

谢柏青 王攻本 主编

个人电脑实用丛书

个人电脑信息安全 ——病毒防范与 文件保密

王新民 朱连章 编著



309
XM/1

科学普及出版社

7p009
WXM/1

个人电脑实用丛书

个人电脑的信息安全

——病毒防范与文件保密

谢柏青 王攻本 主编

王新民 朱连章 编著



科学普及出版社

• 北京 •

0030614

(京) 新登字 026 号

图书在版编目 (CIP) 数据

个人电脑的信息安全: 病毒防范与文件保密/王新民编著。

—北京: 科学普及出版社, 1994. 9

(个人电脑实用丛书/谢柏青, 王攻本主编)

ISBN 7-110-03874-2

I. 个…

II. 王…

III. ①计算机管理—安全技术②微型计算机—计算机病毒—防治
③密码术

IV. TP360. 9

JS384/05

科学普及出版社出版

北京海淀区白石桥路 32 号 邮政编码: 100081

新华书店北京发行所发行 各地新华书店经售

北京孙中印刷厂印刷

※

开本: 850×1168 毫米 1/32 印张: 5.125 插页: 1 字数: 120 千字

1994 年 11 月第 1 版 1994 年 11 月第 1 次印刷

印数: 1—10000 册 定价: 6.00 元

序

80年代,我国出现了第一次计算机普及高潮,其主要特点是,在高等学校非计算机专业设置了相应的必修课,有的中、小学也开设了计算机课程;各行各业开始重视计算机应用,并把计算机技术与某些专业领域的工作结合起来,形成了一种新的局面。计算机的应用和普及又推动了计算机产业的发展,集成度越来越高,工作环境越来越好。进入90年代,特别是1992年以来,我国出现了第二次计算机普及的高潮。这次普及是全方位、多层次的普及,是向一切领域,向各层次人群的普及。目前,计算机教育的对象不仅是大、中、小学生,还有广大知识界及各行各业不同文化程度的人。计算机的普及与广泛应用,将会改变人们传统的工作方式,使我国各行各业的工作面貌发生很大的变化。

计算机是高科技产品,学习使用计算机不是轻而易举的,但也不是高深莫测的。若结合工作需要,循序渐进,持之以恒,就一定能够收到好的效果。

由谢柏青、王攻本主编的“个人电脑实用丛书”,首批选择了计算机应用的十二个方面,从使用的角度,总结了这些方面使用个人电脑的经验,帮助读者较快地学会使用电脑,并且,对于已经有着使用电脑经验的读者而言,也能从中受益,提高计算机应用水平。

相信这套全书对广大知识界及各行各业学习、使用计算机的人士会有帮助,并对计算机应用作出一定贡献。

杨笑清

1994年8月18日

内 容 提 要

本书详细地介绍了有关计算机病毒及防治的知识,软件加密/解密的技术,以及数据恢复等方法。第一章介绍计算机的基本原理;第二~第七章介绍计算机病毒的危害、计算机病毒的发作及传播原理、计算机常见病毒的防治及消除方法,以及对用户的忠告,第八~第十章介绍计算机与现代密码技术,加密、解密技术及磁盘加密、解密实例。本书简练、明确、实用。

本书适宜广大电脑用户使用。亦可作电脑培训班的教材。

序 言

随着微型计算机在我国的逐渐普及,个人电脑已经开始进入家庭,如何选择个人电脑和如何使用个人电脑成为许多家庭和个人需要考虑的问题。为了适应计算机应用的这一新的发展形势,现出版一套《个人电脑实用丛书》。

现在在微型计算机及其应用方面已经正式出版和非正式出版了不少图书和资料,但这类书多数是针对某种机器或某个软件的说明,或是大学教材。其中相当一部分专业性强,非专业人员使用起来相当困难,有的书涉及面广,书的价钱昂贵,用户只能使用其中一小部分内容。为此我们出版的《个人电脑实用丛书》从使用的角度出发,力图深入浅出,能满足具有中等文化程度各种层次的人选择和使用电脑时参考。

