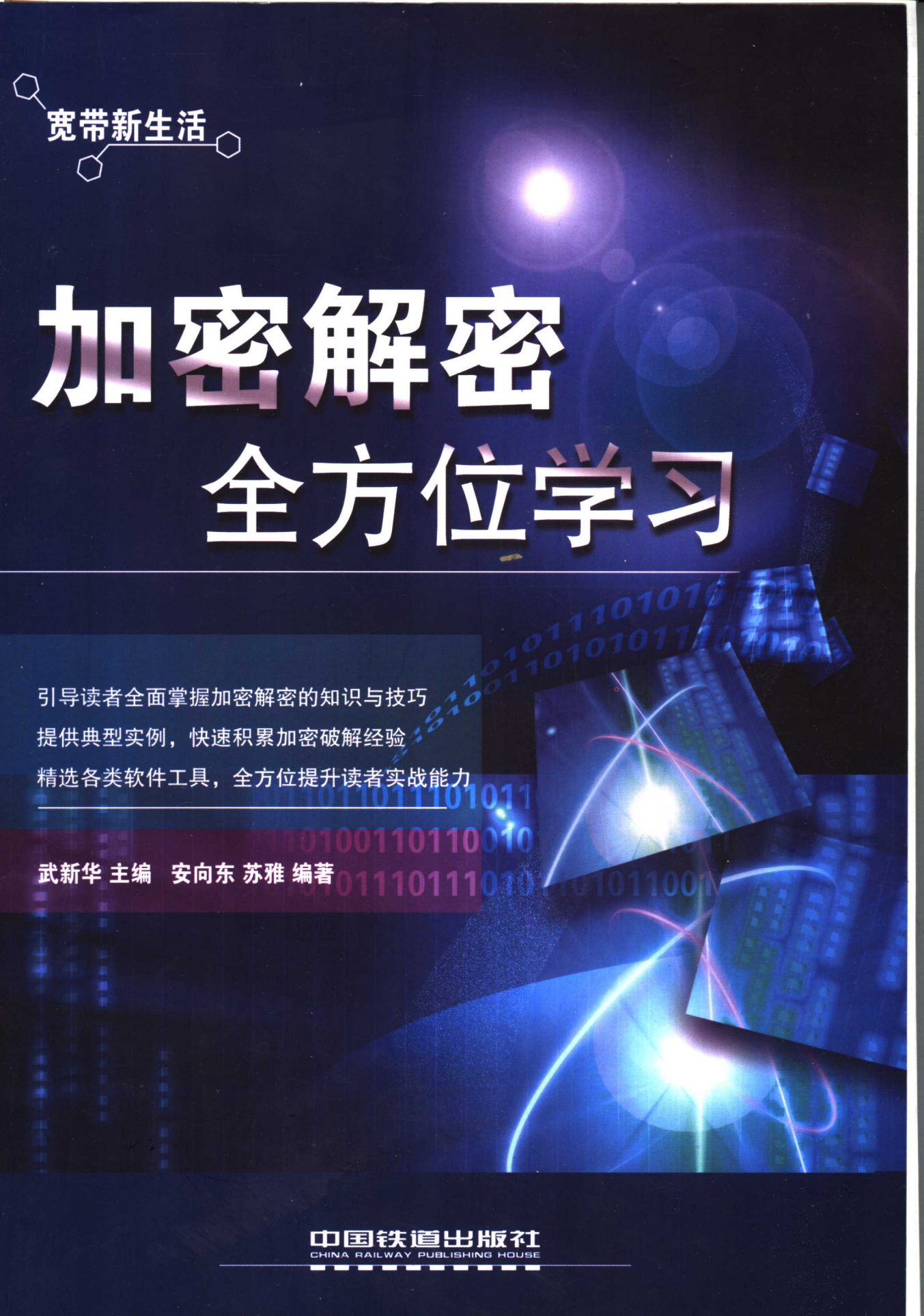
宽带新生活

加密解密
全方位学习



引导读者全面掌握加密解密的知识与技巧
提供典型实例，快速积累加密破解经验
精选各类软件工具，全方位提升读者实战能力

武新华 主编　安向东 苏雅 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

加密解密全方位学习

武新华　主编

安向东　苏　雅　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书紧紧围绕软件的加密与解密进行讲解，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，这就使读者能够对加密解密技术形成系统、深入的了解，能够更深层次地理解别人的编程思路，从而更好地提高自己的编程水平。全书共分为9章，包括反汇编调试静态与动态分析、加壳脱壳技术及其工具、反编译程序语言等内容。

本书内容丰富、图文并茂、深入浅出，适用于广大计算机爱好者；同时可作为一本加密解密爱好者的速查手册，也可作为软件开发人员及编程爱好者的首选用书。

图书在版编目（CIP）数据

加密解密全方位学习/武新华主编；安向东，苏雅编著. —北京：中国铁道出版社，2005.8

（宽带新生活）

ISBN 7-113-06665-8

Ⅰ.加… Ⅱ.①武…②安…③苏… 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（2005）第093246号

书　　名：加密解密全方位学习
作　　者：武新华　安向东　苏　雅
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街8号）
策划编辑：严晓舟　郭毅鹏
责任编辑：苏　茜　荆　波
特邀编辑：汪曙华
封面设计：薛　为
责任校对：李新承
印　　刷：河北省遵化市胶印厂
开　　本：787×1092　1/16　印张：20.25　字数：484千
版　　本：2006年1月第1版　2006年1月第1次印刷
印　　数：1～5 000册
