

# PlayFair Ciphertext Encryption

Submitted by:

Vicky Kumar  
(6th Semester)

Submitted to:

Ms. Shalini Ma'am  
(Assistant Professor)  
(CSE Department)

- We encrypt a pair of alphabets instead of a single alphabet.
- It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II.

# ALGORITHM : GENERATE THE KEY MATRIX ( $5 \times 5$ )

- The key square is a  **$5 \times 5$  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  $5 \times 5$  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.

FOR EXAMPLE:

THE KEY IS "MONARCHY"

Thus the initial entries are...

'm', 'o', 'n', 'a', 'r', 'c', 'h', 'y'

...followed by remaining  
characters of

a-z (except 'j') in that order.

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

# ALGORITHM : ENCRYPT THE PLAIN TEXT

- The plaintext is split into **pairs of two letters** (digraphs).
- If there is an **odd number of letters**, then **Z** is **added** to the last letter.
- PlainText: "**instruments**"
- After Split: 'in' 'st' 'ru' 'me' 'nt' '**sz**'

## RULES 1<sup>ST</sup> FOR ENCRYPTION

*If both the letters are in the same column*

-----

Take the letter **below each one** (going back to the top if at the bottom).

For example:

Diagraph: "me"  
Encrypted Text: **cl**  
Encryption:  
    m -> c  
    e -> l

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

## RULES 2<sup>ND</sup> FOR ENCRYPTION

*If both the letters are in the same row*

---

Take the letter to the **right of each one** (going back to the leftmost if at the rightmost position).

For example:

Diagraph: "st"

Encrypted Text: **tl**

Encryption:

s → t

t → l

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

## RULES 3RD FOR ENCRYPTION

*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: "nt"

Encrypted Text: rq

Encryption:

n → r

t → q

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



# Check Output on Website

The screenshot shows a web browser with two tabs. The active tab is 'Vicks IOT Car Parking System' at the URL 'imvickykumar999.herokuapp.com/converted\_playfair\_cipher'. The page displays the results of a PlayFair cipher encryption:

- Key:** MONARCHY
- Text:** IN ST RU ME NT SZ
- Encrypted:** GA TL MZ CL RQ TX

The browser's address bar shows the URL 'imvickykumar999.herokuapp.com/converted\_playfair\_cipher'. The taskbar at the bottom shows the Windows logo, a search bar, and several application icons. The system tray on the right shows the date and time as '19-04-2021 01:22'.

On the right side of the browser, a sidebar from 'geeksforgeeks.org' is visible, showing a search bar, a menu icon, and a section titled 'Related Articles'. Below this, there is an example of PlayFair encryption:

**For example:**

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