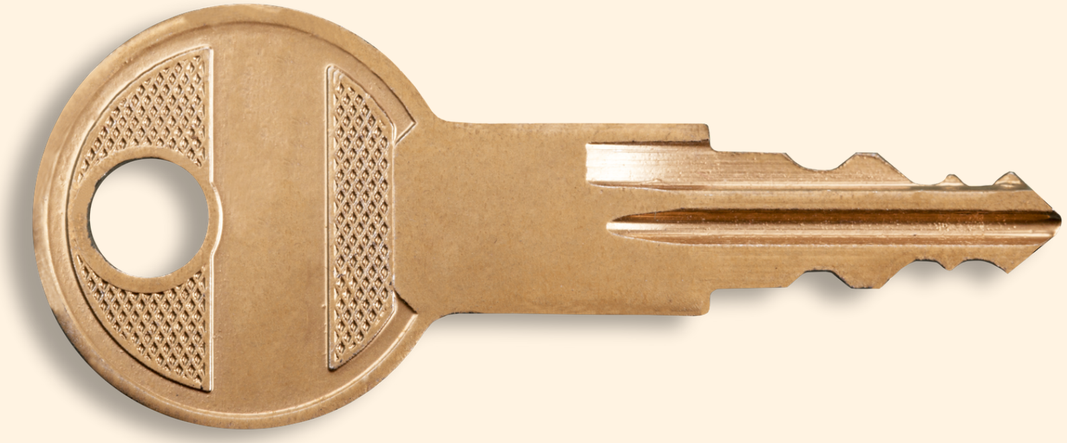
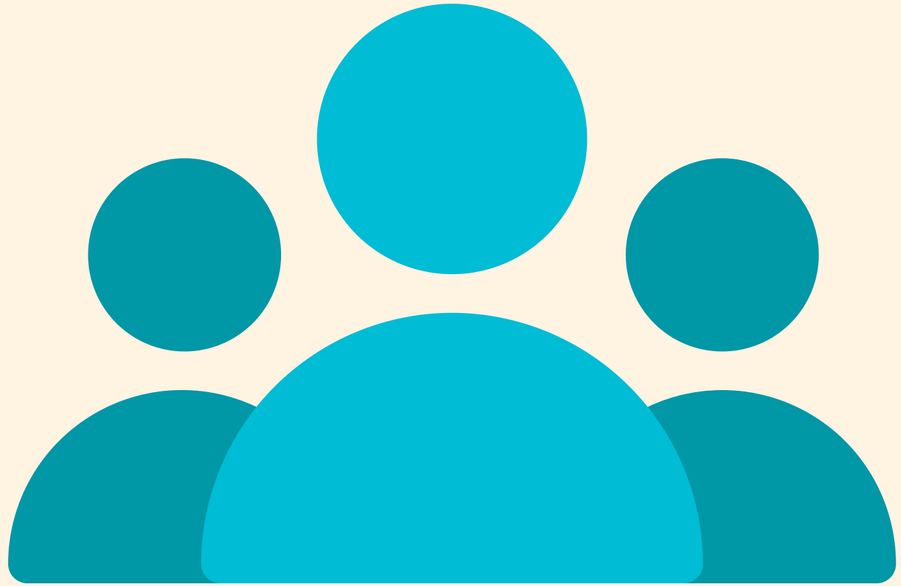
# Understanding Permissions



# Multiple Users

Unix and unix-like systems are **multiuser** operating systems.  More than one person can be using the same computer at the same time (though this is tough logistically with only one display and keyboard!)

Way back when, computers were crazy expensive, massive machines.  A university might only have one computer, but dozens of terminals sprinkled across campus.



# Permission Denied?!

As regular users, we do not have permission to write or even read every file on the machine.

For example, if I try to read the  file /etc/sudoers using cat /etc/sudoers I get a "permission denied" message.

# Groups

On unix systems, a single user may be the owner of files and directories, meaning that they have control over their access.