书　　号：ISBN 7-113-06665-8/TP·1593
定　　价：29.00元

丛书序

着手构思这套《宽带新生活》系列丛书，其实源自自己寻找宽带上网参考书过程中所遇到的一些困难。市面上有关宽带上网的参考书林林总总，表面上看可谓是应有尽有了，但仔细查看之下，要找到真正适合自己的书却很难。笔者是一个有一定软件使用经验且每天都需要在网上泡着的人，虽然算不上专业，但还算熟悉一些宽带上网中的基本常识，根据不同的需求也可以完成一些基础操作。看参考书的目的主要是想学习日常上网操作中一些不容易接触到的、容易被忽略、不容易被掌握或迫切需要掌握的知识和技巧。

笔者在挑选自己需要的宽带上网参考书时，总希望书中能够多一些比较深入的知识和技巧，同时诸如：黑客、数码影音、加密解密、企业网站及个人商铺等内容要能引导自己入门。经过一番挑选，感到目前针对这种需求的参考书还是少了些，一般书中涉及这些专业的内容太少，而专业一点的书中内容又太深，总是令广大非专业的爱好者很难消化。

为了提升自己的宽带上网功力，笔者只好针对不同的需求买不同的书来进行学习，尽管每本书中适合自己的内容也就那么一点。于是当时就想如果有时间的话，一定要编一套能够适合广大宽带上网爱好者的参考书，比如以图解为主，采用任务驱动的写作方式，将一些前卫、时髦、实用的内容（如黑客、数码影音、加密解密、企业网站及个人商铺等）展现在广大读者面前。书的篇幅不要过长，但一定要实用、精练，尽量让读者在较短的时间内，掌握宽带上网应用的主要内容，为进一步深入掌握网络技术打下良好基础。

一、丛书特色

本套丛书在编写过程中贯穿了如下特色。

（1）提出问题

让读者知道自己所学的知识能解决什么具体问题。

（2）解决问题

通过解决问题使读者在对自己所学知识有直观、生动认识的同时，激发其深入探求、学习的兴趣。

（3）系统讲解

有了前两步做铺垫，再系统地讲解才有利于读者真正掌握所能够学习到的内容。一般的参考书更多强调的是知识内容的系统性，一上来就是内容的全面讲解，读者往往不知道哪些内容实用，而哪些功能很少用到，怎么能有耐心看下去？即使有足够的耐心看完，要将其实际应用却依然是一头雾水。

