Programming Assignment#2
CS-G513

Due: 20/4/2018 before 11:59 PM

The goal of this assignment is to understand the importance of performing multiple Fiestal rounds in DES. The DES performs 16 rounds. As part of the Homework #2, you have already implemented the DES algorithm. In this assignment, you can use the same implementation with a only difference that, now we will perform only 2 rounds instead of 16 rounds.

You are provide a plaintext and a corresponding cipheterext pair in the files **sample_plaintext.txt** and **sample_ciphertext.txt** respectively. The ciphertext has been generated using the DES algorithm with 2 rounds only. The 56-bit key used for encryption is derived for a password containing exactly 7 ascii characters (8 bit character), where the last character of the password is the character 'a'. Please note that the password contains ascii characters not the alphabets. Your task is to find the plaintext of the ciphertext given in the file named **target_ciphertext.txt**. The last character of the password is reveled to reduce your effort of performing bruteforce attack and make the attack feasible.

Submit your decoded plaintext along with the source code as a single zipped file by sending an email to me from your official mail Id latest by April 20 (11:59 PM). Please note that this is hard deadline and no request for the extension will be entertained