PLAYFAIR CIPHER METHOD

Despite its invention by Wheatstone, it became known as the Playfair cipher after Lord Playfair, who heavily promoted its use. The first recorded description of the Playfair cipher was in a document signed by Wheatstone on 26 March 1854.

Key Generation

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order. The key can be written in the top rows of the table, from left to right. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key.

Encryption Process

To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, for example, "HelloWorld" becomes "HE LL OW OR LD", and map them out on the key table. If needed, append a "X" to complete the final digraph. The two letters of the digraph are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

Encrypt the new pair and continue. If both letters are the same (or only one letter is left), Some variants of Playfair use "X"

1. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
2. If the letters appear on the same column of your table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
3. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same **row** as the first letter of the plaintext pair.

Example

By using the playfair method encrypting the message "Hide the gold in the tree stump" use "playfair example" as the key, (assuming I and J are interchangeable).

Answer

Step 1//

Generate the key 5*5 table by write the keyword with duplicate the letter then fill the table by with the other letters in order.

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

P L A Y F A

I R E X A M PLE A

B C D EF G H I=J

K LM N O P Q R S

T U V W XY Z

Step 2

Encryption process

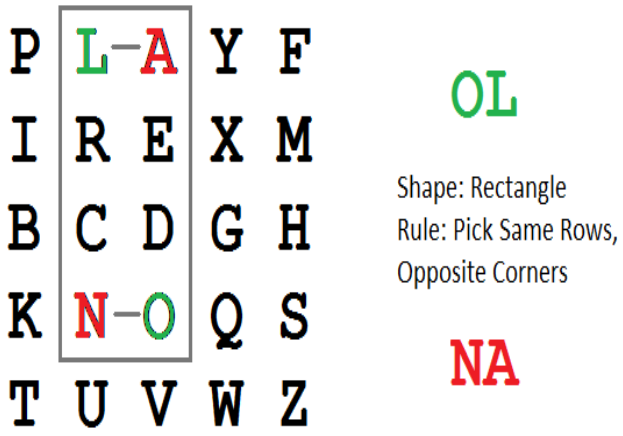
Divide the plaintext message "Hide the gold in the tree stump" in to pair of letters.

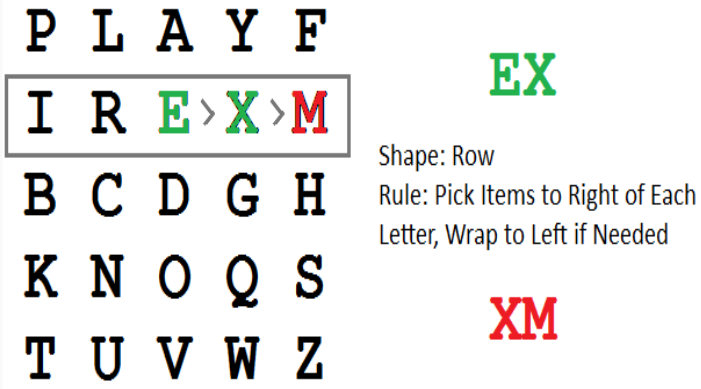
HI DE TH EG OL DI NT HE TR EE ST UM P

Add X between EE, Become

HI DE TH EG OL DI NT HE TR EX ES TU MP

1. The pair HI forms a rectangle, replace it with BM	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	HI Shape: Rectangle Rule: Pick Same Rows, Opposite Corners BM
2. The pair DE is in a column, replace it with OD	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	DE Shape: Column Rule: Pick Items Below Each Letter, Wrap to Top if Needed OD
3. The pair TH forms a rectangle, replace it with ZB	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	TH Shape: Rectangle Rule: Pick Same Rows, Opposite Corners ZB
4. The pair EG forms a rectangle, replace it with XD	P L A Y F I R E X M B C D G H K N O Q S T U V W Z	EG Shape: Rectangle Rule: Pick Same Rows, Opposite Corners XD

5. The pair OL forms a rectangle, replace it with NA	
6. The pair DI forms a rectangle, replace it with BE	
7. The pair NT forms a rectangle, replace it with KU	
8. The pair HE forms a rectangle, replace it with DM	
9. The pair TR forms a rectangle, replace it with UI	

10. The pair EX (X inserted to split EE) is in a row, replace it with XM	
11. The pair ES forms a rectangle, replace it with MO	
12. The pair TU is in a row, replace it with UV	
13. The pair MP forms a rectangle, replace it with IF	

The ciphertext of the message "Hide the gold in the tree stump" becomes

"BMODZBXDNABEKUDMUIXMMOUVIF"

Step3

Decryption Process

Ciphertext is " BMODZBXDNABEKUDMUIXMMOUVIF "

The key matrix is the same

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

1. Divide the cipher into pair as shown belw

BMODZBXDNABEKUDMUIXMMOUVIF

BM OD ZB XD NA BE KU DM UI XM MO UV IF

2. Take every pair and apply the suitable rule

BM apply the square rule becomes HI

I	M
B	H

OD apply the comlumn rule becomes DE

ZB apply the square rule becomes TH

B	H
T	Z

XD apply the square rule becomes EG

E	X
D	G

NA apply the square rule becomes OL

L	A
N	O

BE apply the square rule becomes DI

I	E
B	D

KU apply the square rule becomes NT

K	N
T	U

DM apply the square rule becomes HE

E	M
D	H

UI apply the square rule becomes TR

I	R
T	U

XM apply the row rule becomes EX

MO apply the square rule becomes ES

E	M
O	S

UV apply the row rule becomes TU

IF apply the square rule becomes MP

P	F
I	M

```
Plaintext is: HIDETHEGOLDINTHETREXESTUMP

Remove character X from the message becomes

HIDE THE GOLD IN THE TREE STUMP
```