Network tools: `ssh`

Unix is rich in tools for network connectivity.

One of the most useful is `ssh`. It allows one to execute commands on a remote machine, either one at a time or in a "login" session. Unlike its predecessors `telnet`, `rsh`, and `rlogin`, it provides a secure session, with both encryption for the session and improved authentication security.

ssh

The general form:

```
ssh [-i IDENTITYFILE] [-p PORT] [-x|-X] HOSTNAME | USER@HOSTAME [COMMAND]
```

ssh

If you just specify the hostname, the username will default to your current one. If you specify a command, it will be executed rather than creating a general login shell.

Using -x turns off X11 forwarding. Using -X allows you to forward X11 windows via the encrypted session you are using.

Setting up keys

The general invocation for ssh-keygen is:

```
ssh-keygen -t [dsa|rsa]
```

Setting up keys

For example:

```
[.ssh]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/langley/.ssh/id_rsa): id_rsa3
Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in id_rsa3.
Your public key has been saved in id_rsa3.pub.
The key fingerprint is:
5d:be:5e:50:ab:75:a6:54:bc:16:6e:65:07:9e:ea:f5 langley@machine.cs.fsu.edu
```

Setting up keys

The contents of the resulting ".pub" file are added to the public keys kept in the remote machine's `$HOME/authorized_keys` file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAq33Tkj7QM68HVK17QB
do8CeyFSTj20Wz89JAJYp4eKD8qDFbDlXg/ngurjIqsuEGRuueIX5Q
h7Re84AaNJdJABYSzZytGR0klO8FFXkBpFEL4bli6ygPAa/vq4cyDV
djmy5S9dulr6afFk/2x3ac4nOgC7LtPSiMh1
UF+N8vpPk= langley@machine.cs.fsu.edu
```

Setting up keys

Once you have added the .pub file to the `authorized_keys` on the remote machine, you need to make sure that you have the corresponding private key in your local `.ssh` subdirectory.

By default, the filenames `id_dsa` and `id_rsa` are used. If you want to login with a private key in a different file, just use the -i option:

```
[.ssh]$ ssh -i id_rsa3 langley@machine.cs.fsu.edu
```