二、读者定位

现在市场上的针对全国数千万网民的大多数图书，或者完全是系统的讲解，或者几乎都是一些基础性的操作。因此，有网友感叹：买一本宽带上网的书容易，买一套宽带上网的好书困难。为此，我们特意按照任务驱动的方式，精心推出本套丛书，我们相信，只要您希望按照任务驱动的方式来学习，您一定会喜欢这本书的！

本系列丛书主要以互联网技术为核心，衍生出黑客攻防技术、加密解密秘技及企业宽带应用等，全方位剖析了用户在宽带上网中迫切需要用到的或迫切想要用到的技术，并力求对

其进行傻瓜式的讲解，使这些在外行人眼中本来高深莫测的技术变得通俗易懂，从而最大程度地满足上网爱好者的不同需求。

三、结束语

最后忠告：**不要迷信书本，要相信自己的实践**。由于宽带网络的飞速发展，任何一本书都很难保证书中所讲授的内容和实际应用中的软件完全一致，所以书中的疏漏和错误在所难免，本书当然也不例外。如果读者发现本书中有不妥或需要改进之处，请通过电子邮件 wxh12345@yeah.net 与笔者联系，笔者衷心感谢提供建议的读者，并真心希望在和广大读者互动的过程中能得到提高，谢谢！

前 言

网络的发展无疑极大地推动了共享软件的发展，但共享软件的蓬勃发展无疑也造就了另外一个行业的发展，那就是加密解密。

对于普通的电脑爱好者来讲，阅读本书的意义就意味着自己可能再也 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；但很多时候你又非常无奈，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，本书便具有这样的作用。

因此，这也是编写本书的初衷：目的不是单纯地教会大家如何破解别人的软件，而是让大家学会如何通过跟踪软件了解别人的编程思路，从容分析它的程序原理，从而写出更好的程序。

为了照顾初学者，本书特意经过精心编排，尽力做到以图例讲解代替大段枯燥的代码，使得各个层面的读者，甚至是那些从未接触过汇编和没有多少编程基础的读者也能够在阅读完本书后轻松入门。

而对于更高一级的电脑加密/解密高手来说，阅读本书的意义却另有不同。不断地探索未知，是每一个高手心目中永远的目标。作为一个加密/解密爱好者，则注定了自己与未知的对抗，而不能掌握一些必要的软件加密/解密技术，将是自己心中永远的痛。

为方便广大读者的阅读，本书完全采用图例步骤的讲解方法，使得图文能够紧密结合，尽可能地减少了长篇累牍的枯燥代码，理论讲解深入浅出，同时强调应用技能的快速掌握，使得本书简单易读，无疑是提高广大计算机爱好者知识、水平与技巧的一本不可多得的工具书。

本书凝聚众多网际高手加密/解密思想精华，并在对其加密/解密思想或操作步骤进行重新整理的基础上，进行了进一步的深化和理解，从而使得这些高深的加密解密技术不再遥不可及。我们相信，有这样一本书在手，将会突然发现，那许许多多在自己过去看来难似登天的事情，原来如此简单。

众多秘技尽在——《加密解密技术全方位学习》，欢迎大家阅读与选购本书。

本书由安向东、武新华、苏雅等编写，其中编写情况是：武新华负责第 1、2、5、8 章，安向东负责第 3、4 章，周海燕负责第 6 章，李超玲负责第 7 章，苏雅负责第 9 章，最后由武新华、安向东统审全稿。本书在编写过程中得到了许多热心网友的支持并参考了大量来自网络的资料，并对这些资料进行了再加工和深化处理，在此对这些资料的原作者表示衷心的感谢，没有大家的共同努力，本书是不可能完成的。

