1DVD 500分钟超大容量多媒体视频

- 60段精彩讲解视频倾囊相送
- 多方位展示加密解密安全技巧

加密解密全攻略

[第3版]

武新华 余建国 王英英 王振武 等编著

涵盖广泛 完善的篇章结构，囊括相关理论、常用工具、操作技巧和典型案例。

步步为营 小技巧和大实例相得益彰，操作步骤环环相扣，引导读者迅速上手。

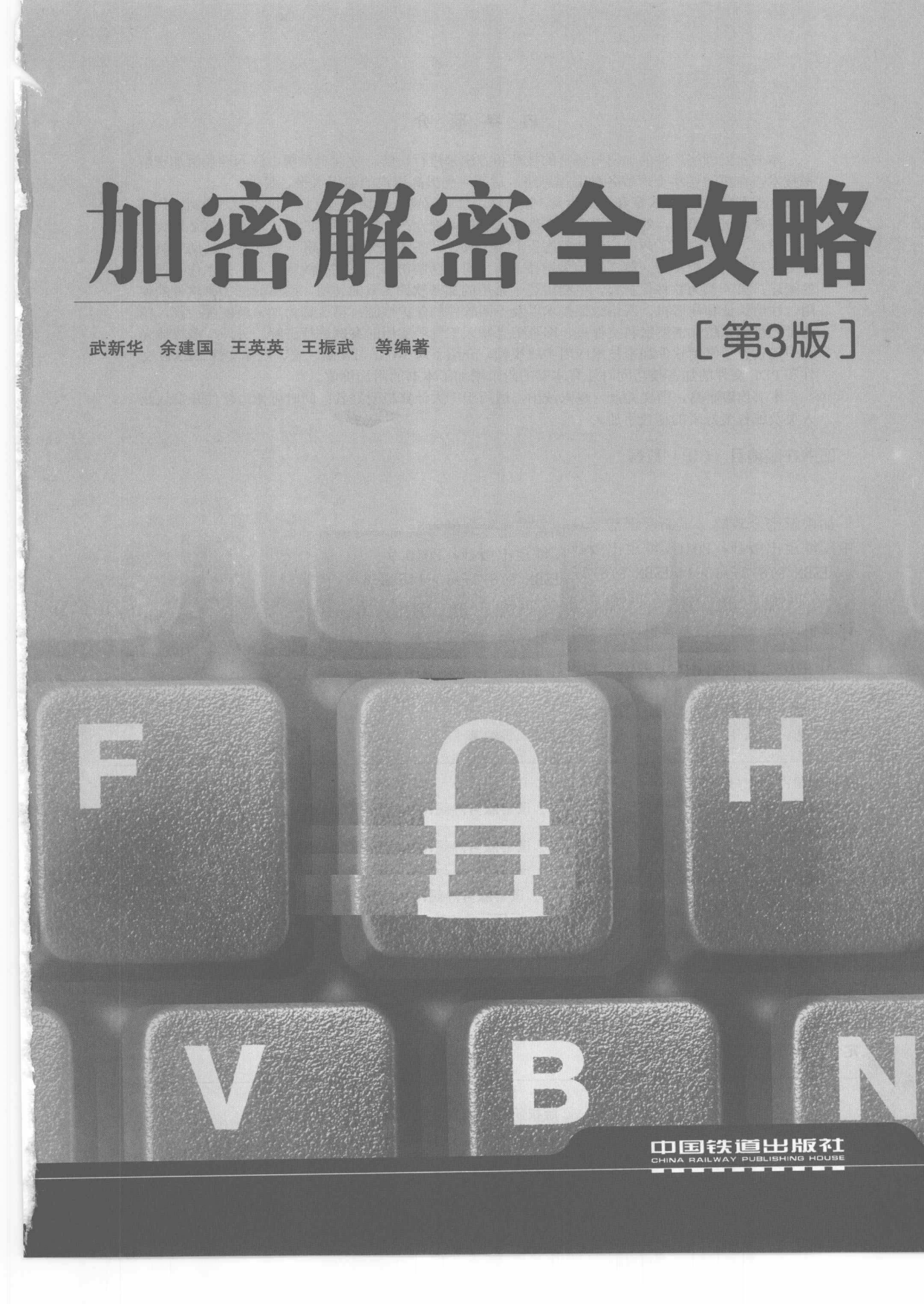
定位精准 秉承实用的理念，着眼于帮助初级读者积累数据、软件加密与解密技巧，提升解决实际问题的能力。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

