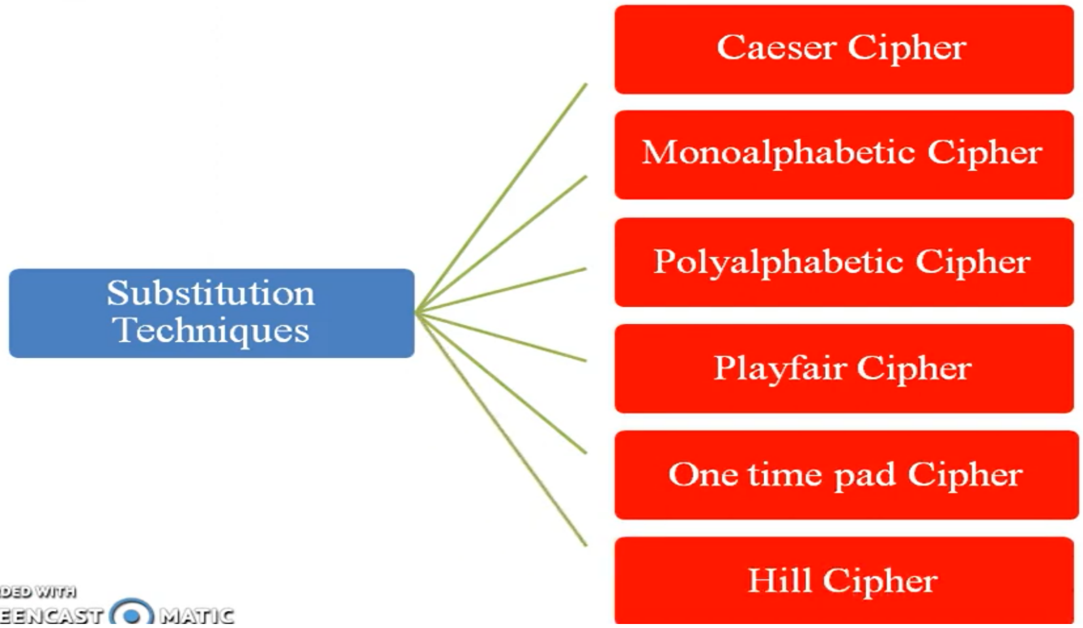
Substitution Cipher

- ❑ Types of substitution techniques:



Playfair Cipher

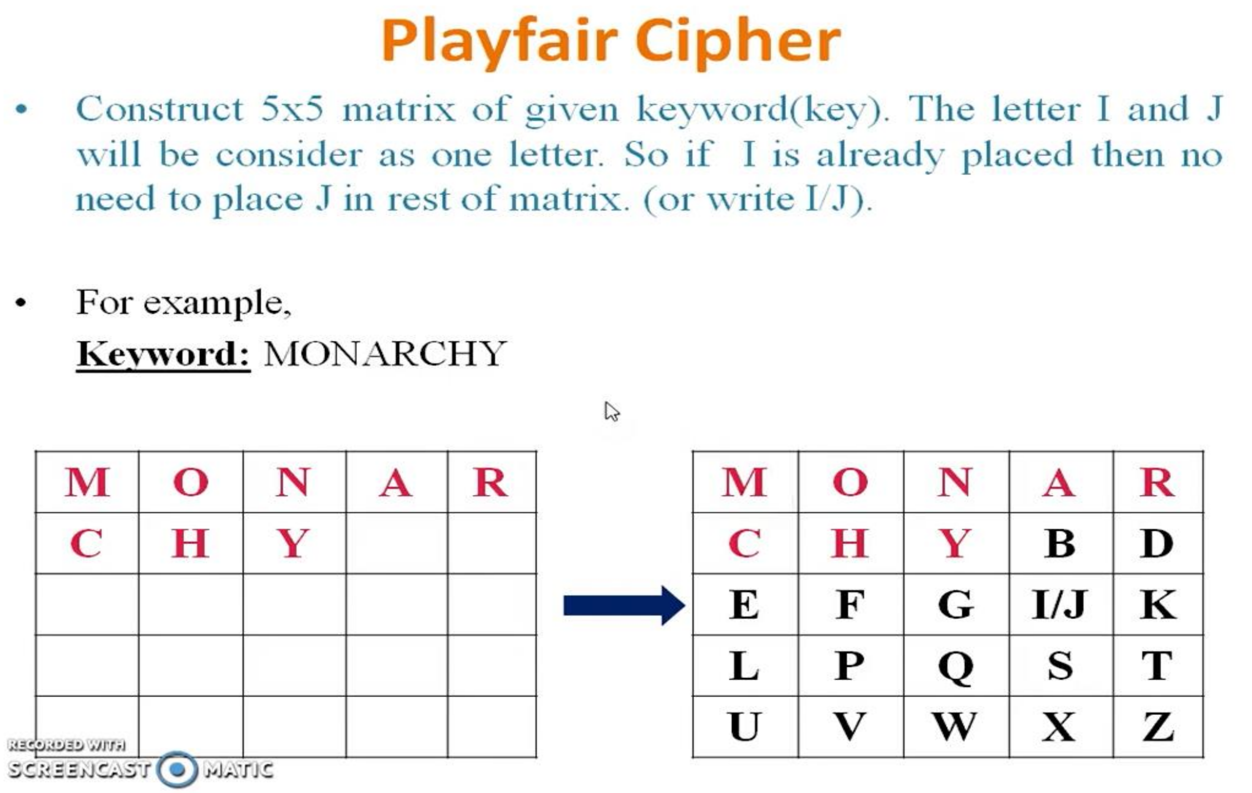
- In this cipher techniques, more than one character are used during encryption/decryption.

