Introduction to Cryptography:

Assignment #1: Last date for submission: 17 Jan 2021

The assignment is to implement substitution cipher.

You have to write a code either in c++ or python (python3): The programme files should be named **encr.cpp** and **decr.cpp** or **encr.py** and **decr.py:**
encr.cpp or encr.py should take as inputs two files named **Key.txt** and **Plain.txt.**
Key.txt that will have an arbitrary permutation of 26 alphabets (in capital) such as PNIYUHZGMKVAQCETXOFRSDLJWB

The file named plain.txt should contain a english language text – over 5000 words (in ASCII code) taken from some book (one source of books is https://www.gutenberg.org which has copies of large number of books. Take some book that you like and take a few pages form the book, say OVER 5000 words).

Important : the programme should not need any arguments to be passed at run time.

In either case, it should (i) remove all characters other than 26 alphabets, replace tab and newline character by "space" and retain the "space" character as it is, then (ii) convert all characters to uppercase, and (iii) encode each character using the permutation given in the file **Key.txt** and the coded text should be written to a file named **Cipher.txt.**

Also, the file decr.cpp or decr.py should have code that takes as input the files **Key.txt** and **Cipher.txt** and produces a file called **Message.txt** .

Of course, if the same permutation is used to encrypt and decrypt then **Message.txt** should be same as **Plain.txt** (minus the extra characters).

Please write your name, your CMI roll number, your current batch (BSC I/BSC II/BSC III / MSC CS I/MSC DS II/.....) in the code files (with comments)

The files :
1. Key.txt
2. Plain.txt
3. Cipher.txt
4. Message.txt
5. encr.cpp or encr.py
5. decr.cpp or decr.py
should be put in a directory and then "zip" the whole directory and name the zipped file again with your roll number-with suffix "_1" (for the first assignment). Thus, if your CMI roll number is BMC201887, the zip file name should be BMC201887_1.zip
---
I do not have a TA for this course. So please follow the exact conventions for coding and file naming that I have described. Else your submission may be rejected.
--
send the zip file by email to me at
rlkcmi+cryp@gmail.com

with subject : CRYP-A1

Last date for submission: 17 Jan 2021