Codebreaking
Programming Assignment 1

In this programming assignment you are supposed to write a CRACK i.e the code that takes ciphertext as input and produces the corresponding plaintext without knowing the key for the ciphertext provided to it.

Steps:

1. Download the cipher that you are supposed to crack.
2. Optionally, you can also download the example plaintext and its corresponding ciphertext generated by the above cipher. Currently the key is hard coded in the cipher. However, I can use any random key at the time of evaluating the CRACK code submitted by you.
3. You are supposed to submit a CRACK code which when supplied with a ciphertex generated by the above 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. The instructions for submitting the code will be provided later. It would be good if you use python language to write your code. In that case only submit the .py file.

About the Encryption Scheme

The plaintext contains usual English paragraphs. The key contains only capital letters. To encrypt a small letter, it is first converted to its corresponding capital letter, which is then encrypted as capital letter, and finally the encrypted capital letter is converted back to corresponding small letter. So, in ciphertext, a small letter corresponds to a small letter in plaintext and same for capital letter. The special characters (characters other than alphabet) are copied as it is in the ciphertext from the plaintext. However, the spaces from the paragraph have been removed. So, it does not matter whether we give spaces between the words in the plaintext or remove it. An example to demonstrate the process of encryption is given here.

- **Plaintext:**

One day a college professor after getting irritated in his college class stands up in front of the class and asks if anyone in the class is an idiot, and if there is one then he/she should stand up. After a minute a young man stands up. The professor then asks that guy if he actually thinks he is an idiot. The boy replied, "No, I just didn't want to see you standing there all by yourself."

Courtesy: Internet

- **Ciphertext**

lkrfkigkhudkgihrkgifjwmlsogmaolgoqwjldksnjgodlfkigjnalgnloriwqlfksnvjoidjtifklsangkodlcmgkieksauvglojqmldkoelan ldmksislo,fklsofjtoglasjvmkgorw/edpgldkgnotaldkscmgkoegldjm. … *ciphertext cont*…….

Notice the presence of symbols “,”, “/” and “.” in the ciphertex

Evaluation Scheme

1. The .py file submitted by you should take the ciphertext from the file with name “ciphertext” only. The output (plaintext) generated by your code should be written in the file with name “plaintext”.
2. The code submitted by you should not take any command line argument.
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. The average degree of similarity between the plaintext provided by your code and the real plaintext would be considered as your score.
5. Note that BORROWING or COPYING the source code will lead to heavy punishment.
6. The procedure to SUBMIT the assignment (.py file) would be announced later.

Important Dates

- Start Date: Feb 5, 2018
- 1st Deadline: Feb 20, 2019 (Max Marks. 20)
- 2nd Deadline: Feb 30, 2019 (Max. Marks 16)
- 3rd (final) Deadline: March 10, 2019 (Max Marks 10)