**Assignment 2**

**Problem Submission Rules:**

1. **Detection of plagiarism will result in Failing grade. Students must do this assignment by themselves.**
2. **After completion, your work must be submitted to an assignment folder in D2L by a corresponding deadline.**

**Problems (total 100 points):**

The aim of this assignment is to implement Playfair cipher. Specifically, your implementation should have the four functions: Key matrix generator, Preprocessing, Encryption, and Decryption.

Pre/post conditions for the algorithms can be described as follows:

* *Key (K)*
* The key matrix generator takes as input an encryption key and outputs the key matrix *KM*.
* *Pre (P)*
* This function takes as input a plaintext (String type).
* The preprocessing converts the plaintext into a list of two characters (*PL*),   
  e.g., “rule” => [“ru”, “le”]
* If two characters are equal, put an ‘x’ at the middle, e.g., “hello” => [“he”, “lx”, lo”]
* If the last block has one character, put an ‘x’ at the end, e.g., “sox” => [“so”, “xx”]
* For your convenience, it is OKAY to change all ‘j’s in the plaintext to ‘i’ in this function.
* This function takes as input the key matrix *KM* and the list of two characters *PL.*
* Case 1: If two characters are on the same column, each of which is replaced to a character in the below cell. If a character is located at the bottom, a character in the top cell should be taken.
* Case 2: If two characters are on the same row, each of which is replaced to a character in the right cell. If a character is located at the rightmost, a character in the leftmost cell should be taken.
* Case 3: “xx” will not be encrypted. It will be just “xx”.
* Case 4: Otherwise, two characters are replaced by the others on the other vertices, e.g., List indices of two characters are (0, 4) and (3,1), then each of which is replaced to a character in the (0,1) and (3,4), respectively.
* The output type should be a list of two characters.
* This function takes as input the key matrix KM and the list of two characters *CL*.
* Case 1: If two characters are on the same column, each of which is replaced to a character in the above cell. If a character is located at the top, a character in the bottom cell should be taken.
* Case 2: If two characters are on the same row, each of which is replaced to a character in the left cell. If a character is located at the leftmost, a character in the rightmost cell should be taken.
* Case 3: “xx” will not be decrypted. It will be just “xx”.
* Case 4: Otherwise, two characters are replaced by the others on the other vertices, e.g., List indices of two characters are (0, 4) and (3,1), then each of which is replaced to a character in the (0,1) and (3,4), respectively.
* The output type should be a String.
* *Your program should have some test codes to show the correctness of your implementation* ***–***

Note 1: If you prefer, you can use a list of characters ([‘r’, ‘u’, ‘l’, ‘e’]), rather than a list of two characters ([“ru”, “le”])

Note 2: For the detail of Playfair cipher, please refer page 79.

**Complier requirement:**

The text converter must be implemented using Python version 3.9.x or higher. Students must use Python official libraries that are accessible from the webpage (<https://docs.python.org/3/library/index.html>). All used libraries and their purpose should be described in the report.

**Submission instructions:**

Please submit your deliverables to D2L Assignments folder: PA 2. You need to submit 4 different things. ***Do not submit zip files. You will get zero if you do.***

1. Your Python code saved as yourlastname.py
2. Your Python code saved as yourlastname.txt - copy and paste your entire Python code, save
3. Your report yourlastname\_Report\_PA2.doc as a word document
4. A short video demo: (3-5 minutes)
   1. Explaining your code
   2. Choose a word as Key, the word should be at least 6 characters or more and should not contain a letter more than once. I am expecting each student will pick a different word. Chosen the same word with another classmate may cause plagiarism.
   3. Show the Playfair matrix as a Key.
   4. Use your first and last name as a plaintext and show the cyphertext.
   5. Use your first and last name as a cyphertext (Output of d) show the plaintext.
   6. Do d and e for a sentence of your choice.

Once you submit, D2L will perform a similarity check for your submission and show you the result. Your similarity score on your code as txt file must be lower than 40% unless something essential is described in the report. *Otherwise, 5 points will be deducted for every additional 5% similarity*. For example, you would get a maximum 95 if your similarity is between 41% and 45%.

**Project Report:**

The report does not have any specific format. Three things you must include:

1. What you did for the project, i.e., explain the project with your own word.
2. Explain your program/code.
3. Explain output, include screen shot.

You could add anything else you like.