计算机软件加密实用技术

毛 明 编著

電子工業出版社

计算机软件加密实用技术

毛　明　编著

电子工业出版社

(京)新登字 055 号

内 容 提 要

本书详细讨论了 PC-DOS 系统支持下软件加密的有关技术。内容包括 DOS 系统的重要知识、磁盘空间的结构、磁盘控制器的工作原理及编程方法、软件加密的基本要求，还着重讨论了软件加密的三大技术，即软件加密防拷贝技术、防静态分析技术和防动态跟踪技术。最后还讨论了软件加密的辅助技术，并讨论了软件加密系统的设计方法以及软件加密的封闭性问题。

本书特别适合于从事微型计算机软件开发和应用的专业技术人员学习和参考，也可以作为大专院校计算机软件专业学生的学习参考书。

计算机软件加密实用技术

毛 明 编著

特约编辑 何小林

责任编辑 王昌铭

*

电子工业出版社出版(北京海淀区万寿路)

电子工业出版社发行 各地新华书店经销

电子工业出版社计算机排版室排版

山东电子工业印刷厂印刷

*

开本 787×1092 毫米 1/16 印张:13 字数:332 千字

1993 年 8 月第 1 版 1993 年 8 月第 1 次印刷

印数:15000 册 定价:8.70 元

ISBN7-5053-2030-0/TP・520

前　言

目前，随着微型计算机硬件技术的不断发展，相应地要求计算机软件产品的功能也要不断地增强和提高，以满足不断发展的计算机硬件的需要，从而使计算机硬件的潜力真正地发挥出来。但是，由于计算机软件的开发工作复杂，知识密集性高，所以研制周期长。而对于研制出来的软件一般是用软盘提供给用户，由于磁盘的复制操作非常容易和简单，至使许多用户未经允许进行了软件的非法复制和使用，严重损害了软件开发部门的经济利益和软件版权。为此，我国已于 1991 年颁布了《计算机软件保护条例》并于同年 10 月 1 日生效，以从法律上对软件版权实施保护。但是，法律的保护只能起到一定程度的作用，并不能完全杜绝软件产品的非法复制。为了阻止软件产品的非法复制，从技术上采取一定的防范措施可以与法律的保护起到相互补充的作用。所以，为了帮助广大计算机软件开发人员保护其软件版权和经济利益，作者将近年来在计算机软件加密和解密实践中摸索出的一些经验进行总结和整理，编写了此书奉献给大家，以供计算机同仁在进行软件加密保护时学习和参考。

本书各章节的内容安排如下：

第一章概括介绍了 DOS 系统的一些重要知识，这是进行软件加密的基础。由于软件加密中的许多关键技术都是在深入研究 DOS 内核机制的基础上而实施的，所以了解 DOS 系统的有关内容是非常必要的。

第二章详细进述了磁盘的组成结构以及磁盘控制器的工作原理和编程方法。由于软件是存储在磁盘上的文件，软件与磁盘是息息相关的。只有了解磁盘的组成结构以及磁盘控制器的工作原理，才能进一步地研究出强有力的软件防拷贝方法。所以，本章详细介绍了磁盘的组成结构、文件分配表和文件目录表、磁盘控制器的工作原理、直接存储器存取 DMA 的编程以及 ROM BIOS 中 INT 13H 的源程序。

本书第三章首先阐述了软件加密的三个基本要求：防拷贝技术、防静态分析技术和防动态跟踪技术，然后详细介绍了软件加密中的一个最基本的技术——防拷贝技术。目前，在软件加密中实施防拷贝的方法从大的方面来说可以分为两种，一种是采用硬件技术在磁盘上制作特殊标记，一种是采用软件的方法在磁盘上制作特殊标记。由于采用软件的方法制作特殊标记既方便又可靠，所以在这一章中我们着重介绍了用软件制作特殊标记的方法——特殊格式化方法。

第四章详细讨论了软件加密的防静态分析技术。防静态分析技术是软件加密技术中又一个重要方面，它主要是采用密码学的有关知识对软件正文进行加密变换。所以，在这一章中我们以密码学中的加密算法为理论指导，在讲述每一种加密算法的同时，都给出了用汇编语言程序实现的方案。通过这些程序既可以使读者理解有关的加密算法，又可以被读者直接所采用。

第五章详细讨论了软件加密的防动态跟踪技术。在软件加密技术中，防动态跟踪技术是一个更为重要的技术。它是软件加密技术中的一个高难度的技术，为了有效地保护软件，许多加密人员在防动态跟踪技术的程序设计上花费了大量的心血。因此，我们在这一章中通过大量的实例，对软件加密防跟踪技术中的种种有效的方法进行了阐述。

