chmod +rwx filename to add permissions. chmod -rwx directoryname to remove permissions. chmod +x filename to allow executable permissions.  
...  
**For example:**

1. chmod 777 foldername will give read, write, and execute permissions for everyone.
2. chmod 700 foldername will give read, write, and execute permissions for the user only.

In Unix-like operating systems, the **chmod** command is used to change the access mode of a file.  
The name is an abbreviation of **change mode**.

1. **Syntax :**
2. chmod [reference][operator][mode] file...

The references are used to distinguish the users to whom the permissions apply i.e. they are list of letters that specifies whom to give permissions. The references are represented by one or more of the following letters:

Reference Class Description

u owner file's owner

g group users who are members of

the file's group

o others users who are neither the

file's owner nor members of

the file's group

a all All three of the above, same as ugo

The operator is used to specify how the modes of a file should be adjusted. The following operators are accepted:

Operator Description

+ Adds the specified modes to the

specified classes

- Removes the specified modes from

the specified classes

= The modes specified are to be made

the exact modes for the specified

classes

**Note :** Putting blank space(s) around operator would make the command fail.

The modes indicate which permissions are to be granted or removed from the specified classes. There are three basic modes which correspond to the basic permissions:

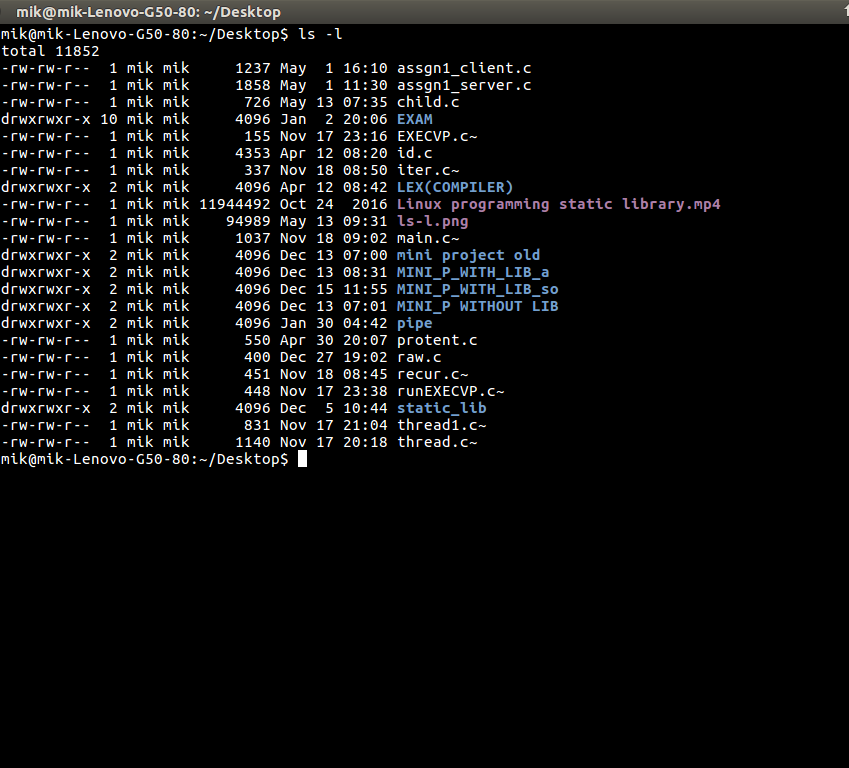
r Permission to read the file.

w Permission to write (or delete) the file.

x Permission to execute the file, or, in

the case of a directory, search it.

Types of permissions which we will be changing using chmod command :  
In linux terminal, to see all the permissions to different files, type ls -l command which lists the files in the working directory in long format. The figure below shows an example to use ls -l and its output :



Let us take a look at above figure. To make things easy to understand some columns and rows are eliminated and extra spaces are added to the permissions column to make it easier to read as shown below:

- rw- rw- r-- mik mik assgn1\_client.c

- rw- rw- r-- mik mik assgn1\_server.c

d rwx rwx r-x mik mik EXAM

- rw- rw- r-- mik mik raw.c

- rwx r-x r-x mik mik header.sh

... so on...

* The very first column represents the type of the file i.e. is it a normal file or a  
  directory where d represents a directory and – represents a normal file.
* The first set three letters after the file type tell what the Owner of the file, have permissions to do. For example: In assgn1\_client.c, has owner’s permission as rw-, which means the owner mik can only read(r) and write(w) the file but cannot execute(x).
* Note: The 3rd and 4th columns represents the name of the owner of the file and the group to which the owner belongs respectively.
* The next three letters after the user’s permission are the group’s permissions.  
  For example: header.sh has group permissions as r-x, which means Other people in the mik group can not write(w) the header.sh script but can only read(r) or execute(x) it.
* Note that when a directory has the x set, this takes the special meaning of “permitted to search this directory”.
* The last three letters in the permissions column tell us what the “others” may do. The general practice is to protect the files from external access so that others can’t write any files or directories. They may read(r) or execute(x) it. For example: The assgn1\_client.c has others permission as r- – which means it can only be read by other(external) access but cannot be written or executed by them.