《个人电脑实用丛书》的特点是突出实用性、强调通俗性、加强趣味性、完整配套形成系列,具体说明如下:

1. 突出实用性。以个人电脑为中心,选择软、硬件知识中实用性强的部分,按实用的方面组织该系列丛书。每一本书结合计算机一个或两个应用方面,讲解这方面的计算机基本知识和概念及这方面使用个人电脑的一些实例、实际经验和技巧,使初学者能较快进入角色,学会使用个人电脑,使原来会使用的人也能从中受益。

2. 强调通俗性。本套丛书主要读者对象是各行各业的个人电脑使用者,特别是刚刚开始使用电脑的科学家、教授、工程师、作家、党政干部、工人、个体工作者等,也可以作为广大中学生、中专生、大专生的课外读物。使用这套丛书可以使初学者较快入门,系统地学习这套丛书,可以初步掌握个人电脑的主要应用方面,为进

一步深入学习和应用电脑打下基础。

为使具有中等文化程度的人都能顺利地阅读这套丛书,书中不过多地使用难懂的名词术语,而是深入浅出地讲解个人电脑的基本知识,结合应用的方面重点教会读者使用个人电脑,在使用中培养使用计算机的能力和提高了计算机知识水平。

3. 加强趣味性。个人电脑的普及使用会给家庭带来新的快乐。电脑的使用,不仅有很强的知识性,也有很强的趣味性。本套丛书注意在取材、选例等方面加强趣味性,力求将知识寓于娱乐之中,使读者感到使用电脑的乐趣,并从中受益。

4. 完整配套,形成系列。选择了个人电脑应用的各个领域,每本书重点解决一个方面应用问题,力求讲清讲透,能使读者受益。选择的方面是各行各业的人在个人电脑使用中共同和经常遇到的问题,特别选择了家用电脑常用的各个方面。各本书之间的内容尽力避免重复,但在书的体例上又有统一的格式和风格,具有自己的特色,形成一个系列。每本书重点说明计算机应用的一个方面,可以单独使用,也可以整套使用。也可以选作培训班和大专计算机应用专业的教材。

《丛书》不同于一般的计算机手册,又不同于大学本科计算机专业的教材,《丛书》的编写目的是帮助个人电脑的使用者快速入门或入门后快速提高。内容编排格式清新,不落俗套。书中图文并茂,由浅入深,通俗易懂,使读者能按书中的方法去做,学会使用个人电脑,在使用电脑的过程中受益,提高计算机应用的水平。

本套《丛书》的作者都是具有多年计算机教学经验,熟练使用个人电脑的教授、副教授、讲师、工程师等。作者在讲述的应用方面已经积累了丰富的经验,书中讲到的问题和各种方法都是经过实验的,读者可以借鉴,为方便读者,有的书将给读者提供软盘,软盘中附上有关的软件和书中的实用程序。读者使用这些程序可以很快进入角色。

《个人电脑实用丛书》是由谢柏青和王攻本主编,第一批共 12 本:

1. 个人电脑必备手册(谢柏青编著)
2. 一种简单易学的汉字输入方法(朱守涛编著) 提供软盘:
智能 ABC 汉字输入法教学版
3. 电脑写作入门(许寿椿编著)
4. 个人电脑入门新途径——WINDOWS 使用指南(王新民编著)
5. C 程序设计及其应用(徐继扬编著) 提供软盘
6. 个人电脑数据库应用(曾秀玲编著) 提供软盘
7. 个人电脑与电算化财务应用(王慧苓等编著) 提供软盘
8. 个人电脑的接口技术与外围设备(王克义编著)
9. 个人电脑的维护与维修(李平、邓小全编著)
10. 个人电脑的信息安全——病毒防范与文件保密(王新民、朱连章编著) 提供软盘
11. 局部网络的安装与使用(何莉、汪洋编著)
12. 个人电脑文字表格处理软件(陈维兴编著)

