TD4/9: Work with secured distant communication tools

Exercise 1: SSH

1. Create an account on a cloud computing platform (AWS, Azure, Google Cloud, IBM Cloud)
   - You must enter your credit card number, I have no affiliation
   - It is free. Delete the account in few month to prevent any fee
2. Create a server instance on the website of your cloud platform (ec2 for AWS, Standard B1s for Azure)
3. Connect to the distant server via your terminal
   - Do chmod 400 your private key file. The connection won't work otherwise
   - Use an SSH instruction to connect to your remote instance
   - Exit to return to your local machine
4. Create a script named *connect.sh* to automatically connect to the remote instance
5. Run the script to check it is working properly. Then exit to return to your local machine.
6. Rename your private key to make it a hidden file. Propagate the changes to your script. Run the script.

Exercise 2: SCP

1. On your local machine create a file named *test_to_remote_instance.txt*
2. Connect to your remote instance and create a file named *test_from_remote_instance.txt*. Then exit
3. Use the **scp** command to :
   - Send your file *test_to_remote_instance.txt* to the home folder of your remote instance
   - Get the file *test_from_remote_instance.txt* to your current local directory
4. Create two scripts :
   - *scp_to_remote_instance.sh* and *scp_from_remote_instance.sh* to respectively send and get data with your remote instance
   - Since you would like to send or receive any file (not just the test file), your scripts should use the path of the file to send / receive as an argument
5. Test your scripts with varying files