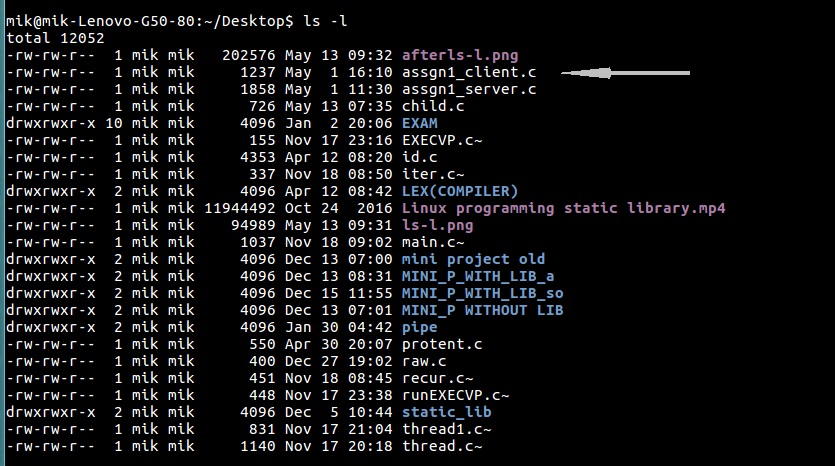
Now, let us see how chmod command can be used to change the access mode of a file.

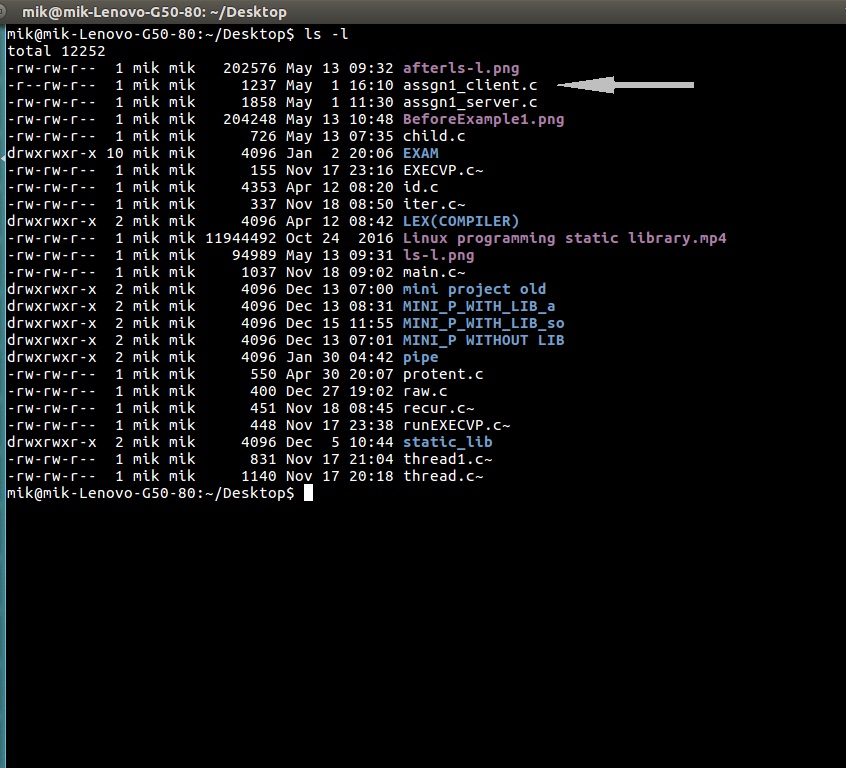
Example 1 :  
Let’s change the assgn1\_client.c permission so that the owner cannot write(w) in the file but can only read it.

BEFORE: -rw-rw-r-- mik mik assgn1\_client.c

COMMAND: chmod u=r assgn1\_client.c

AFTER: -r--rw-r-- mik mik assgn1\_client.c

Before :  


After :  


Example 2 :  
Let’s restrict the permission such that the user cannot search the directory EXAM.

BEFORE: drwxrwxr-x mik mik EXAM

COMMAND: chmod u=rw EXAM

AFTER: drw-rwxr-x mik mik EXAM

After applying the chmod u=rw EXAM command, the user (owner) cannot change the directory. If the user tries to change the directory, then it shows the message “Permission denied” as shown in the figure below :  