欢迎计算机专家、学者,以及各阶层读者对本丛书不足之处,提出改进意见和批评。

谢柏青 王攻本

1994 年 6 月

目 录

引言.....	(1)
第一章 个人电脑工作原理.....	(2)
第一节 二进制数与十六进制数.....	(2)
一、二进制数	(2)
二、十六进制数	(4)
三、二进制数与十六进制数的转换方法.....	(5)
第二节 个人电脑的基本组成.....	(6)
一、中央处理机	(7)
二、内存存储器	(9)
三、外存储器	(10)
四、中断系统及典型中断.....	(16)
第三节 个人电脑的工作原理	(18)
第四节 操作系统 DOS 的基础知识.....	(19)
一、DOS 的工作原理	(19)
二、COM 和 EXE 文件加载	(22)
第二章 计算机病毒的历史及危害	(27)
第一节 计算机病毒的历史及发展	(28)
第二节 计算机病毒产生的原因	(29)
一、娱乐与竞争	(29)
二、一种不合适的软件保护方法	(30)
三、系统的弱点	(30)
第三节 计算机病毒的定义及分类	(31)
一、计算机病毒的定义	(31)
二、计算机病毒的基本分类	(32)
第三章 计算机病毒发作及传播的基本原理	(35)
第一节 计算机病毒的组成	(35)
一、引导部分	(36)

二、传播部分	(36)
三、破坏部分	(37)
第二节 计算机病毒传播与发作的机理	(37)
第三节 计算机病毒的工作流程	(39)
第四节 复杂的计算机病毒工作过程	(41)
第四章 计算机病毒防治的一般对策	(43)
第一节 计算机病毒侵入个人电脑的几种途径	(43)
一、不要非法拷贝软件	(43)
二、警惕隐藏很深的病毒的攻击	(44)
三、警惕家庭内部人员的病毒传染行为	(44)
第二节 计算机病毒的简易诊断	(45)
一、个人电脑的工作效率是否降低	(46)
二、文件的大小是否增加	(46)
三、磁盘上的坏簇是否增加	(47)
四、屏幕上是否出现与程序无关的信息或画面	(48)
五、是否经常出现驱动器无故灯亮现象	(48)
第三节 自我防范措施	(49)
一、防止“病从口入”	(49)
二、作好备份	(49)
三、自我诊断	(50)
第四节 不必大惊小怪	(51)
第五章 常用反病毒软件及操作	(52)
第一节 程序调试工具 DEBUG	(52)
一、DEBUG 程序的启动	(53)
二、DEBUG 命令的一般形式	(53)
三、DEBUG 中的地址形式	(54)
四、反病毒工作中常用的 DEBUG 命令	(54)
五、DEBUG 应用举例	(57)
第二节 PCTOOLS	(58)
一、PCTOOLS 的基本功能	(59)

二、PCTOOLS 的安装	(61)
三、PCTOOLS 的使用	(62)
第三节 磁盘维护程序软件包 NU	(63)
一、NU 的安装	(63)
二、NU 可以提供的基本服务	(64)
第四节 病毒检测软件 SCAN	(66)
第五节 病毒检测软件 CPAV	(66)
一、检测、消除及免疫功能	(67)
二、在线防止病毒扩散	(67)
三、引导扇区和分区表警戒	(68)
第六节 消除病毒软件 Kill	(70)
第六章 常见病毒及消除方法	(70)
第一节 引导扇区型病毒	(70)
一、小球病毒	(70)
二、大麻病毒	(71)
三、巴基斯坦智囊病毒	(72)
四、火炬病毒	(72)
第二节 可执行文件型病毒	(74)
一、黑色星期五	(74)
二、杨基病毒	(75)
三、隐藏光标病毒	(76)
四、DIR-2 病毒	(77)
第三节 交叉型病毒	(78)
一、Liberty 病毒	(78)
二、新世界病毒	(80)
第四节 CMOS 病毒	(82)
第七章 对用户的忠告	(87)
第一节 洁身自好	(87)
第二节 常备无患	(87)

