2016/2017 - Semester 2

EE6032/ED5012 – Term Project Work – 40%

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).

3. Implement the following algorithms in whichever security library you have chosen.
   a) The AES Symmetric Encryption Algorithm.
   b) The SHA Hashing Algorithm (select from SHA1, 2 or 3).
   c) The RSA Public Key algorithm. In this you need to have the generation of the public/private key pair also.

4. Now use the algorithms from part 3 to **implement a protocol of your own design** to allow: Allow two parties to:
   a) ***Mutually generate*** (mutually generated – two parties each provide a share of the password used to generate the secret/session key) a session key (for use with the AES symmetric Algorithm) using the RSA public key algorithm to exchange relevant and signed information.
   b) The following is to be provided in the key establishment communications:
      a. Data confidentiality.
      b. Digital signature of session Key generation components.
      c. Data integrity.

5. Integration of all parts (1 to 4) to provide a secure service that facilitates both secure chat and secure file transfer using the protocol established in part 4 to generate a session key for use with AES. Data **confidentiality** and **integrity** are to be provided in the chat/file transfer service.

6. **Final project files are to be emailed to me after final grading - (No executable files):**

   Thomas.newe@ul.ie
   Subject line: EE6032-ED5012 Project files

   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 40% will be distributed.

2016/2017 - Semester 2

EE6032/ED5012 – Term Project Work – 40%

To be performed by GROUPS of THREE people.

Marking Scheme

Total marks awarded are 40%, divided as follows:

1. **Week 7 Grading in the Lab to include the following:** **(Total worth 20%)**
   a. GUI design. (5%)
   b. Demonstrate Txt Chat **and** File transfer (using sockets) (no security). (5%)
   c. Demonstrate AES, RSA and SHA algorithms working (incl. RSA key generation). (10%)

2. **Week 11 Grading in the Lab to include the following:** **(Total worth 20%)**
   a. Generate generation of a mutually agreed session key: (5%)
   b. Demonstrate secure txt chat using AES and session key. (5%)
   c. Demonstrate secure file transfer using AES and session key. (5%)
   d. Overall system ease of use and design. (5%)

The final project is to be demonstrated in the Lab in week 11.

Some Sites to help:

Java:

https://docs.oracle.com/javase/tutorial/networking/sockets/

http://www.javaworld.com/article/2077322/core-java/core-java-sockets-programming-in-java-a-tutorial.html

http://www.oracle.com/technetwork/java/socket-140484.html

C++:

http://www.qt.io/developers/

http://doc.qt.io/qt-4.8/network-programming.html

http://www.bearcave.com/software/qt_socket_example.html