我们虽满腔热情，但限于自己的水平，书中的疏漏之处在所难免，欢迎广大读者批评指正。

最后，需要提醒大家的是：

根据国家有关法律规定，任何破解他人软件程序用于商业目的的行为都属于违法行为，希望读者在阅读本书后最好不要使用本书中介绍的破解技术对某些软件进行盗版，否则后果自负！

编 者

2005 年 9 月

目　录

目 录

第 1 章　加密解密技术基础

- 什么是加密/解密技术
- 加/解密的相关概念
- 软件加密保护技术与密码破解方式
- 熟悉汇编语言的几条常用命令
- 如何解密经过加密的软件

本章将介绍一些加密与解密的基础知识，这些内容会有助于大家更好地理解加密与解密的过程，并为系统地学习加密与解密知识打下牢固的基础。当然，对理论内容不感兴趣的读者也可以略过本章，并不影响对全书内容的理解。

1-1　什么是加密/解密技术

所谓加密就是利用不同的反跟踪技术将一些程序代码保护起来，在程序正常执行时再将其解开执行。解密则是利用计算机芯片的性质和系统的特点，手动跟踪来找到这些加密点，然后巧妙地利用一段插入的代码将加密点解开或绕开，从而达到使程序能正常运行的目的。

笔者以前也从事过加密与解密工作，在 DOS 下可以任意作为，并不觉得加密解密有多么高深的技术，尤其是现在的互联网时代，各种工具满天飞，大家只要有耐心基本都可以做到。

但解密也是把双刃剑，它极有可能导致众多的软件开发人员失去勇气和战斗力。因此，请大家一定要于事论事，并且要摆正自己的心态去看待加密与解密的关系。

现在我国最新修订的《著作权法》和《计算机软件保护条例》中均增加了有关软件加密的内容，加密技术不但在保护软件知识产权方面起到了重要作用，而且在保证软件及信息技术完整性、安全性方面也同样具有不可替代的作用，数据加密已成为当今信息安全技术的实力象征。

1-1-1　从密码学开始讲起

想必大家都知道，密码学实质上是以研究秘密通信为目的，即研究对传输信息采取何种秘密的变换以防止第三者对信息的窃取。密码学主要研究通信保密（保密有载体保密和通信保密两种），而且仅限于数据通信保密。而高速计算机和现代数学方法的广泛应用，一方面为密码技术提供了新的工具和概念，另一方面也成为了破译者的有力武器。

在密码加密算法的对立面就是密码分析，也就是密码的破译技术研究。加密与破译是一对矛盾，是相辅相成的，因此，了解破译对研究加密是非常必要的。而通常意义上的密码其实就是一组含有参数 k 的变换 E，如果设已知信息为 m，通过变换 E 就得到密文 c，即：$c=E_k(m)$，

这个过程称之为加密，参数 k 称为密钥。

其实，并不是所有含参数 k 的变换都可以作为密码的，还要求计算 $E_k(m)$不困难。如果第三者不掌握密钥 k，即使截获了密文 c，也是无法从密文 c 恢复到明文 m 的。从密文 c 恢复到明文 m 的过程称之为解密。解密算法 D 是加密算法 E 的逆运算，解密算法也是含参数 k 的变换。

因此，传统密码加密的密钥 k 和解密的密钥 k 是相同的，所以也叫对称密码。通信双方用的密钥 k 是通过秘密方式由双方私下约定产生的，只能由通信双方秘密掌握。

1-1-2 加密技术概述

在计算机上实现的数据加密，其加密或解密变换是由密钥控制实现的。密钥（Keyword）是用户按照一种密码体制随机选取的，它通常是一个随机字符串，是控制明文和密文变换的唯一参数。

根据密钥类型不同可将现代密码技术分为两类：一类是对称加密（秘密钥匙加密）系统；另一类是公开密钥加密（非对称加密）系统。对称钥匙加密系统是加密和解密均采用同一把秘密钥匙，而且通信双方都必须获得这把钥匙，并保持钥匙的秘密。

