**Breaking of a Simple Cipher  
Programming Assignment 1**

The python script (**Encrypt.py**) provided along with this assignment implements an encryption algorithm (cipher), that takes a plaintext message file as input and produces an encrypted file as the output. As a sample to demonstrate the working of the cipher, a **plaintext.txt** and its corresponding **ciphertext.txt** is also provided. The key that has been used to produce this sample ciphertext is **bits@f463.** As part of this assignment you are supposed to do the following tasks.

1. Explain the encryption algorithm implemented by the python script **Encrypt.py**.
2. Write the corresponding decryption script which will take output generated by the encryption script and generate the same plaintext as the output that was given to the encryption script as the input, considering both the encryption and decryption scripts are run with the same key.
3. You are supposed to submit a CRACK code (CRACK.py) which when supplied with a ciphertex generated by the cipher should produce the corresponding plaintext. Note that, producing complete plaintext may not be feasible. So, even if your code is able to generate the partially correct plaintext, it is fine. In one sense, we are performing a ciphertext only attack to get the plaintext. It would be good if you use python language to write your code. However, you can convert the python script provided herewith into a C program and then write the CRACK in C.

**Submission Details**

1. Submit a PDF file, **Assignment1.pdf** for the task 1, a **Decrypt.py** script for task 2 and **CRACK.py** script for task 3
2. The **CRACK.py** file submitted by you should take the ciphertext from the file with name “ciphertext.txt” only. The output (plaintext) generated by your code should be written in the file with name “**recoveredtext.txt**”.
3. Your code will be executed multiple times, each time with a new ciphertext, generated by the given cipher with a different key and the different plaintext.
4. Note that BORROWING or COPYING the source code will lead to heavy punishment.

**Submission Date:** BeforeSep 20, 2019, 23:59 hrs