Lab 1: Cracking a Shift Cipher

(Updated on May 20, 2017)
Submission due: Monday, June 12, 2017

Objective: Master the shift cipher cracking method by finding the decryption key and recovering the plaintext for given segment of ciphertext.

Project procedure:

1. This is an individual based project.

2. Write a C program for cracking a shift cipher using **Method three** in the lecture notes. Download the ciphertext assigned to you. (English letter frequency can be downloaded here)

3. A sample pair (updated on May 18, 2017) of plaintext and ciphertext is also available, which can be used to check your program.

4. Your program need to be demonstrated to the GA in a lab class before you submit your lab report.

Programming language: C language

Project report contents:

1. Cover page includes course number & title, lab title, your name and ID;

2. A result page should include the assigned ciphertext, the decryption key, and the plaintext. Letter count and a list of inner product values should be also included. The downable demo.txt could be used as a template for lab report result page.

3. Your program source code

Project report format:

- Arrange the report in one single file in either word, pdf or txt format;

Submission Method:

- Submit your project report through Blackboard website.

Project Grading:

- The full marks for Lab 1 are 100, which has 5% of the total course weight.

- Note that it is required to show intermediate results (letter count and a list of inner product values) in your lab report. Missing or wrong intermediate results could lead to up to 50% mark deduction.