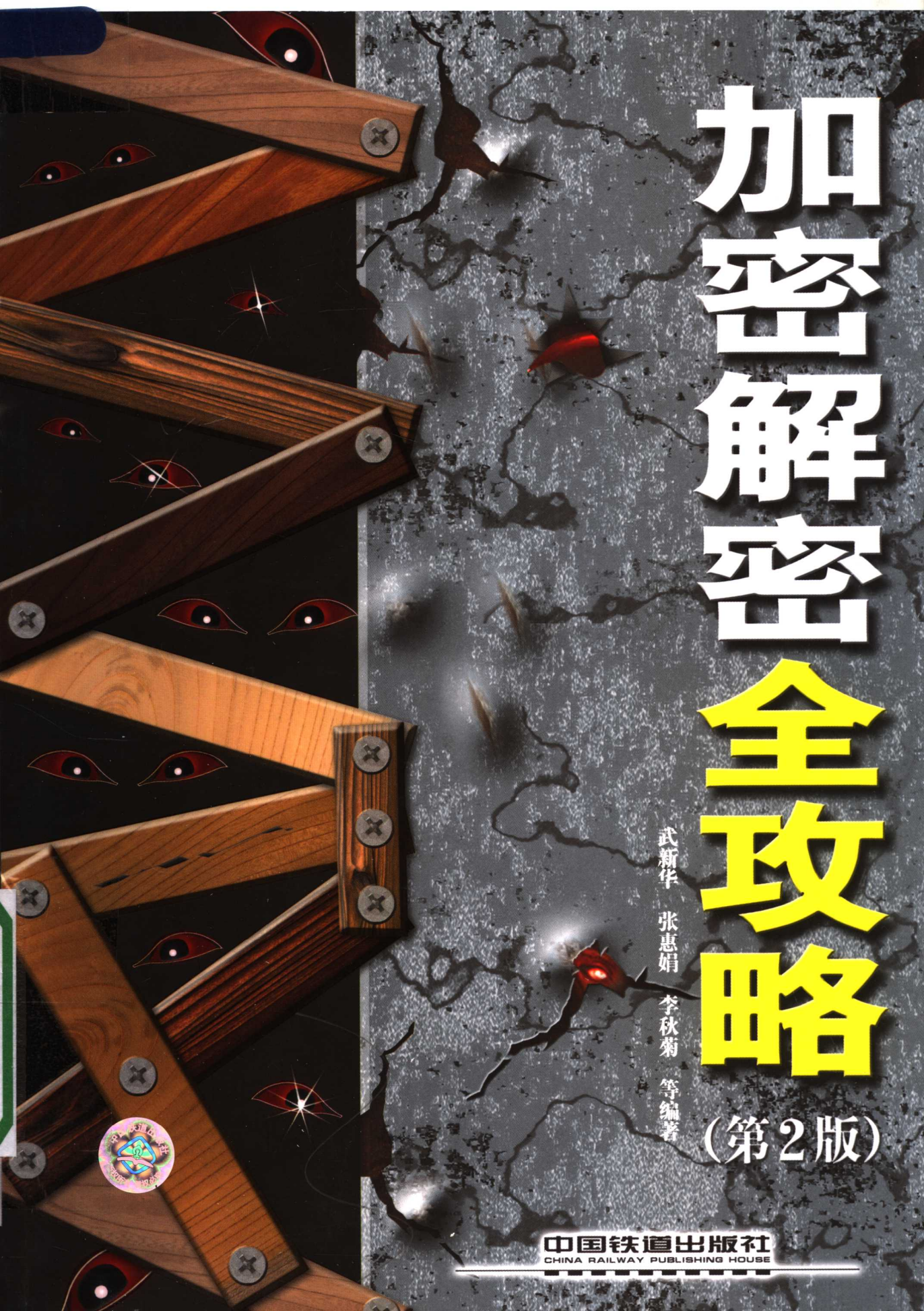

加密解密全攻略

（第2版）

武新华　张惠娟　李秋菊　等编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

加密解密全攻略（第2版）

武新华 张惠娟 李秋菊 等编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书紧密围绕软件的加密解密技术进行讲解，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，使读者对加密解密技术形成系统、深入的了解，通过更深层次地理解程序的编程思路，提高自己的编程水平。全书共分为 14 章，包括加密技术基础、破解技术基础、常见的软件加密技术、Win32 编程技术、静态反汇编工具、动态跟踪分析工具、注册认证和注册机、神秘的壳技术、补丁技术大揭秘、数据加密技术简述、应用加密软件的使用、网络验证技术应用、应用软件加密解密技术、编程技术与光盘加密解密技术等内容。

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、软件开发从业人员和编程爱好者，也可作为加密解密爱好者的速查手册。

图书在版编目（CIP）数据

加密解密全攻略 / 武新华等编著. —2 版. —北京：中国铁道出版社，2008.3

ISBN 978-7-113-08700-5

Ⅰ.加… Ⅱ.武… Ⅲ.电子计算机－密码术 Ⅳ.TP309.7

中国版本图书馆 CIP 数据核字（2008）第 028106 号

书　　名：加密解密全攻略（第 2 版）

作　　者：武新华　张惠娟　李秋菊等

出版发行：中国铁道出版社

策划编辑：严晓舟　荆　波

责任编辑：荆　波　白　钰

封面设计：付　巍

封面制作：白　雪

印　　刷：北京市彩桥印刷有限责任公司

开　　本：787×1092　1/16　**印张**：23.5　**字数**：552 千

版　　本：2008 年 5 月第 2 版　2008 年 5 月第 1 次印刷

印　　数：1～5000 册