一、制作系统备份	(88)
二、制作用户备份	(89)
第三节 强身健体	(89)
第四节 较全面地掌握检测病毒的手段	(90)
第五节 计算机病毒防范工具	(91)
一、消毒软件	(91)
二、防毒卡	(91)
第八章 计算机与现代密码技术	(93)
第一节 加密与解密技术概述	(93)
一、个人电脑与计算机密码学	(93)
二、个人电脑信息的分类及保护方法	(94)
第二节 加密系统的基本构成	(96)
第三节 密钥的保护	(98)
一、多重加密法	(98)
二、分散保管法	(98)
第四节 加密系统的评价	(99)
第九章 个人电脑信息的加密	(100)
第一节 文档类文件的加密	(100)
一、文档类文件的结构	(100)
二、文档类文件的加密方法	(101)
第二节 软件产品的加密	(102)
一、磁盘加密原理	(102)
二、磁盘加密的方法	(102)
第十章 磁盘文件加密解密实例	(108)
第一节 激光加密软件的原理及其破译方法	(108)
一、激光加密软件的加密原理	(108)
二、激光加密软件的解密	(111)
第二节 通用加密软件的设计	(120)
一、反拷贝措施	(120)

二、软件加密的过程及解密模块的建立	(124)
三、可安装的加密软件设计	(125)
第三节 一些实用的加密解密技巧	(126)
一、DEBUG 使用技巧两种	(126)
二、对软件狗的加密软件之跟踪	(128)
三、BASIC 程序的解密	(128)
四、WPS 文件密码的恢复	(129)
附录一 ASCII 码表	
附录二 病毒列表	(131)
参考文献	(146)

引 言

目前，个人电脑迅速普及。已逐渐走入普通人家。借助于个人电脑的强大功能，人们可以非常方便地完成各种各样的工作，如：写作、计算、进行文稿的编排、玩各种各样的电子游戏等等。所有的这一切，使人类的生活更加绚丽多彩。

但是，随着个人电脑应用日趋普及，许多新的问题也就应运而生，其中，使个人电脑用户深感头疼的问题可能就是计算机病毒的传播。为减少计算机病毒对个人电脑用户的损失，人们迫切需要知道什么是计算机病毒、计算机病毒是如何传播的、以及如何防范病毒的侵袭；其次，如何保护个人重要数据的安全、如何防止别人非法盗用自己设计的软件 and 个人的数据等等、也是很多人所关心的。再次，在计算机操作中，几乎每个用户都有因操作不慎而丢失数据的痛苦经历，即使高级计算机人员亦不例外。因此，在使用个人电脑时，还需具有在发生误操作时尽可能恢复原有信息知识。本书正是介绍解决这些问题的方法的一本工具书。

为帮助个人电脑使用者更好地解决上述问题，在本书中详细地介绍了有关计算机病毒及防治的知识，软件加密/解密的技术以及数据恢复等方法。由于这些内容均涉及到计算机的基本原理，因此，在第一章中，首先介绍计算机的基本原理，对大多数个人电脑用户而言，这部分内容可能专业味太浓。如果读者阅读该章感到困难，可暂时越过这一章，直接阅读自己所希望的章节。但是，作者极力建议读者应尽可能地掌握这部分内容，只有在此基础上，读者才有可能全面理解本书所介绍的内容，在工作中有效地应用有关的方法，达到预期的目的。

第一章 个人电脑工作原理

如果说个人电脑的原理比电视机简单。也许有许多人会认为这是在说胡话，但事实确实如此，我们知道电视机中各部分需要不同的电压、电流，要想使画面清晰，声音圆润，需要进行大量繁琐的调整。而计算机却不然，在计算机中只有两种电压，即或有电压或无电压。因此，计算机工作时将省去大量的调整及相关设计。因而，计算机电路设计要比电视机设计简单。也许有读者会问，为什么只要求两种电压？事实上，“有电压”或“无电压”表示着两种根本不同的状态，在计算机中，这两个状态分别表示数字“0”和“1”，虽然这两个状态非常简单，但是，这两个状态的组合、变换却使计算机进入了精彩纷呈的新世界。

