

The Playfair Cipher Decryption Algorithm:

The Algorithm consists of 2 steps:

1. Generate the key Square(5×5) at the receiver's end:

- 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.
- 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 decrypt the ciphertext: The ciphertext is split into pairs of two letters (digraphs).

Note: The *ciphertext* always have **even** number of characters.

1. For example:

CipherText: "gatlmzclrqtx"

After Split: 'ga' 'tl' 'mz' 'cl' 'rq' 'tx'

1. Rules for Decryption:

- **If both the letters are in the same column:** Take the letter above each one (going back to the bottom if at the top).

For example:

Diagraph: "cl"

Decrypted Text: me

Decryption:

c -> m

l -> e

•

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

-
- **If both the letters are in the same row:** Take the letter to the left of each one (going back to the rightmost if at the leftmost position).
For example:

Diagram: "tl"

Decrypted Text: st

Decryption:

t -> s

l -> t

•

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

-
- **If neither of the above rules is true:** Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

Diagraph: "rq"

Decrypted Text: nt

Decryption:

r -> n

q -> t

•

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

•

For example:

Plain Text: "gatlmzclrqtx"

Decrypted Text: instrumentsz

Decryption:

(red)-> (green)

ga -> in

tl -> st

mz -> ru

cl -> me

rq -> nt

tx -> sz

in:

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:

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:

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:

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:

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:

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