CIPHERS

About:
The objective of this assignment is to get students to understand some of the main concepts in cryptography, which are:

Cryptography of **Playfair** cipher

Prerequisites:
Install cryptools 1.4.42 from https://www.cryptool.org/en/ct1/

ASSIGNMENT ONE

Exercise • 1: (5 POINTS)

The Playfair cipher is a digraph substitution cipher. It employs a table where one letter of the alphabet is omitted, and the letters are arranged in a 5x5 grid. Typically, the **J** is removed from the alphabet and an **I** takes its place in the text that is to be encoded. Below is an unkeyed grid. Place your secret key into the table then continue with the rest of the letters.

A	B	C	D	E
F	G	H	I	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

⇨
⇨

K	**E**	**Y**	**W**	**o**
R	**D**	A	B	C
F	G	H	I	L
M	N	P	Q	S
T	U	V	X	Z

After placing "Keyword"

1. Split letters into pairs
2. Separate all duplicate letters by inserting "x"
3. If there is an odd letter at the end insert an "x"
4. Ignore all spaces
5. Insert each pair into a separate table and use these rule to encrypt each pair:
   (1) IF in same COLUMN
   Move each letter **down** one
   Upon reaching the end of the table, wrap around
   (*Pick items below each letter*)
   (2) IF in same ROW

Move each letter **right** one
Upon reaching the end of the table, wrap around
(*Pick items to right of each letter*)

(3) IF it forms a RECTANGLE
Swap letters with the ones on the end of the rectangle
(*Pick same rows, opposite corners*)

a. Using the play fair cipher use the provided 5x5 grid and use it to encrypt your first name, and the key is your last name. Show the steps (2pts)

b. Use Cryptool to **decrypt** the secret message and compare your results. [Take screen shots from the tool] (2pts)

c. If you considered the alphabets + digits 0 – 9, how will you implement the play fair cipher? (1pt)