书　　号：ISBN 978-7-113-08700-5/TP・2746

定　　价：36.00

前　言

随着网络技术的飞速发展，越来越多的人投身于网络大潮。虽然网络给我们的生活带来了方便和快捷，但它不稳定和不安全的特性，使得计算机上信息的安全不容忽视，加密解密技术由此应运而生。

加密解密这个看似新鲜陌生的名词已经在不知不觉中深刻影响我们的日常生活。当有一份私密的文档不想让其他人看到，当公司重要商业机密禁止泄露，当需要找回忘了密码的文件，此时，加密解密技术便是解决这些问题的利器。

使用加密解密技术可以轻易解决上述问题，但本书的目的除了教授破解软件的方法外，还讲解了遇到加密解密难题时的解决方法，使读者学会使用跟踪软件分析破解思路，找出程序运行原理的方法，从而编写出相应的破解程序。

本书为不具备专业的加密解密知识，只是为文档、邮箱加密或破解简单的忘记了密码的文件的用户提供需求。通过大量图例，并配以清晰直观的讲解，使得从未接触过加密解密的读者也可以轻松阅读掌握。

而对于理论水平和实际操作能力都很强的读者来说，本书可作为辅助的工具，通过精心编排的实例让高水平读者不断提高、拓宽思路、开阔视野、获得经验。

本书是《加密解密全方位学习》的修订版，对初版的版式、讲解方式和示例软件等方面进行了改进。本书在编写过程中得到了众多热心网友提供的资料，在此对这些资料的原作者表示衷心的感谢。

本书由武新华、张惠娟、李秋菊等编写，其中编写情况是：武新华负责第 1 章，陈旭生负责第 2 章，彤丽负责第 3 章，张惠娟负责第 4 章，李秋菊负责第 5 章，段玲华负责第 6 章，陈艳艳负责第 7 章，何勇负责第 8 章，陈恩波、张鑫负责第 9 章，李防负责第 10 章，安向东负责第 11 章，岳宝华负责第 12 章，曹燕华第 13 章，梁铎负责第 14 章，最后由武新华统审全稿。

由于编者水平所限，书中难免有疏漏之处，欢迎广大读者批评指正。

编　者

2008 年 2 月

声明：

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行为都属于违法行为。望读者在阅读本书后切勿使用本书中介绍的破解技术对某些软件进行盗版制作，否则，后果自负。切记切记！

