The project (to be done in pairs).

The project has 3 parts.

**First** you are to write a client –server chat program in Java. This program should have a ‘server’ software than manages messages and keeps track of clients. Clients should be able to connect to the server and send messages to other clients.

The server can and should run on one of the computers with a client on it, but at least in theory it should be able to work anywhere.

Requirements for the chat program: You should use sockets. A server should be able to connect to multiple clients, and clients should be able address which client they want to message. This can work entirely on a command line. For example server could have 3 clients all connected at once, (Sri, Jawa and Indi), Sri could send a message “Jawa: Hi” and Jawa’s client would show ‘Hi’, but Indi’s Client wouldn’t show anything. Ideally you should also have the option to broadcast such as All: “Dinner time!”.

­­The First part should be done by **May 30th**

**The second** part is that you are going to take your program, and use wireshark to capture the transmission of information back and forth and observe messages.

You should then encrypt your message using some very trivial encryption scheme, capture the data with wireshark, and decrypt the data with a separate program. If you want a useful real world example to try, swap the endianness of the transmission, but if you want something easier that’s fine too.

The second part should be done by **June 6**

**Lastly** you are going to try and encrypt (using an encryption library don’t write this on your own) your messages. And again, use wireshark to capture those frames. Given that you know the key, decrypt the wireshark frames (that you use in the source code). This may mean hard coding encryption keys which in general is bad practice. You are demonstrating that you’ve thought about how this could go badly, not how to do it perfectly. (Due at the end of the course)

The final part of the project is due **June 15**