Ghulam Ishaq Khan Institute of Engineering Sciences & Technology

Faculty of Computer Science & Engineering (FCSE)

CS231B – Discrete Mathematics

Assignment 1 (Fall 2019)

Total marks – 04 points **Due Date** – 13 December 2019 **Instructor** – Dr. Raja Hashim Ali

Instructions:

1. There are **(1+1)** parts of this assignment, both parts carry **(3+1)** marks.
2. This assignment is a group assignment, please do not share your solutions, designs or ideas with other groups.
3. You have to build a project repository on git, then add each document you make and then add the project files. The git repository must contain the complete project history including all commits.
4. Send me an invitation to be administrator on your git repository, so that I can view your progress. Remember No GIT and no invitation to me, no marks for this assignment.
5. Please remember to commit your code on the repository periodically, so that there is always backup available.
6. Read the details carefully first, understand the statement, write your algorithm in pseudocode and then start coding.
7. There will be vivas in the fifteenth week of selected students.
8. Passing this assignment is a must! You will not be allowed to sit in final exams unless you clear this assignment.
9. Any verified case of cheating (including sharing ideas or solutions) will lead to straight F in this course, (No ifs and Buts).
10. You can use internet, TA or me to get help.

CLO Mapping Table:

	Parts of Assignment
1	
2	

Marks Sheet:

	Parts of Assignment
1	3 marks
2	1 marks

Dated: 19 November 2019

Instructor: Dr. Raja Hashim Ali

In this assignment you are supposed to implement a very basic version of encrypting and decrypting a message using shift cipher. Shift ciphers have been in use for thousands of years, most famously by the Roman emperors in particular Julius Caesar.

You will need to implement a cryptosystem that has the following five elements.

1) E: An encryption algorithm (using Shift cipher).
2) D: A Decryption algorithm.
3) M: The set of plaintext message.
4) K: The set of keys
5) C: The set of ciphertexts.

The plaintext consists of all capital letters of English, space, comma, full stop, new line character, small letters of English language and digits from 0 to 9, in total (26 + 1 + 1 + 1 + 1 + 26 + 10 = 66) characters. The encryption algorithm will shift the plaintext by a user specified value k to produce the ciphertext. The decryption system will first determine the value of k using the first line in ciphertext (more details below), and then decode the whole message. The decrypted message must then be written out to the output file.

As submission, you have to submit two separate programs.

1) Encryption program.
2) The decryption program.

Part 1 – Encrypting the message

You must take in the message in the form of a file starting with (Discrete Mathematics.\newline) exactly as shown in the sample input plaintext file. Then, ask the user for a value of non-negative k, which you will first mod with 66 to determine the actual shift and then apply shift cipher to determine the ciphertext.

Input: A plaintext file that contains (Discrete Mathematics.\newline) as the first line and a non-negative value k for using in shift cipher.
Output: A ciphertext file that contains the encrypted text including all lines, text and paragraphs.

Part 2 – Decrypting the message

Starting with the ciphertext file (preferably hard-coded in your program), you are to first determine the value of k, for which the first line is (Discrete Mathematics.\newline). After determining the k, proceed to decode the whole message and output the decrypted message, including the first line, in a file for user.

Input: A ciphertext file produced from the previous part and the name of output file (to be produced in the same directory as the ciphertext file).
Output: A plaintext file consisting of decrypted message determined by the decryption algorithm.