Playfair Cipher

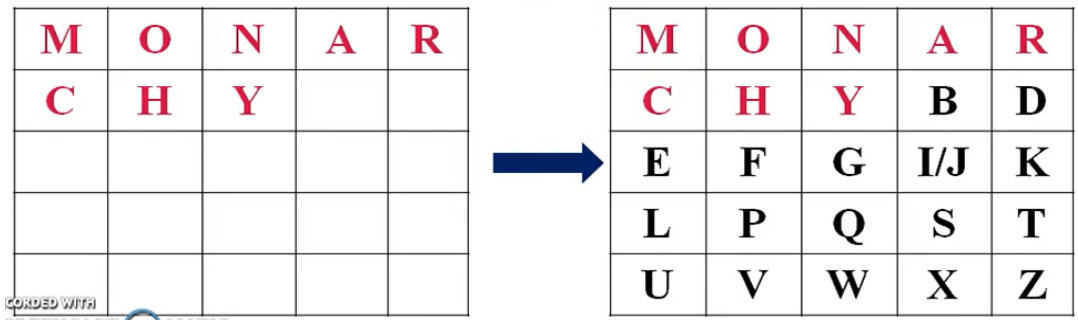
- It is aka Playfair square or Wheatstone-Playfair cipher.
- It is manual symmetric encryption technique.
- It is the first literal diagram or diagraph substitution cipher.
- Invented in 1984 by Charles Wheatstone.
- It is polyalphabetic cipher.
- It needs 5*5 matrix constructed using **a keyword** (Ex: MONARCHY).
- If the keyword has repeating letter, we should not fill more than once.
- We have to always ignore repeating letters.

Playfair Cipher -Algorithm Step 1

- **Generate the key Square (5x5):** The key square is a 5x5 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).
- The letter I and J will be consider as one letter.so If I is already placed then no need to place J in rest of matrix. (Or write I/J)
- 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,

Keyword: MONARCHY



Playfair Cipher -Algorithm Step 2

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

  For example:

  • **Plain Text**: “instruments” **After Split:** ‘in’ ‘st’ ‘ru’ ‘me’ ‘nt’ ‘sz’
- Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

  • **Plain Text:** "hello" **After Split:** ‘he’ ‘lx’ ‘lo’

  • Here 'x' is the bogus letter.

Playfair cipher- algorithms rules for encryption

1. **If the both 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 and 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

2. **If the both 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 and 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

3. **If neither of the above rules is true (If the two letters are in different rows and different columns):** 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 and 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

Solve example

Plain Text: “instruments”

