**Assignment One (Due date 22/4/2016: 4:00pm) (20 marks)**

**Objective:** To implement **Affine Cipher and DES** in any programming language with your preference. **But** you are required to finish this assignment ***independently*** and strictly follow the ***requirements***.

1. Implement the **Affine Cipher** (see lecture notes) in one programing language with the following requirements.

    - You have a separate code to testify whether a given key (a,b) is eligible.
    - You have separate functions for encryption and decryption and also your code should work for encryption and decryption for any given eligible key. (After decryption, the original plaintext is recovered).
    - You code should be capable to encrypt and decrypt both capital and lower case letters (ignore symbols).
    - You code should work for the given test file. (Able to encrypt and decrypt correctly).

After implementing your code, you MUST answer the following questions in your hard copy submission.

- Compute all possible eligible keys you can use and justify your computation convincingly.
- If your code works properly with selected eligible key, show recovered original plaintext after decryption; (the test file is given in the unit website). State the possible reasons if not working properly.
- **Mathematically prove** the decrypted message equals to the original message with logical reasoning.
- Use your code in Tutorial 1, print out the letter distribution with a graph chart for the given test file.
- Submit your code in your hard copy assignment.
- Print out the first page and last page of decrypted file and compare it with the original plaintext, are they the same?

2. Implement **DES** in any programming language. The requirements are follows:
   - Your code should be able to encrypt and decrypt all possible characters on a keyboard.
   - The key for encryption and decryption is required to be any combination of characters in a keyboard with finite length (You need to do padding or chopping if necessary.)
   - You are required to implement **key generation**, **switch function** and **Fk** as three **separate** functions (You should have these three functions separately in your hard copy) and then combine all of these operations to achieve **DES**.
   - Make sure it works properly for the given test file.
   - Change the elements in all S-boxes with the required constraint (S-Box elements are required to be between 0-15) and check whether your code still works as expected.

   Now you can answer the following questions in your hard copy submission after you have done all above.

   - Mathematically prove DES works (After decryption, you can obtain the original plaintext).
   - State your pseudo code structure based on the three separate required functions.
   - State **clearly** what is the main difficulty in the process of your programming if your code is not working **properly**?
   - Print out and submit the outputs for encryption and decryption for a test file given in the unit website. (Only the first page and last pages are required for hard copy.)
   - Print out and submit a hard copy of your code **with structure explanation by using the three functions** (make sure it looks nice).
   - Try to do encryption and decryption with a key of all 0's, and report your findings.

   *You need to report your design/progress and demonstrate your code in the lab for these questions.*