第一节 二进制数与十六进制数

一、二进制数

可以说几乎每个人对十进制数都非常熟悉，我们可以很轻松地计数：0、1、2、3、4、5、6、7、8、9，如果数很大可以在高位加一后再从头数起，如此反复，直到所需要的任何数。在这种计数方法中，数以十为基本计数单位，数字每增加十个，即在高位进一，即有“逢十进一”的规则，而且有：

$$10^0 = 1$$

$$10^1 = 10$$

$$10^2 = 100$$

$$10^3=1000$$

.....

等方便的计算方法。

虽然，我们对十进制数已经非常熟悉，但是，这并不意味着十进制数是一种简单的计数方法。我们人类之所以喜欢十进制，恐怕主要是因为人类有十个手指，或十个脚趾这些简单的十进制计数工具，或者说一种强大的习惯势力。但是对于没有上述简单计数工具の場合，十进制数就相当不好用，尤其是不便于用机器自动计数。因为在物理电路中，很难找出可以同时表示十个数字的稳定的状态。但是在自然界中，具有两个稳定状态的对象却是俯首皆是。譬如，灯泡的亮与灭，门的开与关，电压的有或无等等，皆是这样的例子。那么，只用两个状态能否完成十个状态所具有的功能呢？答案是肯定的。事实上，利用两个状态同样可以完成计数工作，并且毫不逊色于十个状态的计数方法。通常，用两个状态计数时，可用数字“0”和“1”分别表示这两个状态，数字“0”和“1”就构成了二进制计数系统的基本组成部分，其中“0”表示无，“1”表示有一个。如果有两个，用0, 1怎样表示呢？和十进制中用完十个数后“逢十进一”规则相似，在二进制数中，有“逢二进一”的规则。当处理数据多于可用的符号时，即用“10”表示有二个物体，用“11”，“100”，“101”……等分别表示有三、四、五个……物体。一般的，为了不同进制数之间互相区别，在本书中引入一个表示进制类别的下标进行区分，如： $(2)_{10} = (10)_2$ ，表示十进制的2与二进制的10相等。类似的有：

$$(0)_{10} = (0)_2$$

$$(1)_{10} = (1)_2$$

$$(2)_{10} = (10)_2$$

$$(3)_{10} = (11)_2$$

$$(4)_{10} = (100)_2$$

$$(5)_{10} = (101)_2$$

$$(6)_{10} = (110)_2$$

$$(7)_{10} = (111)_2$$

$$(8)_{10} = (1000)_2$$

$$(9)_{10} = (1001)_2$$

.....

由此可以看出，从表达功能上讲，十进制数与二进制数之间没有区别。但是，对于二进制而言，人们非常容易用物理电路进行模拟，从而为用机器表示数据提供了可能。不仅如此，使用二进制数，数据处理的规则还非常简单。

对于二进制数加法，有如下几条规则：

$$0+0=0, 0+1=1, 1+1=10 \text{ (即“逢二进一”)。}$$

对于二进制数乘法，有如下几条规则：

$$0 \times 0 = 0, 0 \times 1 = 0, 1 \times 1 = 1$$

由此可以看出，利用二进制进行计数，不仅可以容易用物理状态进行模拟，而且其运算也可以很容易用电子线路实现，从而，为机器计算数据奠定了基础。

用二进制表示数据为计算机的实现提供了可能，但是它也有缺点，其中之一，就是人类不习惯使用二进制数。再就是当一个数较大且用二进制表示时，就要用很多位表示，如：对于十进制数 255，如果用二进制表示，则为 11111111，需要八位。如果数再大一些，需要的位数就更多，不便于人类阅读。为便于人类阅读，我们还需要一种既可以方便地向二进制转换，又便于人类阅读的数据表示方法。

二、十六进制数

我们知道，对于十进制数，由于存在 $2^{10}=1024$ ， $2^8=256$