SSH, SCP, and SFTP Task

1. SSH connection using password authentication  
2. SSH connection using key-based authentication (with key generation and key copying)  
3. Copying files using SCP  
4. Copying files using SFTP

**1. SSH using Password Authentication**

To connect to a remote server using password authentication, use the following SSH command:

ssh mahmoud@192.168.150.10

You will be prompted for the password of user 'mahmoud' on the remote machine with IP 192.168.150.10. After entering the password, the connection will be established.

**2. SSH using Key-Based Authentication**

**Step 1: Generate an SSH Key Pair**

To generate an SSH key pair on the local machine, execute the following command:

ssh-keygen -t rsa -b 4096

This will create a private and public key pair (by default) in the '~/.ssh/' directory on the local machine.

**Step 2: Copy the Public Key to the Remote Machine**

After generating the key pair, copy the public key to the remote server using the following command:

ssh-copy-id mahmoud@192.168.150.10

Once the key is copied, you can connect to the remote machine without a password by using:

ssh -i ~/.ssh/id\_rsa mahmoud@192.168.150.10

**3. Copying Files using SCP**

**Copy from Local to Remote:**

To copy a file from your local machine to the remote machine using SCP, use the command:

scp /tmp/localfile.txt mahmoud@192.168.150.10:/tmp/

**Copy from Remote to Local:**

To copy a file from the remote machine to your local machine using SCP, use the command:

scp mahmoud@192.168.150.10:/tmp/remotefile.txt /tmp/

**4. Copying Files using SFTP**

**Establish SFTP Connection:**

To connect to the remote machine via SFTP, use the following command:

sftp mahmoud@192.168.150.10

**File Operations:**

Upload a file from local to remote:  
put /tmp/localfile.txt /tmp/

Download a file from remote to local:  
get /tmp/remotefile.txt /tmp/