第六章是软件加密的一些辅助技术，它们一般是与防拷贝技术、防静态分析技术以及防动态跟踪技术结合起来使用，可使得被加密的软件得到更为有效地保护。

第七章讨论软件加密系统的设计方法和软件加密的封闭性问题。软件加密系统的设计是讨论如何将各种加密方法综合运用，编写出一个通用的加密软件，以便对需要加密的软件实施

加密保护操作。加密系统的封闭性问题，是讨论如何设计出一个比较完善的加密系统，尽可能地从各个方面有效地阻止解密者的解密操作，使软件加密的方法更加完善和可靠。

高级工程师何源对本书进行了认真的审阅，并提出了许多宝贵的意见。北京电子科技学院王贵和副教授在本书编写过程中，也给予了热情的指导和帮助，作者对两位良师深表谢意。

由于水平所限，经验不足，书中缺点错误在所难免，敬请读者批评指正。

毛　明

1992 年 10 月

目　录

第一章　DOS 系统的重要知识

PC-DOS 是 IBM PC 及其兼容机上广泛使用的磁盘操作系统，由于本书所讨论的软件加密技术就是针对 PC-DOS 支持下的软件而进行的，所以了解 PC-DOS 的组成结构以及有关的重要内容是软件加密的基础。总结目前大多数加密软件所采用的技术我们就可以看到，它们都是在充分研究 PC-DOS 及其支持下的一些工具软件后，采取了一系列的措施，或者是利用了工具软件的某些缺限，或者是挖掘了 PC-DOS 的一些鲜为人知的重要功能，进行了非常巧妙的程序设计，从而一方面有效地阻止了非法用户的拷贝、解密等操作，另一方面又保证了被加密软件的正常执行。所以，要想研究出一种比较有效的加密方法，深入研究 PC-DOS 的组成结构及其工作原理是非常必要的。

§1.1　DOS 的组成、启动及内存分配

§1.1.1　DOS 的基本组成

PC-DOS 简称为 DOS，是一个层次型、模块化结构的磁盘操作系统，如图 1-1 所示。

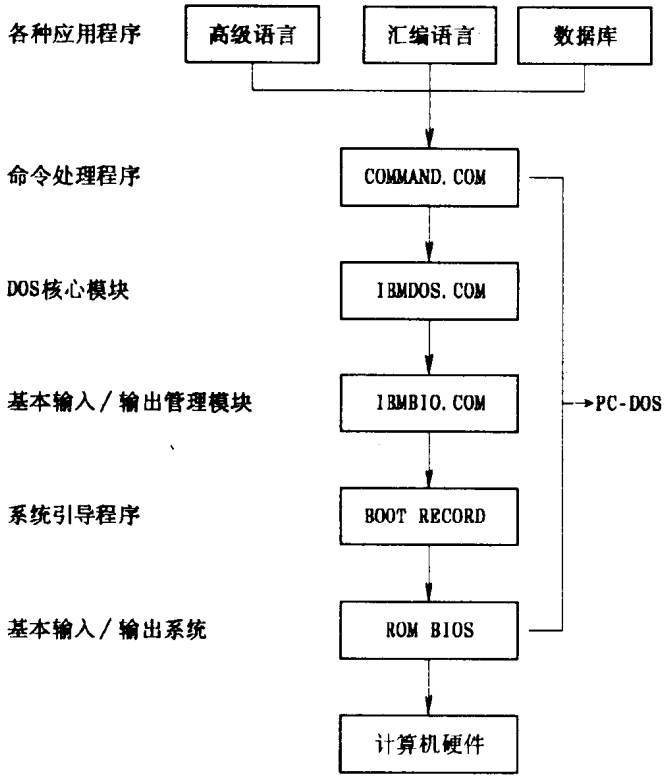

图 1-1　PC-DOS 组成模块及层次结构

它由如下五个模块组成：

1. ROM BIOS—基本输入/输出系统。它提供了对计算机输入/输出设备进行管理的程序，被固化在主机板上的 8K ROM 中，是计算机硬件与软件的最低层接口。

2. BOOT RECORD—引导记录。它驻留在系统盘的 0 面 0 道 1 扇区，在启动时它首先被自动调入内存，然后由它负责把 DOS 的其它程序调入内存。

3. IBMBIO. COM—基本输入/输出管理模块。它完成系统的初始化工作，并提供系统软件与 ROM BIOS 之间的接口。

4. IBMDOS. COM—DOS 的核心模块。主要提供了设备管理、内存管理、磁盘文件及目录管理的功能，这些功能可以通过所谓的系统功能调用 INT 21H 来使用，它是用户程序与计算机硬件之间的高层软件接口。

5. COMMAND. COM—命令处理程序。它是 DOS 调入内存的最后一个模块，其主要工作是负责接受和解释用户输入的命令，执行 DOS 的所有内、外部命令和批处理命令。该模块由三部分组成：常驻部分、初始化部分和暂驻部分。

(1)常驻部分装在内存的低部，在 IBMDOS. COM 及其缓冲区之上，用来处理磁盘输入/输出错误和下列类型的中断：

INT 22H　　程序终止中断

INT 23H　　Ctrl-C 和 Ctrl-Break 处理中断

INT 24H　　严重错误处理中断

INT 27H　　驻留结束中断

(2)初始化部分紧接常驻部分之后，它含有 AUTOEXEC. BAT 文件处理程序配置。在启动系统之后，这一部分最先得到控制权并执行 AUTOEXEC 批文件中的所有命令，然后初始化部分即被舍弃。