In = GA

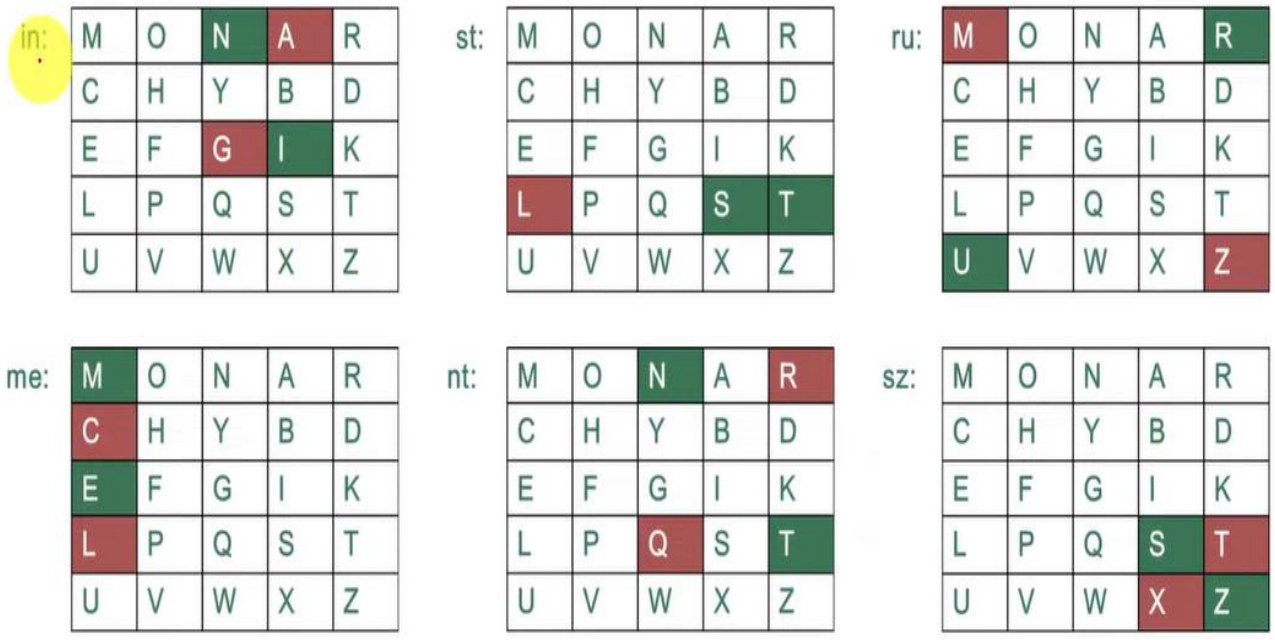
St=TL

Ru=ZM

Me=CL

Nt=RQ

Sz= TX



Cipher Text or Encrypted Text= GATLZMCLRQTX

Playfair cipher- algorithms rules for Decryption

1. **If the both 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"

   Encryption: C→ M and 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

2. **If the both 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:

Diagraph: “TL”

Decrypted text = “ST”

Encryption: T→ S and 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

3. **If neither of the above rules is true (If the two letters are in different rows and different columns):** Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Example:

Diagraph: “RQ”

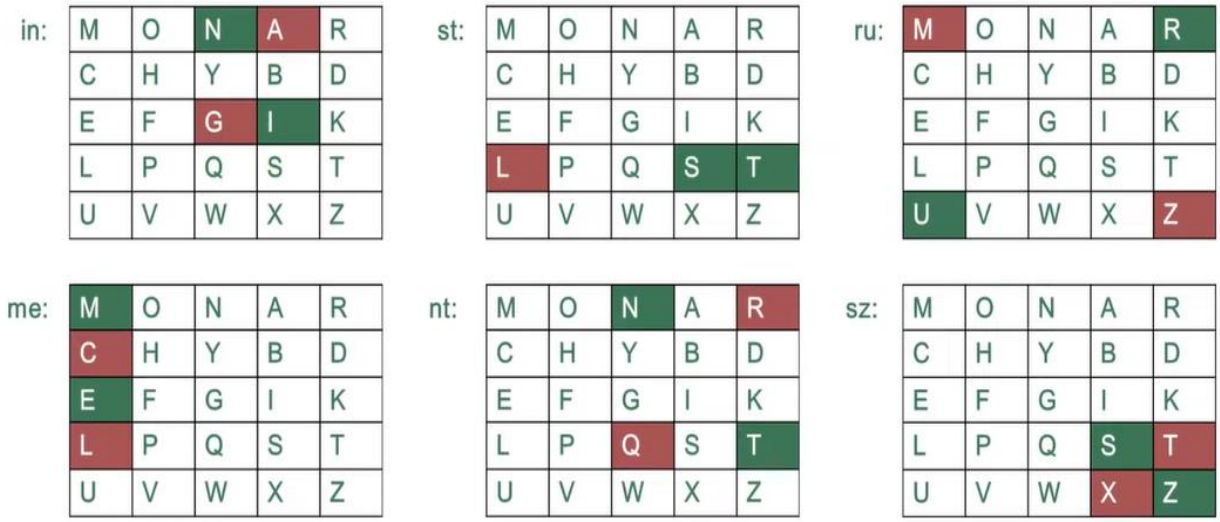
Decrypted text = “NT”

Encryption: R→ N and 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

Solve example

Cipher or encrypted Text: “GATLZMCLRQTX”



GA= **In**

TL= **St**

ZM= **Ru**

CL= **Me**

RQ= **Nt**

TX= **Sz**

So, Plain Text= instruments