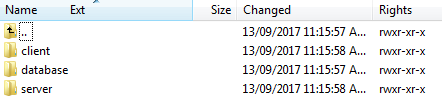
**INTE3070/3071 Secure Electronic Commerce**

**Assignment**

(10 marks)

Based on your practices in labs, develop an online e-commerce (shopping) system using **html**, **javascript** and **php**. You can assume any products for sales.

Please create a folder called “assignment” under your student folder, and construct the website as three folders (same as previous labs), **client**, **server** and **database** as follows:



We will assess your assignment on the basis of the website under the following link:

titan.csit.rmit.edu.au/~sXXXXXXX/assignment/

where the sXXXXXXX is your student number. **Please make sure to put everything (with correct permission) under the folder “assignmnet ”.**

Please add a readme.txt file to explain your website, such as how to register, how to login, ect.

**The marking scheme is as follows:**

1. **Registration of your website (up to 1 point)**
   1. Keep username and plain password in the database (+0.5 point)
   2. Keep username and hashed password in the database (+1 point)
2. **Login to your website (up to 2 point)**
   1. Username and plain password are POSTed to server for check (+1 point)
   2. Username and hashed password are POSTed to server for check (+2 points)
3. **Shopping Cart page (up to 1 point)**
   1. Only successful login user can access to the shopping cart (+0.5 point)
   2. The quantity of each item in the shopping cart can be updated (+0.5 point)
4. **Post shopping cart information and credit card number to Server (up to 6 points)**
   1. Post plain information and display plain information (+1 point)
   2. Post encrypted information and display plain information - RSA only:
      1. Shopping cart information and credit card number are encrypted with RSA encryption algorithm (+2 points).
      2. The server decrypts the information with RSA decryption algorithm and stores it in the database (+2 points).
   3. Post encrypted information and display plain information - RSA and DES:
      1. A successful login user posts an encrypted DES key (chosen by the user) to the server with RSA encryption algorithm (+2 points).
      2. The server retrieves the DES key with RSA decryption algorithm and keeps the DES key for this user (+2 points).
      3. The user will encrypt the shopping cart and credit card number with DES encryption algorithm and DES key (shared between the user and the server) before POSTing to the sever, and the server decrypts the encrypted shopping cart and credit card number with DES decryption algorithm and the shared DES key and stores it in the database (+2 points).

**NOTICE!** Please use **RSA** **encryption** **key** and **decryption** **key** in Lab 8 of Week 9, all other necessary files, such as des.js, rsa.js, private.key, public.key, …, can be downloaded from the blackboard.