(3)暂驻部分装在内存的高端，它所在的内存可能被其它应用程序所占用。当应用程序终止时，COMMAND. COM 的常驻部分对暂驻模块求代码和，以确定暂驻部分是否被破坏，并在必要时由常驻模块重新装入。

§ 1. 1. 2　PC-DOS 的启动过程

图 1-2 描述了 DOS 启动的主要过程。

1. 在系统复位或加电时，计算机程序的指令指针自动从内存地址 0FFFF:0000H 处开始执行，该处含有一条无条件转移指令，使控制转移到系统的 ROM 板上，执行 ROM BIOS 中的系统自检和最初的初始化工作程序。系统自检和初始化过程的主要工作是：

(1)存储器测试。包括对 8K ROM BIOS 作代码和检查，对 32K ROM BASIC 作代码和检查，对主机板和扩展存储器板上的内存作 AA、55、FF、00 图像的测试，对显示器缓冲区作上述四种图像的测试等。

(2)对 8088 标志寄存器各标志位和通用寄存器、段寄存器等进行测试。

(3)对各个接口芯片进行测试，如：定时器芯片 8253、中断控制器 8259A、8237DMA 控制器、外围接口 8255A 等。

(4)测定设备配置，如内存容量、软盘驱动器个数、显示器类型、打印机以及 RS-232 通信口等，并作相应的初始化。

(5)填写 1FH 以前的中断向量表。

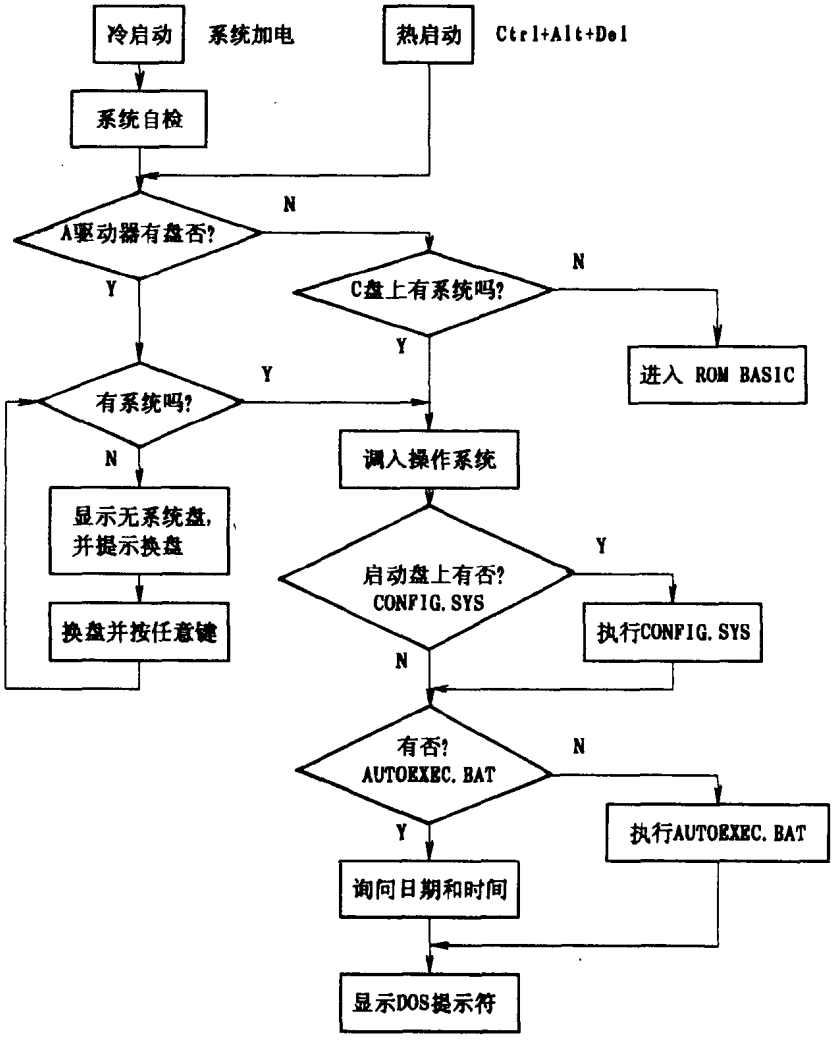

图 1-2　DOS 启动流程图

(6)检测是否有增加的 ROM 板,若有,则对其中的程序进行代码和检查并执行该程序。

如果上面的各项测试都正常,则把系统盘上存在 0 面 0 道 1 扇区的系统引导记录读入内存地址 0000:7C00H,并把控制权交给引导程序中的第一条指令。