1．对称加密系统

对称加密系统最著名的是美国数据加密标准 DES、AES（高级加密标准）和欧洲数据加密标准 IDEA。1977 年美国国家标准局正式公布实施了美国的数据加密标准 DES，公开了它的加密算法，并批准用于非机密单位和商业上的保密通信。随后 DES 成为全世界使用最广泛的加密标准。加密与解密的密钥和流程是完全相同的，区别仅仅是加密与解密使用的子密钥序列的施加顺序刚好相反。

对称加密系统的安全性主要依赖于以下两个因素。

① 加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的。

② 加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性。

因此，就没有必要确保算法的秘密性，而需要保证密钥的秘密性。对称加密系统的算法实现速度极快，从 AES 候选算法的测试结果看，软件实现的速度都达到了每秒数兆或数十兆比特。对称密码系统的这些特点使其有着广泛的应用。

因为算法不需要保密，所以制造商可以开发出低成本的芯片以实现数据加密。这些芯片有着广泛的应用，适合于大规模生产。

2．公钥加密系统

自公钥加密问世以来，学者们提出了许多种公钥加密方法，它们的安全性都是基于复杂的数学难题。根据所基于的数学难题来分类，有以下 3 类系统目前被认为是安全和有效的：大整数因子分解系统（具有代表性的有 RSA）、椭圆曲线离散对数系统（ECC）和离散对数系统（具有代表性的有 DSA）。

当前最著名、应用最广泛的公钥系统 RSA 是由 Rivet、Shamir、Adelman 提出的（简称为 RSA 系统），它的安全性是基于大整数因子分解的困难性，而大整数因子分解问题是数学上的著名难题，至今没有有效的方法予以解决，因此可以确保 RSA 算法的安全性。RSA 系统是公钥系统的最具有典型意义的方法，大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是 RSA 算法。

1-1-3 数据加密的基本概念

数据加密是一种限制对传输数据的访问权的技术。原始数据（也称为明文，plaintext）被加密设备（硬件或软件）和密钥加密而产生的经过编码的数据称为密文（ciphertext）。将密文还原为原始明文的过程称为解密，它是数据加密的反向处理，但解密者必须利用相同类型的加密设备和密钥对密文进行解密。

数据加密的基本功能包括：

① 防止不速之客查看机密的数据文件。

② 防止机密数据被泄露或篡改。

③ 防止特权用户（如系统管理员）查看私人数据文件。

④ 使入侵者不能轻易地查找一个系统的文件。

个人用户最常见的加密就是在上网输入密码时，文本框中显示出的是星号（*），这是一种简单的数据加密，不管密码是什么，这种加密技术都会将它显示为星号。

本书将主要讲述软件的加密和解密，这也许是一个令广大读者感到高深莫测的话题，因此认为是一些晦涩难解的专业技术讲解而不愿去阅读。

其实阅读本书时大可不必这样想，本书中所讲述的加密与解密，由于篇幅和作者相应技术水平的限制，只是简单介绍了一些加密解密的基本原理和相关的软件使用方法，而没有妄自研究加密与解密技术，因为本书的目的只是想让大家了解那些比较流行的加密和解密技术实现机理，起到一个软件加密与解密的启蒙作用。

众所周知，计算机软件极易被复制。一套商业软件从构思、编程、调试到完成，软件开发者付出了很多心血，如果轻易被他人盗版，损失将是巨大的。

所以软件商为了维护自己的利益，一般都采取了各种保护手段来防止非法用户盗用自己的软件。软件狗便是一种插在计算机并行口上的软硬件结合的软件加密产品，软件开发者可以通过接口函数和软件狗进行数据交换（即对软件狗进行读写），来检查软件狗是否插在并行口上；或者直接用软件狗附带的工具加密自己的 EXE 文件（俗称“包壳”）。