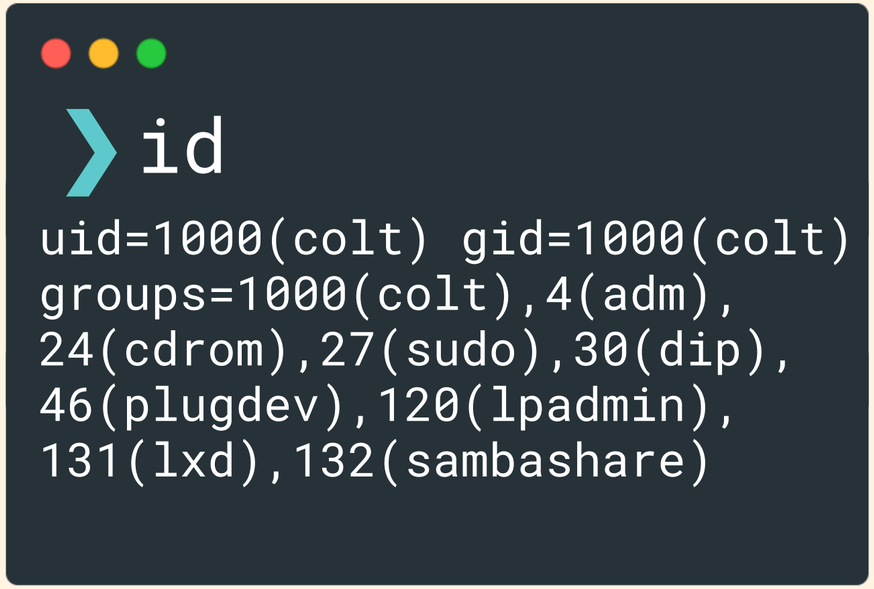
Additionally, users can belong to groups which are given access to particular files and folders by their owners.

# User & Group IDs

When a new user account is made, it is assigned a user ID. The user is also assigned a group ID.

We can use the **id** command to view user and group ids.

These user ids are stored in /etc/passwd, and the group ids are in /etc/group




echo "hi" > greet.txt
ls -l greet.txt
-rw-rw-r-- 1 colt colt 6 Oct 7 14:34 greet.txt

# File Attributes

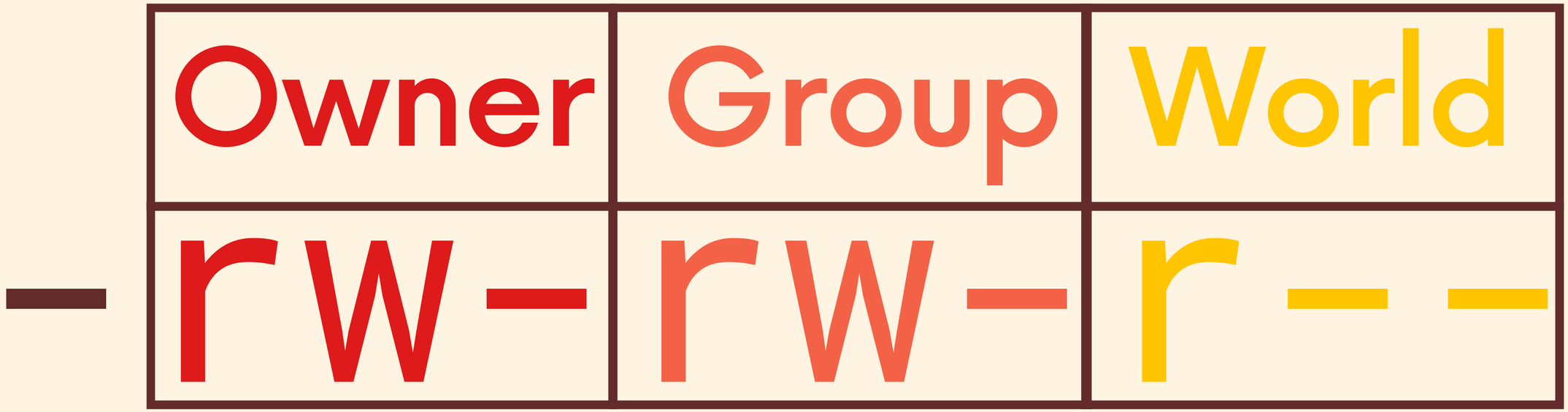
The weird looking 10 characters we see printed out first are the file attributes.