2. 引导记录用于检查系统所规定的两个文件"IBMBIO. COM"和"IBMDOS. COM"是否按规定的位置存于启动盘中,若符合要求就把它们读入内存地址 0070:0000H,否则启动盘被认为不合法,启动失败。

3. IBMBIO. COM 与 IBMDOS. COM 被装入内存以后,引导记录的使命即完成,控制权交给 IBMBIO. COM,该程序完成初始化系统、定位 IBMDOS. COM 以及装入 COMMAND. COM 等工作。其主要过程是:

(1)建立新的磁盘参数表,修改 INT 1EH 向量地址指向该磁盘参数表。

(2)初始化异步通信口 RS-232 和打印机口。

(3)修改 01,03,04,和 1BH 中断入口。

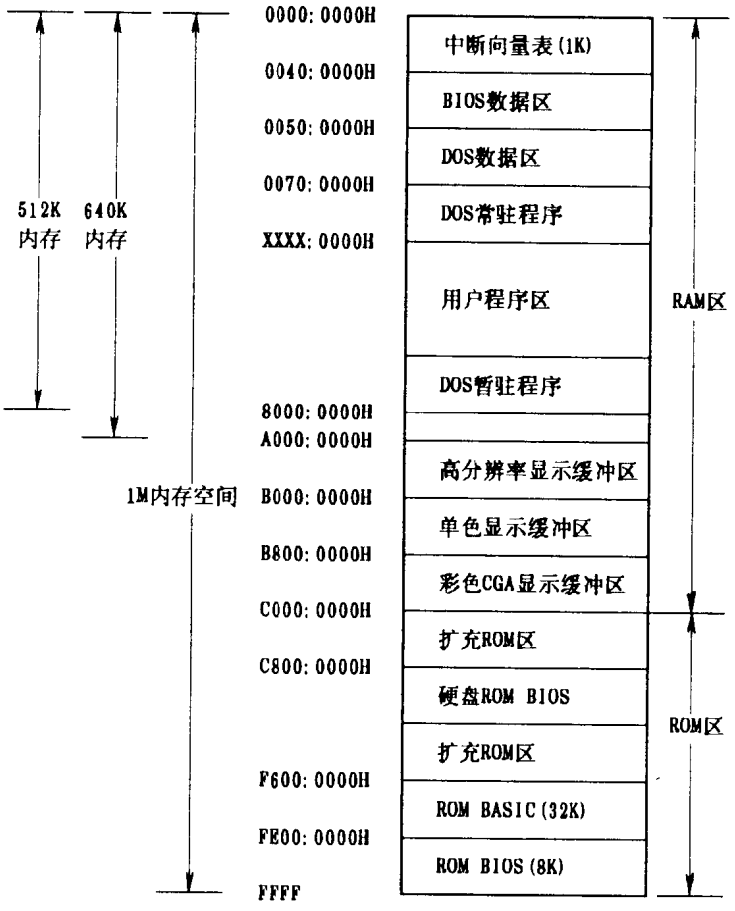

图 1-3　DOS 内存分配示意图

(4)调用 INT 11H 及 INT 12H 确定系统的硬件配置和内存 RAM 容量。

(5)将系统初始化程序移到内存高端并将 IBMDOS. COM 程序下移占据其位置。

(6)控制权交给 IBMDOS. COM。IBMDOS. COM 是 DOS 的核心部分,它在接受控制权以后,也进行一系列的初始化工作,这些工作包括:初始化 DOS 内部表和工作区、初始化 DOS 的中断向量 20H～27H、建立磁盘输入/输出参数表以及设置磁盘缓冲区和文件控制块等。完成这些工作以后,继续执行 IBMBIO. COM 的系统初始化程序。

(7)初始化程序检查系统盘上的系统配置程序 CONFIG. SYS,如果存在,则执行该程序,按配置命令建立 DOS 的运行环境,包括:设置磁盘缓冲区大小、能同时打开的句柄文件个数、加载可安装的设备驱动程序等。