目　录

CHAPTER 1

加密解密技术基础

重点提示：

加密解密技术的概述

加密解密中的相关概念

几个常见的汇编语言命令

软件解密与注册保护方式

学习目标：

本章主要讲述了什么是加密解密技术，为什么要进行加密解密以及软件解密方式与注册保护方式等。通过对本章的学习，读者可以对加密解密技术基础、常用的汇编语言命令等有一个全面了解，为以后深入学习加密解密知识打下基础。

随着计算机技术的不断发展，互联网用户的数量与日俱增，涉及到的数据安全问题就成了当今计算机领域中的焦点问题，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、远程侦听等让人一听就胆战心惊。病毒、黑客的放肆猖獗，更是使身处今日网络时代的人们时刻感觉到危险无处不在。如何才能保障计算机数据信息的安全，也就成为不容人们回避的问题。

因此，人们就想到了要对自己的数据进行加密。例如打开计算机时要输入密码，上网时在各式各样文本框中要输入验证码，这些都是最基本的加密技术。现代的计算机加密技术就是为了适应网络安全需要应运而生的，它为一般的电子商务活动提供了安全保障，如在网络中进行文件传输、电子邮件往来和进行合同文本的签署等。

1.1 加密解密技术概述

加密解密技术是一门古老而深奥的学文，它对一般人来说是陌生的，因为长期以来，它只在如军事、外交、情报部门等很小的范围内使用。计算机加密技术是研究计算机信息加密、解密及变换的科学，是数学与计算机之间的交叉学科，也是一门新兴的学科。在国外，它已成为计算机安全最主要的研究方向，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，而不在算法的保密性。

对数据的加密的确是这样。对于不愿意让别人看到这些数据（数据的明文）的人来说，使用可靠的加密算法对数据进行加密后，只要破解者不知道被加密数据的密码，他就不可能解读这些数据。

但是，软件的加密不同于数据的加密，它只能被“隐藏”。不管愿意不愿意让别人（合法用户，或 Cracker）看见这些数据（软件的明文），软件最终总要在机器上运行，因此对于机器来说，它就必须是明文。既然机器可以“看见”这些明文，那么 Cracker 通过一些技术便也可以看到这些明文。

于是，从理论上来说，任何软件加密技术都可以被破解，只是破解的难度不同而已，有的要让最高明的破解者忙上几个月，有的可能不费吹灰之力就被破解了。所以，要不想被盗版，就只有增加 Cracker 的破解难度。让破解者花费在破解软件上的成本，比破解这个软件的获利还要高。

加密也可提高终端和网络通讯的物理安全，有三种方法可用来加密传输数据：

（1）链接加密

在网络节点间加密，在节点间传输加密，传送到节点后解密，不同节点之间使用不同的密码。

（2）节点加密

与链接加密类似，不同的只是当数据在节点间传送时，不用明码传送，而是用特殊的加密硬件进行解密和重加密。

（3）首尾加密

对进入网络的数据加密之后，再等数据从网络传送出之后再进行解密，网络本身并不会知道正在传送的数据是否为加密数据。这种加密方法的优点是：网络上的每个用户可有不同的加密关键词，并且网络本身不需添加任何专门的加密设备；缺点是每个系统必须有一个加密设备和相应的软件即每个系统必须自己完成加密工作。

摘要是一种防止数据被改动的方法，其中用到的函数叫摘要函数。这些函数的输入可以是任意大小的消息，而输出是一个固定长度的摘要。摘要有这样一个性质，如果改变了输入消息中的任何东西，甚至只有一位，输出的摘要都将会发生不可预测的改变，也就是说输入消息的每一位对输出摘要都有影响。

总之，摘要算法从给定的文本块中产生一个数字签名（fingerprint 或 message digest），数字签名可以用于防止有人从一个签名上获取文本信息，或改变文本信息内容和进行身份认证。摘要算法的数字签名原理在很多加密算法中都被使用。

