

<<一级MS Office教程>>

图书基本信息

书名：<<一级MS Office教程>>

13位ISBN编号：9787564704421

10位ISBN编号：756470442X

出版时间：2010-2

出版时间：电子科技大学出版社

作者：乔保军 编

页数：224

字数：410000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 内容概要

本书是按照教育部考试中心制定的《全国计算机等级考试大纲》中针对一级MS Office的考试要求编写的。

本书的主要内容包括：计算机基础知识、中文操作系统Windows XP、文字处理软件Word 2003、电子表格软件Excel 2003、演示文稿制作软件PowerPoint 2003、计算机网络基础与简单应用等。

本书内容简练，通俗易懂，可供参加全国计算机等级考试(一级)的考生使用，也可以作为高等院校相应课程的参考书。

## 书籍目录

第1章 计算机基础知识 1.1 计算机的发展历程 1.1.1 计算机的发展阶段及趋势 1.1.2 计算机的特点  
1.1.3 计算机的应用 1.1.4 计算机的分类 1.1.5 计算机在我国的发展 1.2 计算机中常见的数制 1.2.1  
几种常见的进位计数制 1.2.2 不同数制之间的转化 1.3 计算机中的数据表示 1.3.1 数据的单位  
1.3.2 字符编码 1.4 计算机系统组成 1.4.1 计算机硬件系统 1.4.2 计算机软件系统 1.5 微型计算  
机的主要性能指标 1.6 多媒体技术 1.6.1 多媒体的概念 1.6.2 主要多媒体技术的介绍 1.6.3 多媒体  
技术应用领域 1.7 计算机病毒与防治 1.7.1 计算机病毒 1.7.2 计算机病毒的分类 1.7.3 计算机病  
毒的防范 第2章 中文操作系统Windows XP 2.1 操作系统简介 2.1.1 操作系统的分类 2.1.2 操作系  
统的功能 2.1.3 操作系统的特征 2.1.4 常见的操作系统 2.2 Windows XP的安装 2.3 Windows XP的一  
般操作 2.3.1 Windows XP的启动与退出 2.3.2 Windows XP的桌面 2.3.3 鼠标的操作 2.3.4 开始菜单  
2.3.5 任务栏 2.3.6 对话框 2.3.7 窗口 2.3.8 菜单 2.3.9 使用帮助 2.4 文件和文件夹的管理 2.4.1 文  
件和文件夹的基本概念 2.4.2 Windows XP的资源管理器 2.4.3 新建文件和文件夹 2.4.4 文件和文件  
夹的选定 2.4.5 文件和文件夹的移动 2.4.6 文件和文件夹的删除 2.4.7 文件和文件夹的重命名 2.4.8  
文件和文件夹的复制 2.4.9 文件和文件夹的查找 2.4.10 文件和文件夹属性的设置 2.5 Windows XP控  
制面板 2.5.1 外观和主题 2.5.2 日期和时间的设置 2.5.3 添加或删除程序 2.5.4 鼠标和键盘的设置  
2.5.5 打印机的设置 2.5.6 用户账户 2.6 常见附件 2.6.1 画图 .....第3章 文字处理软件Word  
2003第4章 电子表格软件Excel 2003第5章 演示文稿制作软件PowerPoint 2003第6章 计算机网络基础  
与简单应用附录1 全国计算机等级考试一级MS Office考试大纲(2007年版修订版)附录2 全国计算  
机等级考试一级MS Office考试样题

## 章节摘录

版权页：插图：1.7.2 计算机病毒的分类 按照计算机病毒存在的媒体进行分类，病毒可以划分为网络病毒、文件病毒和引导型病毒。

网络病毒通过计算机网络传播感染网络中的可执行文件，文件病毒感染计算机中的文件（如：COM，EXE，DOC等），引导型病毒感染启动扇区（Boot）和硬盘的系统引导扇区（MBR）。

还有这三种情况的混合型，例如：多型病毒（文件和引导型）感染文件和引导扇区两种目标，这样的病毒通常都具有复杂的算法，它们使用非常规的办法侵入系统，同时使用了加密和变形算法。

按照计算机病毒传染的方法进行分类，病毒可分为驻留型病毒和非驻留型病毒。

驻留型病毒感染计算机后，把自身的内存驻留部分放在内存（RAM）中，这一部分程序挂接系统调用并合并到操作系统中去，它处于激活状态，一直到关机或重新启动。

非驻留型病毒在得到机会激活时并不感染计算机内存，一些病毒在内存中留有小部分，但是并不通过这一部分进行传染，这类病毒也被划分为非驻留型病毒。

1.7.3 计算机病毒的防范 鉴于计算机病毒传播危害性大，计算机系统一旦感染上病毒，可能会使计算机系统瘫痪，从而可能造成灾难性的后果。

所以，各国一直对计算机病毒的防范给予高度重视，并且逐步采取了一系列科学管理方法和预防措施。通常采用如下安全管理方法和对策。

（1）对工作人员应该加强关于计算机病毒及其危害的教育使有关人员认识到，程序和数据的破坏或系统瘫痪，不仅给公司或厂方造成巨大的经济损失，而且还会严重地损害公司和厂方的社会形象和信誉。

（2）为了防范病毒的入侵，对于系统软件应予以写保护。

注意对需要的可执行程序和数据文件进行写保护。

（3）对于予以保护的文件，为了防止文件的任何可能的修改，只允许使用读操作，而且要经常检查这些文件是否被修改了。

（4）对于计算机系统中的程序，要定期进行比较测试和检查，以检测是否有病毒侵入。

（5）要谨慎使用公共软件，防止计算机病毒的传播和扩散。

（6）在使用口令（Password）时，要尽可能选择随机字符作为口令，让口令本身无意义，不要用名字生日等作为口令，以增加破译口令难度。

（7）加强使用软盘的管理，尽量不用软盘引导。

因为用软盘引导造成病毒感染的机会要多一些，而用硬盘引导，则较安全。

（8）要严禁将其他部门的程序带入本系统。

外来程序如确需要使用，必须经管理人员授权，并要经过严格检查和测试，在确信无病毒感染时，才允许在本系统中运行。

（9）不允许随便将本系统与外界系统接通，以防止外界系统的病毒乘机侵入。

（10）不允许将各种游戏软件装入计算机系统，因为游戏软件被病毒侵入的机会很多，带病毒可能性大，以防止计算机病毒乘机侵入。

（11）使用杀毒软件，病毒本质上是一种程序，故可以通过软件的方法来预防或清除病毒程序，这就是杀毒软件。

现今市面上流行的国际、国内的杀病毒软件很丰富，如：Scan、Clean、kill系列、KV200、KV300等。

#### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>