(8)将命令处理程序 COMMAND. COM 程序装入内存,并把控制权交给该程序。至此 IBMBIO. COM 文件的使命即告完成。

4. 命令处理程序在接受控制以后,重新设置中断向量 22H、23H、24H 和 27H 入口地址,然后检查系统盘上是否存在 AUTOEXEC. BAT 文件。若系统盘上不存在该文件,则显示日期和时间等待用户输入,显示 DOS 提示符;若存在该文件,则程序转入暂驻区,由批处理程序对其进行解释和执行,执行完成后显示 DOS 提示符。至此,DOS 的整个启动过程全部结束,系统处

于命令接受状态。

§1.1.3 PC-DOS 的内存分配

DOS 启动后，内存的组织即分配如图 1-3 所示。从总体上来说，分为两大部分，一部分是 RAM 区，另一部分则是 ROM 区。而 RAM 区又分为系统程序、数据区和用户程序区两部分。由于 DOS 的版本不同，DOS 系统文件的长度就不同，从而驻留在内存中的系统程序占用的内存空间也就不同，这样用户程序区的段地址就是一个不确定的值。

§1.2 重要的系统参数及口地址

在 IBM PC 及其兼容机中，内存地址 0040:0000H 至 0050:00FFH 的区域被作为系统通信区，ROM BIOS、DOS 以及用户的应用程序可以直接访问这一区域的数据以获得有关系统状态的内部信息，某些数据甚至可以被修改，从而达到对机器运行状态有目的的控制。

§1.2.1 ROM BIOS 通信区的重要参数

从内存绝对地址 0040:0000H 至 0040:00ABH 开始存放着一些重要的数据，这些数据是由 ROM BIOS 程序在引导过程中装入的，它们是提供给 ROM BIOS 例行程序在进行设备操作时必备的重要数据。下面是对这些数据按照偏移地址、长度及含义三部分进行的说明。