MAD 摘要算法的设计是出于利用 32 位 RISC 结构来最大化其吞吐量，而不需要大量的替换表的目的来考虑的。

MAD 算法是以消息给予的长度作为输入，产生一个 128 位的“指纹”或“消息化”。要产生两个具有相同消息化的文字块或产生任何具有预先给定“指纹”的消息，在计算上都被认为是不可能的。

MAD 摘要算法是个数据认证标准。MAD 的设计思想是要找出速度更快，比 MAD 更安全的一种算法，MAD 的设计者可以通过使 MAD 在计算上慢下来，以及对这些计算进行一些基础性的改动来解决安全性这一问题，它是 MAD 算法的一个扩展。

1.1.1 什么是加密技术

所谓加密技术是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。加密技术包括两个元素：算法和密钥。算法是将普通的信息或者可以理解的信息与一串数字（密钥）结合，产生不可理解的密文的步骤，密钥是用来对数据进行编码和解密的一种算法。通过数据加密技术，可以在一定程度上提高数据传输的安全性，保证传输数据的完整性。

一个加密系统至少包括如下四个组成部分：

- 未加密的报文，也称明文。
- 加密后的报文，也称密文。
- 加密解密设备或算法。
- 加密解密的密钥。

明文用 M（消息）或 P（明文）表示，它可以是比特流（文本文件、位图、数字化的语音流或数字化的视频图像）。至于涉及到计算机，P 是简单的二进制数据。明文可被传送或存储，无论在哪种情况，M 指要进行加密的信息。

密文用 C 表示，它也是二进制数据，有时和 M 一样大，有时稍大（通过压缩和加密的结合，C 有可能比 P 小些。然而，仅仅加密通常达不到这一点）。

加密函数 E 作用于 M 得到密文 C，用数学表示为：

$$E(M)=C$$

相反地，解密函数 D 作用于 C 产生 M：

$$D(C)=M$$

先加密后再解密消息，原始的明文将恢复出来，下面的等式必须成立：

$$D(E(M))=M$$

数据加密的基本过程就是对原来明文的文件或数据按照某种算法技术处理，使它成为一段不易辨认的乱码，称为“密文”，只有在输入相应的密钥之后，才能显示出其本来的文

字内容，利用这种方法来达到保护数据文件不被非法窃取、阅读的目的。

1.1.2 为什么要进行加密/解密

在当今社会必须要使用加密技术来保护数据的安全，众所周知，使用互联网进行文件传输、发送电子邮件是进行业务往来的重要手段，但互联网是基于 TCP/IP 协议存在，TCP/IP 协议由于本身具有不安全性，就需要引起人们的高度重视，特别是在进行一些机秘密文件的网络传输的时候。

互联网把全世界连接成一个整体，带来了无限的商机和便利，为了能在安全的基础上享受这些便利，就要使用数据加密技术和基于数据加密技术的数据签名。

加密技术在网络上的应用非常必要，主要就是防止机密文件或有用的内容在网络传输时被非法截获或破坏。

如果一个公司通过电子邮件给另一公司发送一份比较机密的文件，说不定此时就会有人准备窃取这份关乎两个公司生死存亡的文件，这样的损失是无法估价的。解决这个难题的方法就是加密，加密后的文件即使被窃取也是不可读的，只是一堆乱码，所以说使用加密技术是当今网络社会的必然趋势。

数字签名基于加密技术，其作用是用来确定用户是否真实存在，一般应用在收发电子邮件上。当用户接受到一封电子邮件，邮件上标有发信人的姓名和邮箱地址，有些人简单地认为邮件标示的发信人的姓名就是真实的，实际上并不完全是这样，这时，就可以用到加密技术基础上的数字签名来确认发信人的真实身份了。

文件加密不只是针对电子邮件和网络上传输的文件，也可以对静态的文件进行加密保护，像 PIP（Project Information Portal，项目信息平台）软件就可对磁盘、硬盘中文件或文件夹进行加密。

加密类型可以大致分为 3 类：

（1）私用密钥加密技术

即利用一个密钥对数据进行加密，另一方收到数据之后，使用同一个密钥进行解密。这种加密的特点就是运算量小，速度快。缺点是加密解密使用同一个密钥，一方泄露密钥，整个数据信息就暴露无遗。