加密解密全攻略

[第3版]

武新华　余建国　王英英　王振武　等编著



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的技巧和方法来进行讲解，使读者系统、深入地理解加密解密技术，在更深层次上理解各种编程思路，从而达到提高用户的编程水平之目的。

全书共分为 5 篇 13 章和 1 个附录，第 1 篇为加密解密入门篇，包括加密解密技术基础，代码分析与常用工具简介，对基本概念和文件格式等作详细介绍，夯实读者的理论基础。第 2 篇为典型工具篇，详细介绍了应用广泛的静态反汇编工具、动态跟踪分析工具和一些必备的辅助工具，并配备翔实的分析实例。第 3 篇为关键技术篇，对加密解密方面的加壳脱壳、补丁技术作了详细的阐述；第 4 篇为软件保护篇，主要讲述了常用的加密软件工具的使用，网络验证加密软件的使用，注册认证和注册机、网络验证技术以及不同软件的保护措施；第 5 篇为加密解密实战篇，精选了光盘和系统加密解密和文件夹、网页信息聊天工具等实用的案例进行讲解。另外，多媒体光盘中还设置了常用软件加密技术应用实战视频，介绍了对 word、Excel、宏、压缩文件、EXE 文件和 PDF 文件的加密技巧同时还有本书的附录增加了本书的附加价值。

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；同时可作为软件开发从业人员及编程爱好者的速查手册。

图书在版编目（CIP）数据

加密解密全攻略 / 武新华等编著. —3 版. —北京：中国铁道出版社，2010.9

ISBN 978-7-113-11532-6

Ⅰ. ①加… Ⅱ. ①武… Ⅲ. ①电子计算机－密码术② 计算机网络－安全技术 Ⅳ. ①TP309.7②TP393.08

中国版本图书馆 CIP 数据核字（2010）第 117417 号

书　　名：加密解密全攻略（第 3 版）

作　　者：武新华　余建国　王英英　王振武　等编著

策划编辑：严晓舟　荆　波

责任编辑：荆　波　　**读者服务热线：**400-668-0820

编辑助理：何　佳　　**封面制作：**白　雪

封面设计：付　巍　　**责任印制：**李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）

印　　刷：三河市华业印装厂

版　　次：2006 年 1 月第 1 版　2008 年 5 月第 2 版　2010 年 9 月第 3 版　2010 年 9 月第 3 次印刷

开　　本：787mm×1092mm　1/16　**印张：**26　**字数：**608 千

印　　数：4 000 册

书　　号：ISBN　978-7-113-11532-6

定　　价：49.80 元（附赠光盘）

前　言　Foreword

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，但从另一角度来讲，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。加密可以保证数据的安全，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。

为什么写这本书

为了使读者能够在学习和掌握加密、解密新技术时，做到“知其然，知其所以然”，本书在写作中还加入了一定篇幅的理论讲解，尽量做到“授人以渔而非授人以鱼”，使读者在全面掌握这些加密、解密知识时，能够举一反三，更好地保护自己的数据，尽最大可能地为数据打造出坚实的“铜墙铁壁”。