这样，软件开发者可以在软件中设置多处软件锁，利用软件狗作为钥匙来打开这些锁，如果没有插软件狗或软件狗不对应，软件将不能正常执行。常见的加密狗有：微狗、USB 狗、光盘狗等（由于软件狗的加解密技术涉及到更深层次的商业软件保护的内容，所以在本书中笔者暂不做介绍。）

【提问】

首先大家需要懂得一个原则，进行软件解密在某种程度上并不仅仅是为了破坏软件，任何破解都只能是用于个人，而绝不能用于网络传播或转予他人，否则是违法的。

下面来看几个常见的需要进行软件解密的情况：

① 磁盘加密技术

绝大多数的教学盘都用磁盘加密技术来保护正版软件的合法使用性，但这样做最大的弊端就是磁盘的反复读取会大大地缩短磁盘的使用寿命，如果使用一些解密技巧，便可以高枕无忧了。

② 密码破解

很多游戏软件都需要密码才能进入，每次翻阅说明书夹缝中的密码表是不是很烦？既然是花了钱的正版用户，为什么还要这样烦琐？而且一旦说明书丢了，那该怎么办呢？因此，最简单的方式就是破解。

③ 硬件保护

诸多的不良接触是不是令人头疼？如果机箱动不动就要让自己不断地尝尝“触电”的感觉，是不是扔了这个铁皮包裹的家伙更好？

④ 最有效的学习方式

有时候为了学习软件编程高手们的加密算法应用技巧，或是为了试验一个破解工具的实用程度，通常会对一些常见软件进行破解，从中学习国外软件加密算法应用的技巧。

⑤ 口令遗忘

口令在增加安全性的同时，也增加了遗忘口令可能带来的不必要麻烦，破解口令在这个时候就显得十分重要。

1-1-4 为什么要进行加密/解密

为什么要加密呢？加密的结果就是让用户不能随便使用软件产品，从而防止盗版。为什么不能随便使用软件呢？因为这是个商品经济社会，一切都要以经济利益为核心和出发点。别人在开发软件产品中付出了人力、物力和财力，需要从中得到回报，维持生存，所以只有在付出了合适的费用之后，才能得到使用别人软件的权力。

为什么要解密呢？这个问题不太好回答，因为解密的缘由很多，不同的人有不同的动机。可能只是因为对解密技术感兴趣；可能就是因为想要无偿地、免费使用软件；可能是因为需要用某个软件，虽然愿意付钱，但是很难办到；可能是为了盗版，获取非法利益……总之，你有你的理由，我有我的根据，但大家都走到一起来了。

早期软件加密的操作系统平台主要是 DOS，在那个时代，人们可以很容易地写个程序控制整个计算机。因为 DOS 比较简单，安全性较差，用户可以进行各种低层操作，例如调用各种中断、读写内存区域、操作 I/O 端口等。总之，利用 DOS 本身提供的环境，几乎可以控制任何想要控制的东西，甚至控制 DOS 本身也不是难题。

那个时候的加密技术主要有磁盘加密（包括软盘和硬盘）、文件和目录的加密、各种硬件（加密卡、加密狗等）加密等。当时最流行的莫过于软盘的加密技术了，包括特殊磁道（如额外磁道、螺旋磁道、无缝磁道等）、特殊扇段（超长扇段、乱序扇段、异常 ID 等）、特殊方法（如弱位技术、FM 格式法、磁道噪声法、针孔加密技术等）。

那时常会见到很多软件都需要钥匙盘，那些钥匙盘用的就是各种各样的软磁盘加密技术。

为了防止解密，很多软件还运用了多种反跟踪技术，比如修改中断向量、锁键盘、关闭显示屏、覆盖技术、废指令、逆指令流、指令队列预取法等。

总之，DOS 时代可以充分运用自己的想像力去构造各种各样新奇的加密技术，因为 DOS 给了用户很多自由发挥的空间。

到了 Windows 时代，就会觉得一切都变了，自己不再是主人，而只能在限定的范围内活动。Windows 把底层的东西都隐藏了起来，人们只能看到各种各样的壳，至于里面的东西，