CSE2023

ASSIGNMENT #4

Due date: 12.12.2018

The process of recovering plaintext from ciphertext without knowledge both of the encryption method and the key is known as *cryptanalysis* or *breaking codes*.

In this homework, you will break the code of a text encrypted by an affine cipher.

An affine cipher uses functions of the form $f(p) = (ap + b) \bmod 26$, where a and b are integers, chosen so that f is a bijection. Note that the function is a bijection if and only if $\gcd(a,26) = 1$.

You will firstly write a program that encrypts a given text with affine cipher with randomly chosen a and b values. (Note that the program should choose a from a set of values that are relatively prime with 26.) The output of this program is another text file containing the encrypted version of the original text.

Then your second program will take place, which will take the output text file of the first program as the input and will try to decrypt it. See that the number of combinations of a and b for creating an affine cipher is really low (about 312), so you can apply a brute force algorithm to break the code. However, an important tool for cryptanalyzing ciphertext produced with an affine ciphers is the relative frequencies of letters. The nine most common letters in the English texts are E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6%, and R 6%. So, you can use this fact to make a guess on the a and b pairs that you are looking for. The output of the second program will be to print a and b to the screen.

To check whether a guess on a and b really works, you will use the dictionary provided as attachment to this HW. To reach to a decision you can simply check whether a high percentage (like 90%) of words created from decryption process are in the dictionary.

You can try the attached text files as inputs to your program, but your program should work with any other input file.

Notes:

- In the encryption and decryption process, any character other than a letter can be left as it is.
- The programming language can be either Java or C.
- Send your homework to muhammed.avcil@marmara.edu.tr with the subject line "CSE2023, HW4, Your Name, Your ID."