ABBTS BSU Reference Sheet	#3	SSH / Secure Shell

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. Used primarily on Linux and Unix based systems to access shell accounts, SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, leaving them open for interception. The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet.

SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. SSH uses the client-server model. The standard TCP port 22 has been assigned for contacting SSH servers.

- **ssh client**: `/usr/bin/ssh`
(available per default under Debian GNU/Linux and most of the other Unixes)

Usage: `ssh username@remotehost`
or `ssh -l username remotehost`

Options: -v : verbose (debug info displayed)
-C : compress all data on the fly (slow lines, gsm/gprs)
-p : to connect to another port

To run a command on a remote host: (for example: uptime)

```
ssh -v username@hostname uptime
```

- **ssh server** (sshd): optional under Debian, openssh-server package.

Configuration: `/etc/ssh/sshd_config`
Recommended change:

- "`PermitRootLogin no`" to prevent dictionary attacks on root user (-> connect as user, then become root with su/sudo)
- "`Port 22`" -> change the port to a non standard value ("security by obscurity", protects against some script kiddies / robots)
- list authorized IP's under /etc/hosts.allow + /etc/hosts.deny

- **sshd restart** (after configuration change) : `/etc/init.d/sshd restart`

- **logging**: "`last`" (uses information from `/var/log/wtmp`)
and "`fgrep ssh /var/log/auth.log`"

- **public key access** : `ssh-agent`, `ssh-keygen` (more about that later this semester)