Liam and Ruben

Short description of the project:

We will create an SSH client capable of connecting to a remote (host) machine

List of learning goals:

1. Understand packets/how info is sent between machines
2. Understand how the TCP handshake is performed
3. Understand how parameters are agreed upon by host and client
    a. E.g. encryption algorithm
4. Understand DH exchange and how it results in establishing secure symmetric encryption
5. Understand how ssh fingerprints and challenges work

Stretch goals:

- Create an SSH daemon.

List of development goals:

1. Performing the TCP handshake between client and server
2. Perform Diffie Helman exchange to establish secure symmetric encryption
3. Perform symmetric encryption + send packets
4. Handle the challenge that the ssh server sends

A discussion of how you will test (for correctness) and benchmark (for performance) your tool:

We can use a real SSH host, and if we are able to connect, then our client is probably correct. We can also use Wireshark to monitor the packets that we are sending.

A rough schedule of development:

Weeks 3-4: Accomplish goals 1-4

Weeks 9-10: Poster + presentation preparation