CS 35L Software Construction Laboratory (Lab8-A)
Wed, Feb 22, 2012, Ver 1.2

Cryptography

-- Symmetric-key cryptography

```
                    +-----------+
        Message --> | Algorithm | --> Encrypted Data
                    +-----------+
                          ^
                          |
                         Key
                          |
                          V
                    +-----------+
 Encrypted Data --> | Algorithm | --> Message
                    +-----------+
```

-- Public-key cryptography (a.k.a. Asymmetric-key cryptography)

```
                     Public Key
                          |
                          V
                    +-----------+
        Message --> | Algorithm | --> Encrypted Data
                    +-----------+

                     Private Key
                          |
                          V
                    +-----------+
 Encrypted Data --> | Algorithm | --> Message
                    +-----------+

                     Private Key
                          |
                          V
                    +-----------+
        Message --> | Algorithm | --> Signature
                    +-----------+

                     Public Key
                          |
                          V
                    +-----------+
      Signature --> | Algorithm | --> Message
                    +-----------+
```

more reading:
http://en.wikipedia.org/wiki/Cryptography
http://en.wikipedia.org/wiki/Public-key_cryptography

Telnet vs SSH

Telnet:

```
          Sending Unencrypted Data
 Client --------------------------------> Server
          Username / Password
```

SSH:

```
          Sending Encrypted Data
 Client --------------------------------> Server
          cx73@?1= / jJp12;Yt
```

Getting Started with SSH

-- install openssh if you do not have it

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

-- generate SSH key pairs (client side)

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

Get two files:

```
  .ssh/id_rsa     (private key)
  .ssh/id_rsa.pub (public key)
```

-- authorizing access (server side)

.ssh/authorized_keys

This file stores authorized pubkeys from client machines. Append other's pubkey to this file can authorize access without typing passwords.

-- other ssh cammands (check manpage for more information)

Remote host shell access

```
ssh login@remote
```

Execute a single command on a remote host

```
ssh login@remote 'command'
```

Secure Copy

```
scp login@remote:/remote/path/to/file /local/path/to/file
```

Port Forwarding

```
ssh -L [bind_address:]port:host:hostport
```

Enables X11 forwarding

```
ssh -X login@remotehost
```

more reading: http://kimmo.suominen.com/docs/ssh/