒计时时，“注册表编辑器”和“系统策略编辑器”无法使用，输入密码后方可使用。