本书注重对日常加密、解密技巧的剖析，使读者在遇到疑难时，能够尽可能地心中有数，进而制定出相应措施。

本书特色

情景教学、案例驱动与任务进阶为本书的鲜明特色。通过本书介绍的一个个实践任务，读者可以轻松掌握各知识要点，在不知不觉中快速提升实战技能。

- 通俗易学，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，以及有志于从事数据安全或加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，并对实战过程中常见问题作必要的说明与解答，让读者用更少的时间更快掌握加密、解密技术。
- 内容涉及当前最新技术、热点技术和常用相关工具软件，有关加密、解密的编程技术、方法与思路，并通过综合实例介绍技术的运用手段，使读者能够举一反三。
- 赠送超值多媒体配套教学光盘。读者在阅读时可参考光盘中的视频教程，轻松、快速地掌握书中内容。

读者定位

作为一本面向广大软件加密、解密技术爱好者的速查手册，本书适合于如下读者使用：

- 电脑爱好者；
- 具备一定加密、解密基础知识和工具使用基础的读者；
- 网络管理人员；
- 热衷研究软件加密、解密者；
- 大中专院校相关专业学生。

本书结构安排与内容简介

本书以配图、图释、标注、指引线框等丰富的图解手段，介绍了加密、解密的一般方法、步骤。可使读者对常用软件加密、解密技术有一个全面的认识。

第 1 篇　加密与解密入门篇

第 1 章　加密与解密技术基础。主要介绍什么是密码学、文件读写、动态链接库、包的设计、软件的试用期等加密、解密知识，帮助读者对加密、解密加深理解。

第 2 章　代码分析与常用工具简介。本章从代码分析技术、静动态分析技术及其工具、注册表分析技术及其工具三方面阐述，帮助读者了解代码分析的用途，常用分析工具的基本操作等相关知识。

第 2 篇　典型工具篇

第 3 章　静态反汇编工具。本章主要介绍用户经常使用的一些反汇编工具及这些工具的使用方法，还介绍了反汇编后代码各项内容的含义，如什么是关键字 call、什么是关键跳转以及如何使用工具对源代码进行修改等内容。

第 4 章　动态跟踪分析工具。本章主要介绍目前常用的动态跟踪分析工具的使用方法及其与破解软件相关的操作功能，可以使用户对被破解软件进行动态跟踪和分析，进而提高解密者破解软件的效率。

第 5 章　必备的辅助工具。本章主要介绍在加密、解密过程中所用到的一些辅助工具及其使用技巧，可使用户在掌握这些工具使用技巧的同时，实现对文件的分析和修改编辑。

第 3 篇　关键技术篇

第 6 章　加壳与脱壳技术。本章主要介绍有关加壳、脱壳、重建输入表等相关基础知识以及其使用技术，可使用户掌握一些常见加壳、脱壳软件的使用方法，进而实现对常见软件的壳进行脱壳操作。

第 7 章　补丁技术。本章介绍了程序补丁文件的组成部分和分类，制作补丁工具的使用、各种补丁技术的应用、常用 SMC 技术，以及注册机制作工具 CrackCode 的具体使用方法等。

第 4 篇　软件保护篇

第 8 章　常用加密软件工具的使用。本章介绍了几种常用的多媒体加密软件和多功能加密工具的具体使用方法，如 Privage Pix、CryptaPix、WinFiles 等，熟练掌握这些加密软件，有助于对需要加密的文件进行加密操作。

第 9 章　网络验证加密软件的使用。本章主要介绍网络验证技术的各种具体应用，例如 Web 服务器验证加密技术、本地服务器验证加密技术、在线升级验证加密技术等。

第 10 章　注册认证和注册机。本章主要介绍各种注册认证机制和使用这些注册认证机制的注册机的制作过程，以方便用户注册和提高软件的保护强度。

第 11 章　不同软件的保护措施。本章主要介绍不同软件的保护措施，主要包括如何对抗不同破解软件的手段、如何制作不同程序包程序的保护措施以及一些不同软件的保护措施和邮件加密软件 PGP 等的相关内容。

