The Playfair Cipher Encryption Algorithm:

The Algorithm consists of 2 steps:

1. Generate the key square:

a) The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

b) The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2. Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

For example:

PlainText: "instruments"

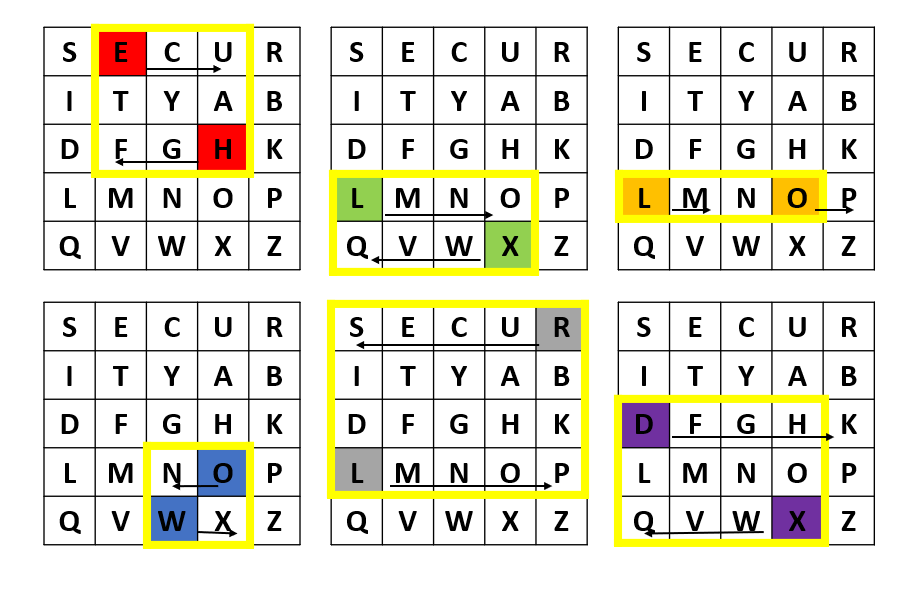
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

Plain Text: “hello”

After Split: ‘he’ ‘lx’ ‘lo’

Plain Text: “helloe”

AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ex’



Rules for Encryption:

1. If both letters in the pair are in the same row of the key square, we replace each letter with the letter to its right (wrapping around if necessary).

2. If both letters in the pair are in the same column of the key square, we replace each letter with the letter below it (wrapping around if necessary).

3. If the letters are in different rows and columns, we form a rectangle with the pair and replace each letter with the letter at the rectangle’s opposite corner (moving only left or right).

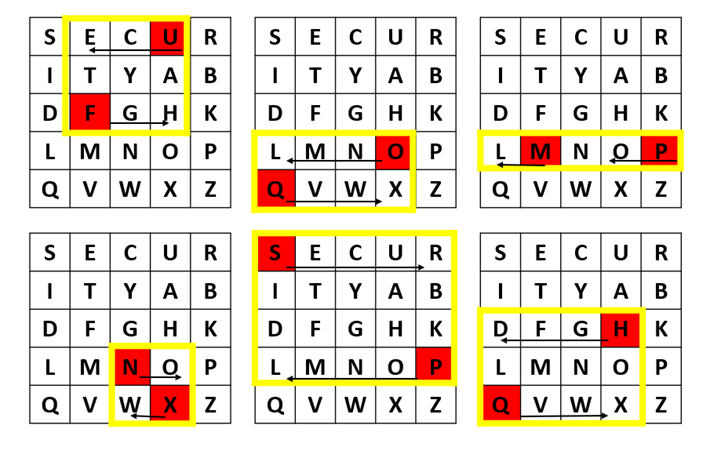
Using the matrix with the keyword SECURITY, let?s find the row and column of each pair and apply the encryption rules to HELLOWORLD, whose pairs are HE LX LO WO RL DX:

After applying the encryption rules to all the letter pairs, we get FUOQMPXNSPHQ.

Decryption rule: The decryption rules are reverse encryption rules.

Let’s decrypt the message FUOQMPXNSPHQ using these decryption rules.

The pairs are:



At this point, we have HELXLOWORLDX. After dealing with Xs, we get HELLOWORLD