

Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- fill rest of matrix with other letters
- e.g., using the keyword **MONARCHY**

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

Encrypting and Decrypting

- plaintext is encrypted **two letters** at a time
 1. if a pair is a repeated letter, insert filler like 'X'
 2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end) **S -> T, T -> L**
 3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom) **M -> C, E -> L**
 4. otherwise, each letter is replaced by the letter in the same row and in the column of the other letter of the pair
 5. Decrypting of course works exactly in reverse. Can see this by working the example pairs shown, backwards.

Playfair Encryption

Plain Text: "INSTRUMENTSZ"

Encrypted Text: GATLMZCLRQTX

Encryption:

I -> G

N -> A

S -> T

T -> L

R -> M

U -> Z

M -> C

E -> L

N -> R

T -> Q

S -> T

Z -> X

in:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	st:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	ru:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
me:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	nt:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	sz:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												

Playfair Decryption

Plain Text: "gatlmzclrqtz"

Decrypted Text: instrumentsz

Decryption: (red)-> (green)

ga -> in

tl -> st

mz -> ru

cl -> me

rq -> nt

tx -> sz

in:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	st:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	ru:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
me:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	nt:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z	sz:	<table border="1"><tr><td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr><tr><td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr><tr><td>E</td><td>F</td><td>G</td><td>I</td><td>K</td></tr><tr><td>L</td><td>P</td><td>Q</td><td>S</td><td>T</td></tr><tr><td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr></table>	M	O	N	A	R	C	H	Y	B	D	E	F	G	I	K	L	P	Q	S	T	U	V	W	X	Z
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												
M	O	N	A	R																																																																												
C	H	Y	B	D																																																																												
E	F	G	I	K																																																																												
L	P	Q	S	T																																																																												
U	V	W	X	Z																																																																												