**三种不同的用户类型能够访问一个目录或者文件：**所有者、用户组或其他用户。所有者就是创建文件的用户，用户是所有用户所创建的文件的所有者，用户可以允许所在的用户组能访问用户的文件。通常，用户都组合成用户组，例如，某一类或某一项目中的所有用户都能够被系统管理员归为一个用户组，一个用户能够授予所在用户组的其他成员的文件访问权限。最后，用户也将自己的文件向系统内的所有用户开放，在这种情况下，系统内的所有用户都能够访问用户的目录或文件。在这种意义上，系统内的其他所有用户就是other用户类。

1.1 文件所有者（owner）

　　文件属于谁， 即用户。

1.2 用户组(group)

用户的集合。 体现共享的特性。

1.3 其他人(others)

不属于用户组的集合。注意，root也属于其他人，但是root用户可以访问用户组的内容。

当执行ls -l 或 ls -al 命令后显示的结果中，最前面的第2～10个字符是用来表示权限。第一个字符一般用来区分文件和目录：  
  
d：表示是一个目录，事实上在ext2fs中，目录是一个特殊的文件。  
－：表示这是一个普通的文件。  
l: 表示这是一个符号链接文件，实际上它指向另一个文件。  
b、c：分别表示区块设备和其他的外围设备，是特殊类型的文件。  
s、p：这些文件关系到系统的数据结构和管道，通常很少见到。  
下面详细介绍一下权限的种类和设置权限的方法。

**特殊权限**

其实文件与目录设置不止这些，还有所谓的特殊权限。由于特殊权限会拥有一些“特权”，因而用户若无特殊需求，不应该启用这些权限，避免安全方面出现严重漏洞，造成黑客入侵，甚至摧毁系统!!!  
  
s或S（SUID,Set UID）：可执行的文件搭配这个权限，便能得到特权，任意存取该文件的所有者能使用的全部系统资源。请注意具备SUID权限的文件，黑客经常利用这种权限，以SUID配上root帐号拥有者，无声无息地在系统中开扇后门，供日后进出使用。  
  
s或S（SGID，Set GID）：设置在文件上面，其效果与SUID相同，只不过将文件所有者换成用户组，该文件就可以任意存取整个用户组所能使用的系统资源。  
  
T或T（Sticky）：/tmp和 /var/tmp目录供所有用户暂时存取文件，亦即每位用户皆拥有完整的权限进入该目录，去浏览、删除和移动文件。  
  
因为SUID、SGID、Sticky占用x的位置来表示，所以在表示上会有大小写之分。**加入同时开启执行权限和SUID、SGID、Sticky，则权限表示字符是小写的：**  
  
-rwsr-sr-t 1 root root 4096 6月 23 08：17 conf

4.文件权限 r-S-wxr-t对应的八进制表示形式为[2分]

A.04536

B.05544

C.05435

D.04534

参考答案：C

100 011 101

435