偏移　类型　含义

0010H～0011H：字，表示系统的设备配置情况，其各位含义如图 1-4。

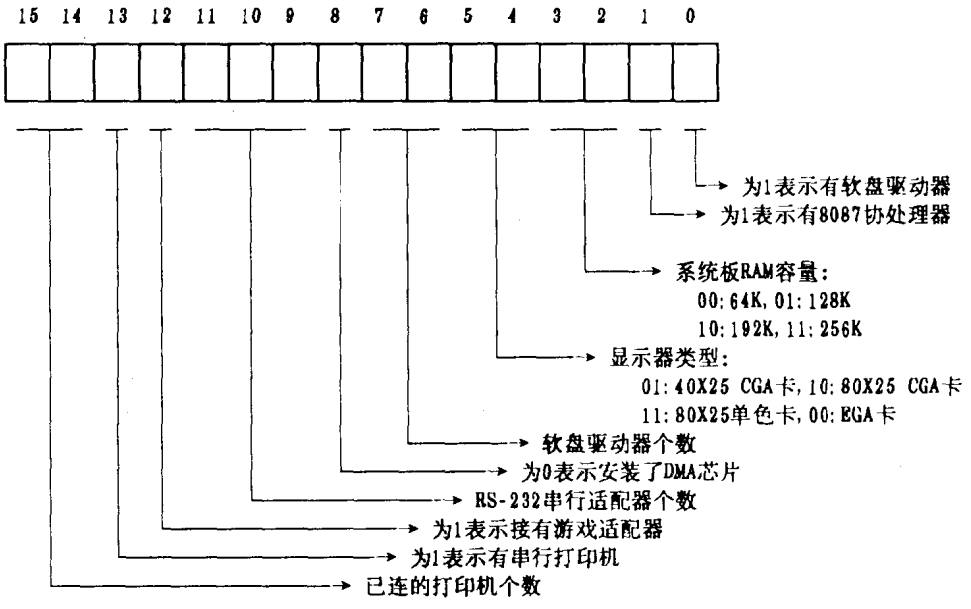

图 1-4　系统配置字节各位定义

0012H，字节，测试标志。为 1 表示测试键盘，为 0 表示操作键盘。

0013H～0014H：字，以 K 字节为单位表示的内存容量。

0015H～0016H：字，以 K 字节为单位表示的扩充内存容量。

0017H：字节，键盘第一个状态字，状态字如图 1-5 所示。

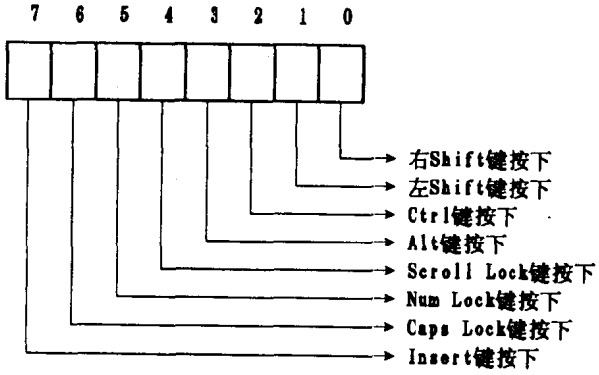

图 1-5　键盘特殊键状态的第一字节

0018H：字节，表示键盘特殊键状态的第二字节，状态字如图 1-6。

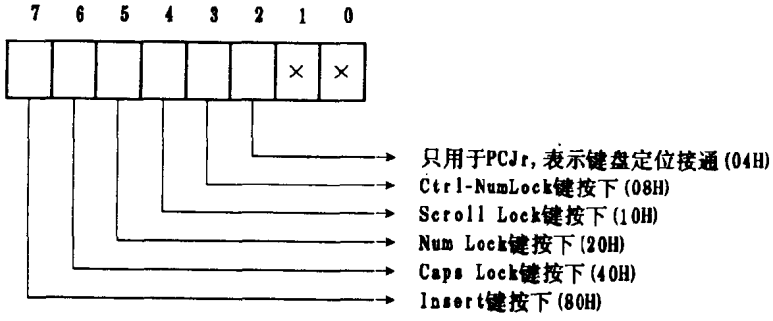

图 1-6　键盘特殊键状态的第二字节

0019H：字节，为存储由备用键盘键入的字符而保留。

001AH～001BH：字，键盘缓冲区首指针。

001CH～001DH：字，键盘缓冲区尾指针。

001EH～003DH：16 个字，键盘缓冲区，可以存放 16 个键盘输入的字符扫描码。

003EH：字节，表示磁盘驱动器的搜索状态，0～3 位对应于驱动器 0～3。如果这些位中有一位为 0，则在搜索到磁道之前，必须重新校准相应的驱动器，状态字如图 1-7 所示。

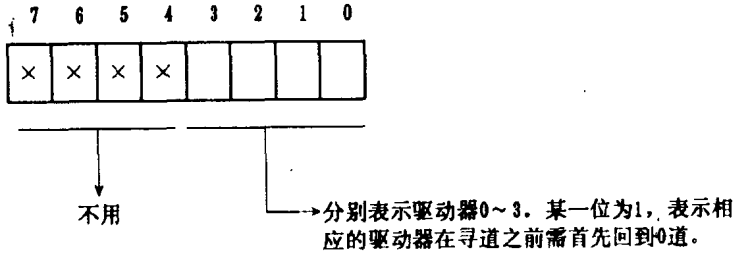

图 1-7　软盘寻道状态字节

003FH：字节，表示磁盘驱动器的马达状态，如同前一个字节，0～3 位对应驱动器 0～3，如果某一位被置 1，则相应驱动器的马达正在运转，状态字如图 1-8 所示。

0040H：字节，表明每次软盘操作后直至马达停转时的延时。

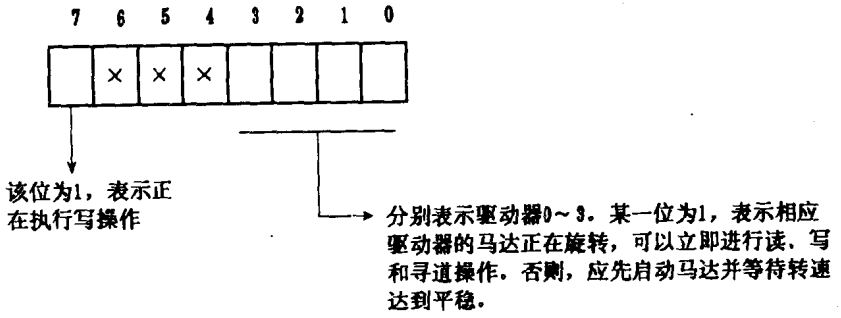

图 1-8　软盘驱动器状态字节

0041H：字节，表明出错原因：

01—磁盘控制器命令错

02—地址标记未找到

03—磁盘写保护

04—扇区未找到

08—DMA 错

09—DMA 企图超越 64K 段界

10—CRC 错

20—NEC 控制器错

40—寻道错

80—连接器未响应

0042H～0048H：7 字节，表示从 NEC 磁盘控制器返回的状态信息。

0049H：字节，表示当前显示器的工作方式。常见的显示方式有：

00—40×25 黑白字符方式

01—40×25 彩色字符方式

02—80×25 黑白字符方式

03—80×25 彩色字符方式

04—320×200 彩色图像方式

05—320×200 黑白图像方式

06—640×200 黑白图像方式

07—80×25 单色板

004AH～004BH：字，屏幕显示列数存放单元。

004CH～004DH：字，字符方式下，显示缓冲区每一页所占的内存字节数。

0065H：字节，存放 CRT 方式寄存器的当前值。

0066H：字节，屏幕颜色控制字。

006CH～006FH：双字，时钟计数值。PC/XT 及长城 0520-CH 机每隔 55 毫秒产生一次时间中断，该计数值即加 1。006CH 的一个字是计数低位，006EH 的一个字是计数的高位。当计数达到 24 小时后，该两个字的内容恢复为 0，并使 0070H 字单元内容加 1。

