# Laboratory Session 4

## Introduction

The purpose of this lab is to investigate the use of public key encryption for authentication. We will be using a public / private key pair to authenticate an SSH session.

In public / private key cryptography different, but related keys are used to encrypt and decrypt. A message encrypted with the public key can only be decrypted with the private key and vice-versa. Public keys are not secret. Private keys are.

These keys can be used for authentication. Possession of a private key that corresponds to a public key can be regarded as proof of identity. In this approach to authentication, a challenge is issued to the person who holds the key pair. They then encrypt the challenge with their private key which becomes the response. The challenger then uses the public key to decrypt the response. If it is the challenge then they have proven they have the private key.

We will use the Virtual Machines VM1 and VM2 from the first three labs. You will set up an SSH server on VM1 and log into it from VM2 using the public key. You should be able to log in without using a password.

## Method

1. Set up the Virtual Machines used in the previous labs. Check connectivity between the two VMs. Note the IP addresses of VM1 and VM2 using **`ifconfig`**.
2. Install OpenSSH on VM1 and VM2. Do the following on both machines.

   Type the following into a command line terminal:

   **`sudo apt-get update`**

   **`sudo apt-get install openssh-server`**

   You may be asked for a password. All passwords are **`user`**.
3. Generate the public/private key pair on VM2

   Type the following into a command line terminal:

   **`ssh-keygen -t rsa`**

   Accept all the defaults. Do not include a passphrase.

   You should now have a private key pair in the directory **`/home/nsr/.ssh`**. Display the private key by typing **`cat /home/nsr/.ssh/id_rsa`** and the public key by **`cat /home/nsr/.ssh/id_rsa.pub`**
4. Still on VM2, transfer the public key to VM1. In the following instruction <VM1 IP address> is the IP address of VM1 as noted in step 1.

   **`ssh-copy-id nsr@<VM1 IP address>`**

   You should now be able to see the file **`/home/nsr/.ssh/authorized_keys`** on VM1 which should contain the contents of your public key. Again examine it using **`cat /home/nsr/.ssh/authorized_keys`**
5. From VM2 try to log into VM1 using ssh. You should not need a password. If you are asked for a password you have done something wrong. Check what you have done and try again.

   To login from VM2 to VM1 use the following where <VM1 IP address> is the IP address of VM1 as noted in step 1. (Note: the following command uses the letter "l" not the number "1").

   **`ssh -l nsr <VM1 IP address>`**

   Do a screen capture showing the successful login.
6. You should now be logged into VM1. Check by typing **`ifconfig`**. If successful log out and log back in but this time capturing the exchange of packets with Wireshark.

7. You should see the three way handshake, a Diffie-Hellman key exchange and authentication messages. Do a screen capture to show the instructor.

## Assessment of this lab

This lab will be assessed by showing the following to the lab supervisor:

1. Screen dumps showing a successful log in using the public/private key pair. You should not be asked for a password.
2. A wireshark screen dump showing the exchange of SSH messages generated as a result of your login.
3. A short explanation in very broad terms of how the log in works.