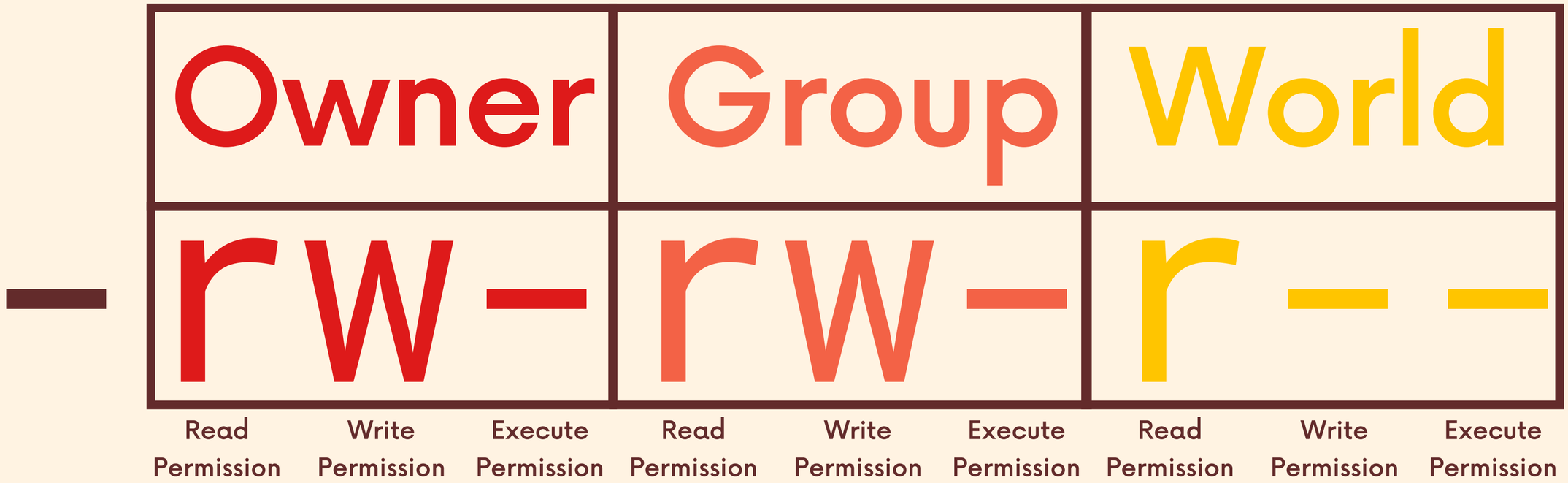
These characters tell us the type of the file, the read, write, and execute permissions for the file's owner, the file's group owner, and everyone else.

# File Type

The very first character indicates the type of the file.  Some of the more common types and their corresponding attributes are:

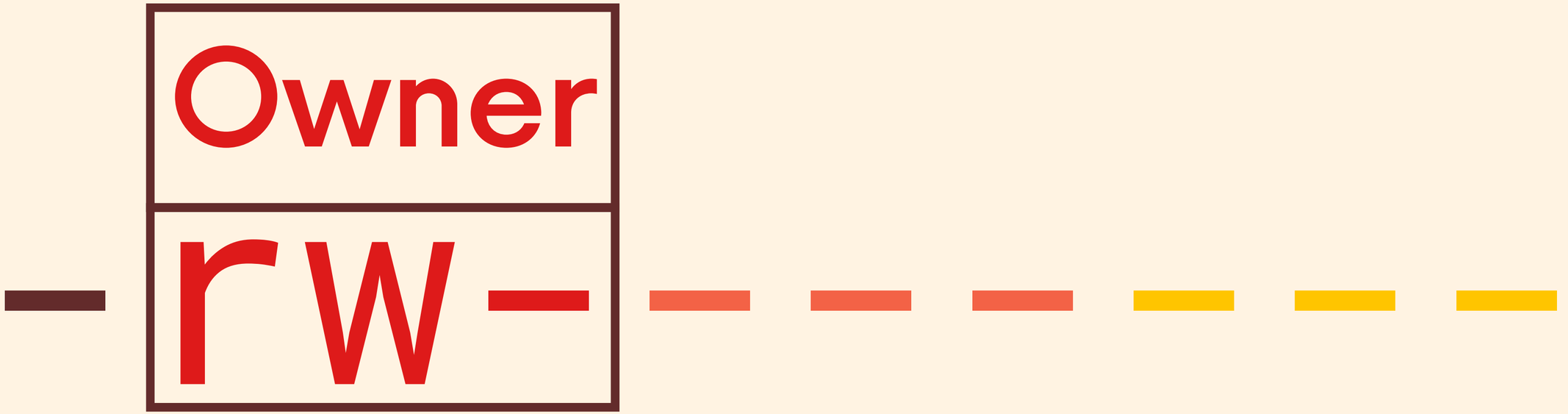
- `-` regular file
- `d` directory
- `c` character special file
- `l` symbolic link



Owner
Group
World
-
rw-
rw-
r--


Owner
Group
World
-rw-rw-r--
Read Permission
Write Permission
Execute Permission
Read Permission
Write Permission
Execute Permission
Read Permission
Write Permission
Execute Permission

