Part 1

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDD9me72swWhampF1ZeJpyJ7UcEHC3EfWiDjdFK
yDjkzTn3/0y+2wpAdO/toOLEYsNJ2QIxvyFkAO3KFy7QDp7rS3XTf+XOlASO8AZ7W7Rxagwyz
GrLFo2K33PobxXqoyaArnkV4qPnlVW/ckcz3tyyRdv7DUjdn64xV++dJZhplDX1xve7EVDhRrfsn5
UI1nVOXAmTXmV12qZ71Qej1gN/4Lrrqyj18p18iBUEvDba3I22tp57K9czpvijdHXoakypytSXXyc
OPlQVqyuZk4R09QRWEQlNuCRC5O06fIH1AaEGVmmN4mNSD7HcQabqKK6rGhkHwO01RIc
oSiwcpXGKSg6C9utJNePckRVzUtT92NoupmZcVtadF8CRqMY4woZy5z0QwdK9p2XWhfwzuB
1kz6p/9//w0fxu+1GfjPc610UQhswmt8mBLk+RY9vQY/JqRQONlv8y6t82Fl5Apt4Q/KwCwQuZ0F
xxCKa4GLibalwbDgRZnEWQoH+js5FvDCE= 2018oliviac@POM1143

Part 2: Unix Commands

Command	Description
`cd`	changes the working directory
`cp`	copies from a source (1st argument) to a directory (2nd argument)
`exit`	exits out of the shell
`ls`	lists the files in the directory you are in
`ls -a`	lists *all* the files in the directory, including hidden ones [starting with '.']
`mkdir`	make a directory
`scp id_rsa.pub`	copies a file between remote computers or between a remote and local computer[1]
`ssh labXXX`	logs into a remote computer specified by the argument[2]
`ssh-keygen`	"creates a key pair for public key authentication"[2]
`ssh-keygen -t rsa`	-t specifies the type (in this case rsa)
`touch`	make an empty file[3]

[1] https://docs.oracle.com/cd/E26502_01/html/E29001/remotehowtoaccess-55154.html
[2] https://www.ssh.com/academy/ssh/command#ssh-command-in-linux
[3] https://www.geeksforgeeks.org/touch-command-in-linux-with-examples/

Part 3

1. **When and how are the public and private keys used?**

The public key system is made and used for enhanced security over just a passcode. They also help because you don't need to worry about memorizing them to use SSH as they are saved on a file in your computer. The public key, also known as an authorized key, is stored in the SSH and allows for encrypting information. Once this key is authorized, it is stored in the server in a file containing authorized keys. Private keys, also known as identity keys, correspond to the public key and give a user access data encrypted with the public key. It is important to guard the private key.

2. **How is the config file used by SSH?**

[4]The config file is helpful for keeping track of multiple remote systems for use by SSH. Each section of the config file begins with `Host` and then a nickname. This nickname is used in the terminal command to call upon these specifications and establish a server connection. Within the section are then specified options about the connection. HostName specifies the name of the host to be connected to and User specifies the name of the user you are logging in as.

3. **What does `ProxyCommand ssh -q -W %h:%p goldengate` do?**[567]

ProxyCommand is used to connect to a server using commands that it specifies. The -q flag calls for quiet mode, suppressing most warning and diagnostic messages. The -W flag takes in the argument host:port, where in this case %h specifies the remote hostname and %p specifies the remote port. 'goldengate' calls to use a secure connection from the server specified in the 'goldengate' nicknamed entry.

---

[4] https://linuxize.com/post/using-the-ssh-config-file/
[5] http://man.openbsd.org/ssh.1
[6] http://man.openbsd.org/ssh_config.5
[7] https://www.redhat.com/sysadmin/ssh-proxy-bastion-proxyjump