（2）公开密钥加密技术

这种加密技术使用一对密钥进行加密，一个是公开密钥，一个是私有密钥。加密时使用公开密钥，接收者收到信息可以使用私有密钥解密。它的安全系数比私用密钥加密技术高，可以广泛用于通信、数字签名上。

（3）不用考虑解密问题。

这种加密技术就是一些像口令加密的类型，用户只需要进行加密后，与以前的加密进行比较就可以了，而不需要考虑解密问题。

1.1.3 加密技术的发展趋势

加密技术的渊源距离现代社会甚为久远，最早源于大约公元前 2000 年，那时的埃及人就发明了象形文字来保护秘密信息不会轻易被别人发现。它不是现在要讲的加密技术，只是作为一种加密的概念来进行理解。

在现代社会中，加密解密技术最常用于对军事领域中机密信息进行加密、破解。随着

计算机技术的不断发展，运算能力的不断增强，以往的密码就变得十分不安全，非常容易破解，于是人们又研究出了新的数据加密方式，比如利用 ROSA 算法产生的私钥和公钥。

加密技术大致有以下几种发展趋势：

（1）私用密钥加密技术与公开密钥加密技术相结合

这两种加密技术各有优势，在实际应用中可以结合使用 DES/IDEA 和 RSA，以 DES 为“内核”，RSA 为“外壳”，对于网络中传输的数据可以用 DES 或 IDEA 加密，而加密用的密钥则用 RSA 加密传送，这样既能保证加密信息的安全又提高了加密和解密的速度，可以看作是加密技术发展的趋势之一。

（2）寻找新的加密算法

现在广泛使用的加密算法，普遍存在这样或那样的缺点和不足，有的加密速度快却不能保证数据安全，有的算法繁琐却实现速度极慢。正因为这样，所以跳出常规算法为基础的思路，脱离基于数字问题的构造方法，寻找新的加密方法也是当今加密界的一大趋势。

（3）加密最终要集成到网络和系统中

例如 IPV6 协议就实现了内置加密的支持，而硬件方面 Intel 公司正在研制一种加密协处理器，就可以集成到计算机的主机上。

1.2 加密解密中的相关概念

在学习加密解密技术的过程中要经常涉及到一些常用概念，只有熟悉并理解了这些概念的具体所指，才能更加深入地进行学习。

下面就详细介绍一下在加密解密过程中经常涉及的几个概念。

1. 断点

所谓断点是指程序被中断执行的地方。程序产生中断就是由于有特殊事件发生，计算机暂停当前的程序运行，转而去执行别的程序，当执行完毕后再返回执行被中断的程序。

解密的过程就是当程序去获取输入的注册码，并准备和正确的注册码相比较时将其中断，通过分析找到正确的注册码。这就需要为被解密的程序设置断点，在适当的时候切入程序内部，追踪到程序的注册码，以达到破解该程序的目的。

2. 领空

所谓程序的领空，说白了就是程序自己的地方，也就是要破解程序的程序码所处的位置。在 DOS 时代，基本上所有的程序都是工作在中断程序之上的，即几乎所有的 DOS 程序都会去调用各种中断来完成任务。

但到了 Windows 时代，程序没有权力直接调用中断，Windows 系统提供了一个系统功能调用平台（API），就像 DOS 程序以中断程序为基础一样，Windows 程序以 API 为基础来实现和系统打交道，从而实现各种功能，所以 Windows 下的软件破解其断点设置是以 API 函数为基础的，即当程序调用某个 API 函数时中断其正常运行，然后进行解密。

例如，在 SoftICE 中设置下面的断点：Bpx GetDlgItemText（获取对话框文本），当要破解的程序要读取输入的数据而调用 GetDlgItemText 时，将立即被 SoftICE 拦截到，从而被破解的程序停留在 GetDlgItemText 的程序区，而 GetDlgItemText 是处于 Windwos 自己管