0070H：字节，时钟计数超过标志。当时钟计数器达到一天结束且复位时，此字节置 1，以表示新的一天开始。中断 1AH 功能调用 0 在读取这一天的时间后，将此字节复位。

0071H：字节，若按下 Break 键，则该字节的第 7 位为 1。
0072H～0073H：字，当系统热启动时，该字内容为 1234H。
0074H：字节，硬盘操作状态字节。
0075H：字节，硬盘驱动器个数。
0076H：字节，驱动器控制字节。
0077H：字节，硬盘访问起始地址口的偏移量。
0078H～007BH：4 个字节，打印机操作最长等待时间。
007CH～007FH：4 个字节，RS-232 口操作最长等待时间。
0080H～0081H：字，存放键盘缓冲区起始单元的偏移量。
0082H～0083H：字，存放键盘缓冲区结束单元的偏移量。
0084H～00ABH：用于 EGA 系统的附加显示器参数。
00ACH～00EFH：为 ROM BIOS 保留的通信区。

§ 1.2.2 用户程序通信区

从内存地址 0040:00F0H 至 0040:00FFH 为“用户程序内部通信区”，可被任何应用程序所使用。但由于任何应用程序都可以向这一区域读/写数据，所以这一区域的数据往往不可靠。

§ 1.2.3 DOS 通信区

从内存地址 0050:0000H 至 0050:00FFH 的区域为 DOS 保留区和 BASIC 保留区。其中有两个较为重要的字节参数，它们是 0050:0000H 和 0050:0004H。

0050:0000H：字节，用于记录屏幕打印操作的状态。

00H—屏幕打印不工作或已正确完成。

01H—正在进行屏幕打印。

FFH—在屏幕打印中发生错误。

0050:0004H：字节，当系统仅有一个磁盘驱动器，而要当作两个逻辑磁盘驱动器使用时，DOS 使用该字节，其数值指明物理驱动器何时作为逻辑驱动器 A 或 B 使用。

00H—驱动器作为 A 驱动器使用

01H—驱动器作为 B 驱动器使用

§ 1.2.4 机器标识

在内存地址 F000:FFFEH 处的一个字节标识了 IMB PC 系列微机的机器类型，见表 1-1。

需要说明的是，对于 IBM PC 兼容机，此位置的数值变化很大。例如对于 Compaq 286Portable 此字节的值为 0FCH，这是由于该机器完全模仿了 IBM PC/AT。

确定一台微机为非 IBM 机器的方法可以通过对 ROM 空间进行搜索，以查找是否有特定的字符串。例如，要确定一台机器是否为 Compaq 机，可以在 ROM 空间搜索是否有字符串“COMPAQ”，若有则为原装机，否则为兼容机。

表 1-1　IBM PC 系列微机的标识

数值	机器类型
0FFH	PC
0FEH	PC/XT
0FDH	PCjr
0FCH	PC/AT
0F9H	PC Convertible

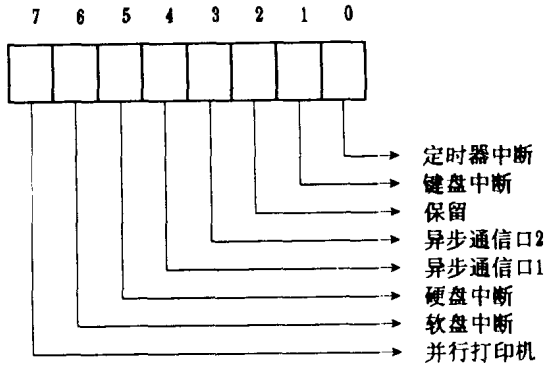

图 1-9　中断屏蔽寄存器位定义

§1.2.5　常用的口地址

下面是程序设计中经常使用的一些口地址，了解它们的功能和编程方法可以控制主机和外设的运行状态，它们在软件加密与解密工作中有着非常重要的作用。

1. 8259 中断控制寄存器口地址

(1) 20H 口：中断命令寄存器

在每次外部中断结束以后，要给该口发送中断结束信号，其指令为：

```
MOV   AL,20H
OUT   20H,AL
```

(2) 21H 口：中断屏蔽寄存器

8259 芯片可以接收 8 个外部可屏蔽中断。这些中断有两种状态，即允许和屏蔽状态。21H 口的 8 位分别对应于 8 个外部中断源，某位为 0，则允许接收相应的中断，否则不接收相应的中断。其对应关系如图 1-9。

2. 8253 定时器口地址

8253 共有三个独立的通道寄存器，其口地址分别为 40H、41H 和 42H，另外还有一个命令寄存器 43H。每个通道都可以单独编程，编程时先给命令寄存器送一个通道编程方式字，再给相应通道的口地址送计数值。命令寄存器的各位含义如图 1-10。