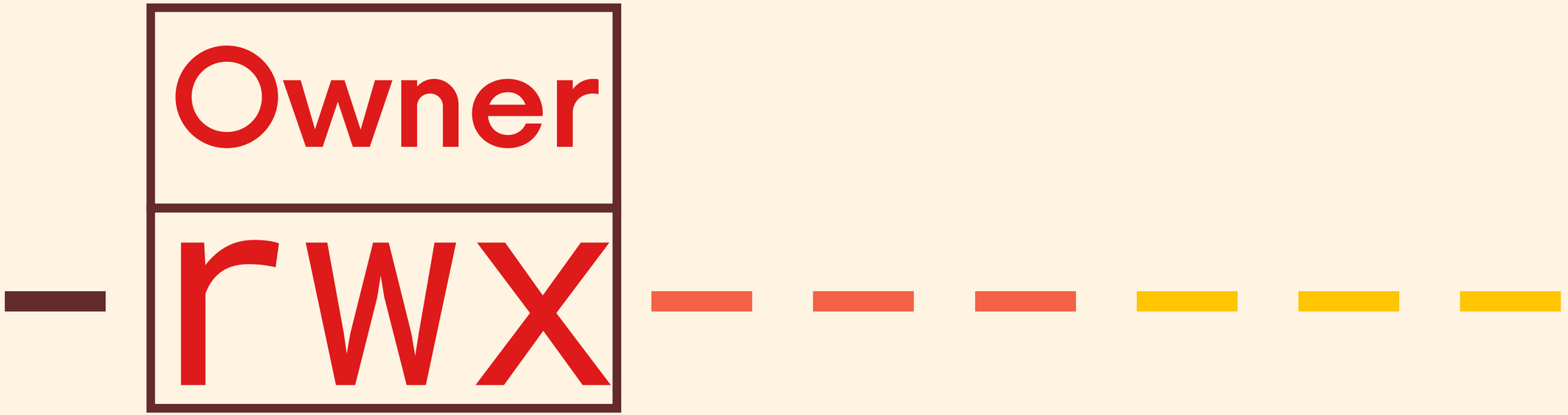
# Permissions

| Character | Effect On Files | Effect On Directories |
| --- | --- | --- |
| r | file can be read | directory's contents can be listed |
| w | file can be modified | directory's contents can be modified (create new files, rename files/folders) but only if the executable attribute is also set |
| x | file can be treated as a program to be executed | allows a directory to be entered or "cd"ed into |
| - | file cannot be read, modified, or executed depending on the location of the - character | directory contents cannot be shown, modified, or cd'ed into depending on the location of the - character |



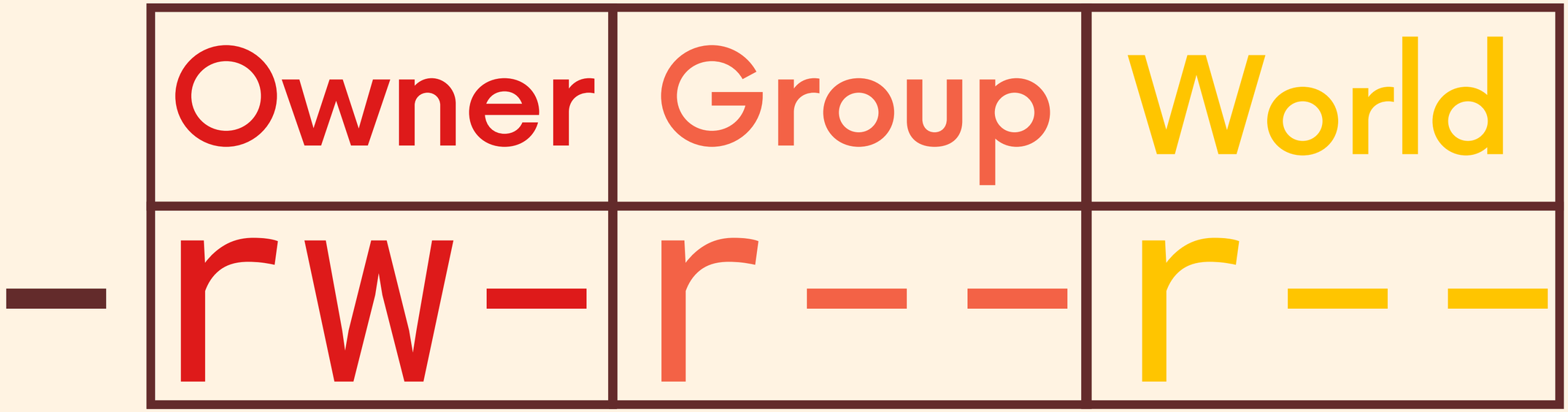

In the above example, we see that the file's owner has read and write permissions but NOT execute permissions

No one else has any access




In the above example, we see that the file's owner has read, write, AND execute permissions.

No one else has any access




In the above example, we see that the file's owner has read, and write BUT NOT execute permissions.

Members of the file's owner group can only read the file

Everyone else can read the file too.

| | Owner | Group | World |
|---|---|---|---|
| d | rwx | rwx | - - - |

In the above example, we see that the directory's owner AND member's of the owner group can enter the directory, rename, and remove files from within the directory

d

| Owner | Group | World |
| --- | --- | --- |
| rwx | - - x | - - - |

In the above example, we see that the directory's owner can enter the directory, rename, and remove files from within the directory.

Members of the owner group can enter the directory but cannot create, delete, or rename files.