第 5 篇　加密与解密实战篇

第 12 章　光盘和系统加密与解密技术。本章主要介绍了光盘和计算机系统两个方面的加密、解密技术，用户可丰富自己的加密、解密经验，对光盘和计算机系统中的一些重要资料进行加密，以确保光盘和计算机系统的安全。

第 13 章　加密与解密实用技术突破。本章主要介绍各种比较实用的加密、解密技术，例如文件夹加密与解密、网页信息的加密、解密、网吧限制与防范等内容，帮助读者成功将这些技术应用于日常生活中。

附录 A　常用文件、软件加密技术。本章主要介绍一些常用文件、软件的加密、解密方法。如 Microsoft Office 系列、压缩包、PDF 文件、电子邮件、数据库、EXE 文件等，熟练常握这些常用文件、软件后加密、解密技术，保证信息不被窃取。

结束语

本书由众多经验丰富的高校教师编写，其中大多长期从事数据安全管理工作。参与本书编写的老师有：刘双红负责第 1、2 章，王英英负责第 3 章，王振武负责第 4、5 章，杨平负责第 6 章，余建国负责第 7 章，张晓新负责第 8 章，李防负责第 9 章，李伟负责第 10 章，陈艳艳负责第 11 章，安向东负责第 12、13 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，书中疏漏之处在所难免，编者心存谨敬，随时恭候您提出的宝贵意见。

编者

2010 年 5 月

目　录　Contents

第 1 篇　加密与解密入门篇

第 1 章　加密与解密技术基础

第 2 章　代码分析与常用工具简介

第2篇 典型工具篇

第3章 静态反汇编工具

第3篇 关键技术篇

第6章 加壳与脱壳技术

第7章 补丁技术

第 4 篇　软件保护篇

第 8 章　常用加密软件工具的使用

第 9 章　网络验证加密软件的使用

第 10 章 注册认证和注册机

第 11 章 不同软件的保护措施

第 5 篇　加密与解密实战篇

第 12 章　光盘和系统加密与解密技术

第 13 章　加密与解密实用技术突破

第 1 篇　加密与解密入门篇

本篇作为全书的开局篇，主要向读者阐述：加密、解密技术的基本原理与应用，帮助读者建立起相关的知识轮廓；同时会针对应用讲解代码分析技术和常用工具，引领读者顺利跨入加密、解密技术的门槛。

本篇包含：

第 1 章　加密与解密技术基础

重点提示：

- 初识加密、解密技术
- 文件读/写与动态链接库
- BPL 组件设计
- 软件的试用期

本章精粹：

随着计算机和互联网的普及与发展，越来越多的人习惯于把自己的隐私数据保存在个人计算机中。隐私数据的涵盖面很广，如私人（商业）电子信函、各类金融系统的账号和密码、私人照片、商业合同等，只要是能够带来经济利益的私密数据，都有可能会成为窃取的对象。于是网络安全防护专家想到了对隐私数据进行加密的措施，但是有些时候基于某些特殊需要或者网络犯罪分子为了窃取机密信息，会设法对密码进行解密。

本章主要介绍加密、解密技术知识，包括什么是密码学、文件读/写、动态链接库、包的设计、软件的试用期等加密、解密知识，使读者对加密、解密有一个新层次的理解。

1.1　初识加密与解密技术

计算机加密技术是为了网络安全需要而产生的，它为计算机进行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、合同文本的签署等。

1.1.1　什么是密码学

密码学是一门研究编制密码和破译密码的技术科学。其中，研究密码变化的客观规律，并应用于编制密码以保守通信秘密的，称为编码学；而应用于破译密码以获取通信情报的，称为破译学，其总称为密码学。密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照密码学的这些法则，把明文变为密文，称为加密变换；相反，把密文变为明文，称为脱密变换。

进行明文和密文之间变换的法则，称为密码的体制，而指示这种变换的参数，称为密钥，它们是密码编制的重要组成部分。密码体制的基本类型可以分为如下 4 种：

- 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变成密文。