## 2019/2020 - Semester 2

## EE6032/ED5012 – Term Project Work – 30%/20%

## To be performed by GROUPS of THREE people.

## SECURE CHAT SERVICE

1. You can use a programming language and toolbox of your own choice to code this project.

2. **A User Interface/GUI of your own choice/design**.
   This is to allow a user to establish a Chat with another user – localhost IP is 127.0.0.1 for single PC socket to socket communications.
   a) Use socket communications to allow two parties to establish a chat between them. Local IP address is 127.0.0.1
   b) String entered directly by the user and sent – chat service.
   c) Full file transfer – filename specified by the user (***images are best to test transfer***).

3. **There are two options for this part:**
   **Option (i) is marked out of 30% and option (ii) is marked out of 20%.**

   **(i) Implement a protocol of your own design: (30%)**
   Allow two parties to:
   a) **Mutually generate** (mutually generated – two parties each provide a share of the password/passcode used to generate the secret/session key**) a session key** (for use with the AES symmetric Algorithm) using the RSA public key or DH algorithm to exchange relevant shared information. The following is to be provided in the key establishment communications:
      a. Data confidentiality.
      b. Digital Signature/Authentication of session Key generation components.
      c. Data Integrity – **this is optional.**

   # OR

   **(ii) Use the toolbox from your programming tool to establish a session key to be used with SSL. (20%)**
   a) This option will use a standard protocol for the security toolbox you are using.

4. **Note:** Data **confidentiality** is to be provided for all data in the chat/file transfer service.

5. **Final project files are to be submitted via Sulis**

   **Make sure all group members are cc on the email to me.**
   **Only one email submission per group.**

**Look at the marking scheme on the next page to see how the 30% will be distributed.**

# 2019/2020 - Semester 2

# EE6032/ED5012 – Term Project Work – 30%/20%

# To be performed by GROUPS of THREE people.

## Marking Scheme

**The final project is to be demonstrated in the Lab in week 11 and it will be graded at the same time according to the following Schema.**

**Each group member will be asked a number of questions and you will be individually scored based on your answers.**

**<u>Total marks awarded are 30%, divided as follows:</u>**

1. **Week 11 Grading in the Lab to include the following: (Total worth 30%)**
   In this part (20%) you can use standard library functions to establish a session key.
   a. GUI design. (5%)
   b. Session key establishment. (5%)
   c. Demonstrate Txt Chat - using sockets with security. (5%)
   d. Demonstrate secure file transfer - using sockets with security. (5%)

2. Implementation of a mutually agreed session key generation protocol of your own design: (10%)