3. 8255 可编程外围接口

8255 是通用的 I/O 接口芯片，有很多配置方法。它可以支持许多设备和信号，包括键盘、扬声器、配置开关等。这个芯片包括三个口，分别叫做 PA 口、PB 口和 PC 口。三个口分配的口地址分别为 60H、61H 和 62H。另外，在这个芯片上还有一个命令寄存器，口地址为 63H，对于三个口的编程必须通过设置命令寄存器来进行。系统在启动时向 63H 口发送 99H，把该芯片设置成 PA 和 PC 为输入口，PB 为输出口。63H 口的各位含义如图 1-11。

PA 口有两种用途，一是当 PB 口的位 7＝0 时，PA 口返回的是键盘扫描码；二是当 PB 口的位 7＝1 时，PA 口返回系统板上的设备配置情况。

PA 口、PB 口和 PC 口的位定义如图 1-12、图 1-13 和图 1-14 所示。

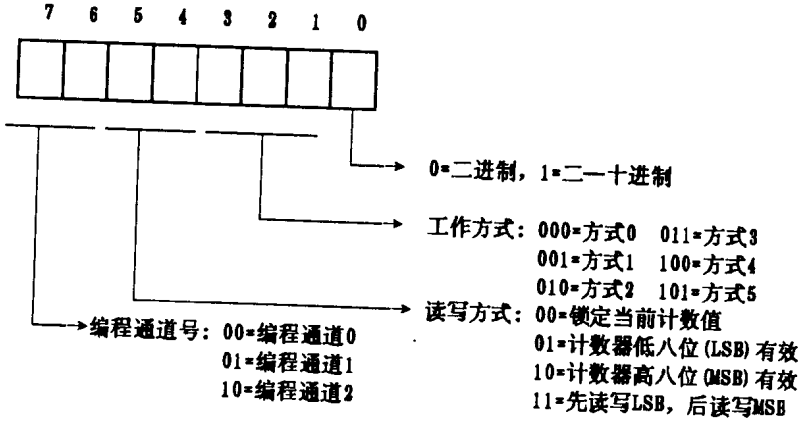

图 1-10　8253 命令寄存器位定义

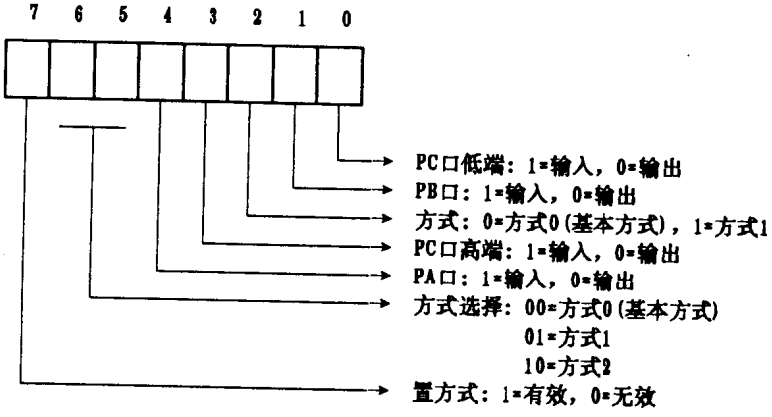

图 1-11　8255 命令寄存器(63H 口)位定义

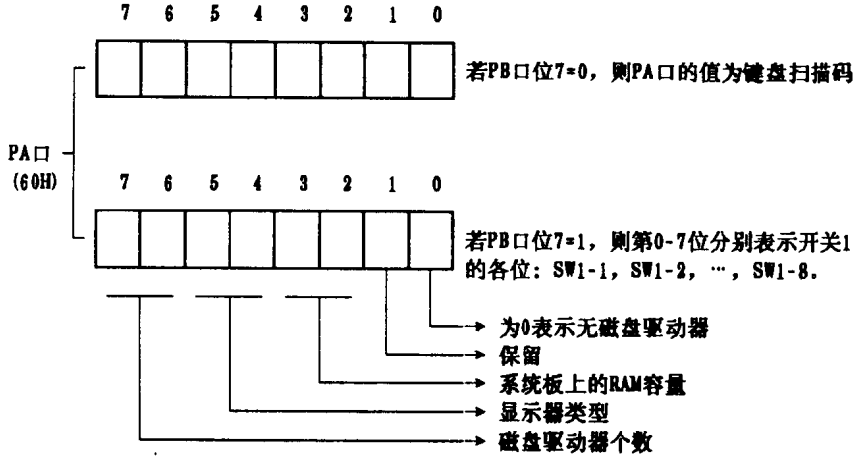

图 1-12　8255 PA 口的位定义