- So, this cipher technique is called multiple substitution cipher technique.

- Input of this technique are ***keyword*** and *plain text*.

- **Keyword** is one type of string.

- Rules of encryption is as follows:



Playfair Cipher

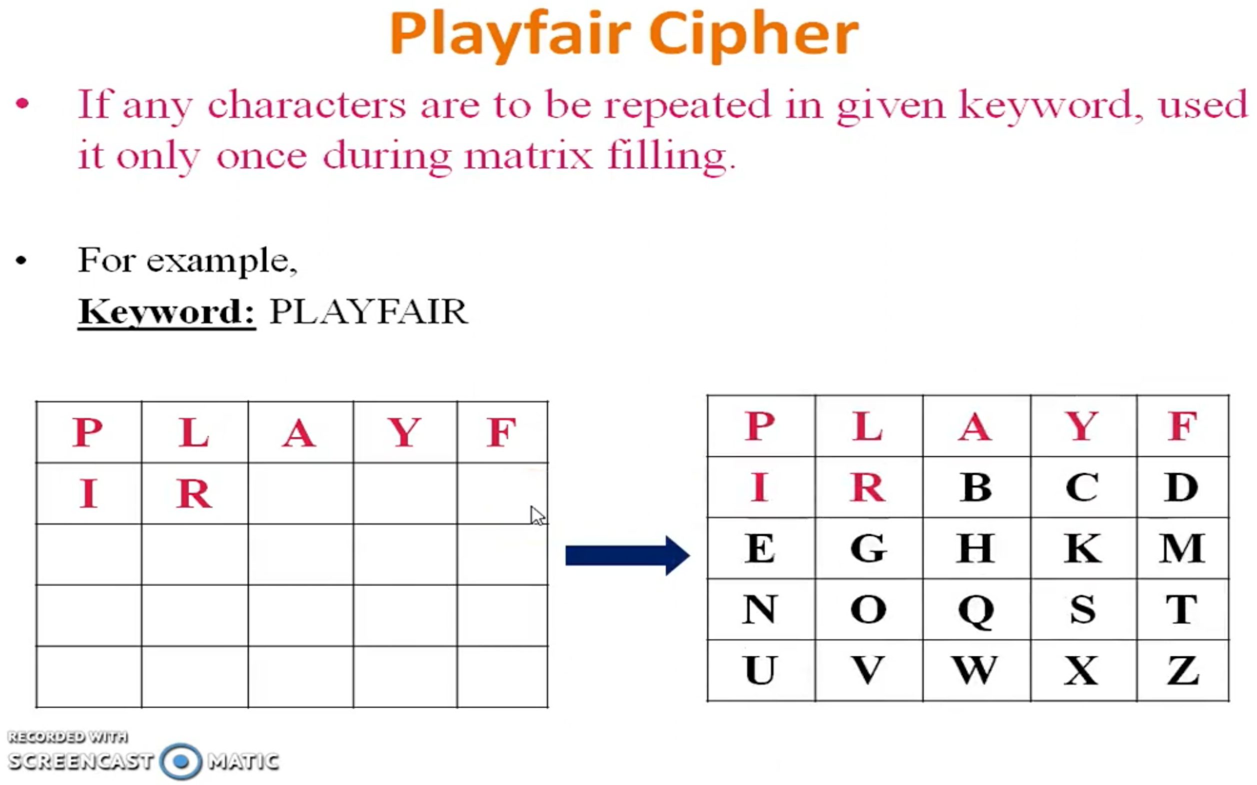
- Construct 5x5 matrix of given keyword(key). The letter I and J will be consider as one letter. So if I is already placed then no need to place J in rest of matrix. (or write I/J).

- For example,
  Keyword: MONARCHY

M	O	N	A	R
C	H	Y		

→

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



Playfair Cipher

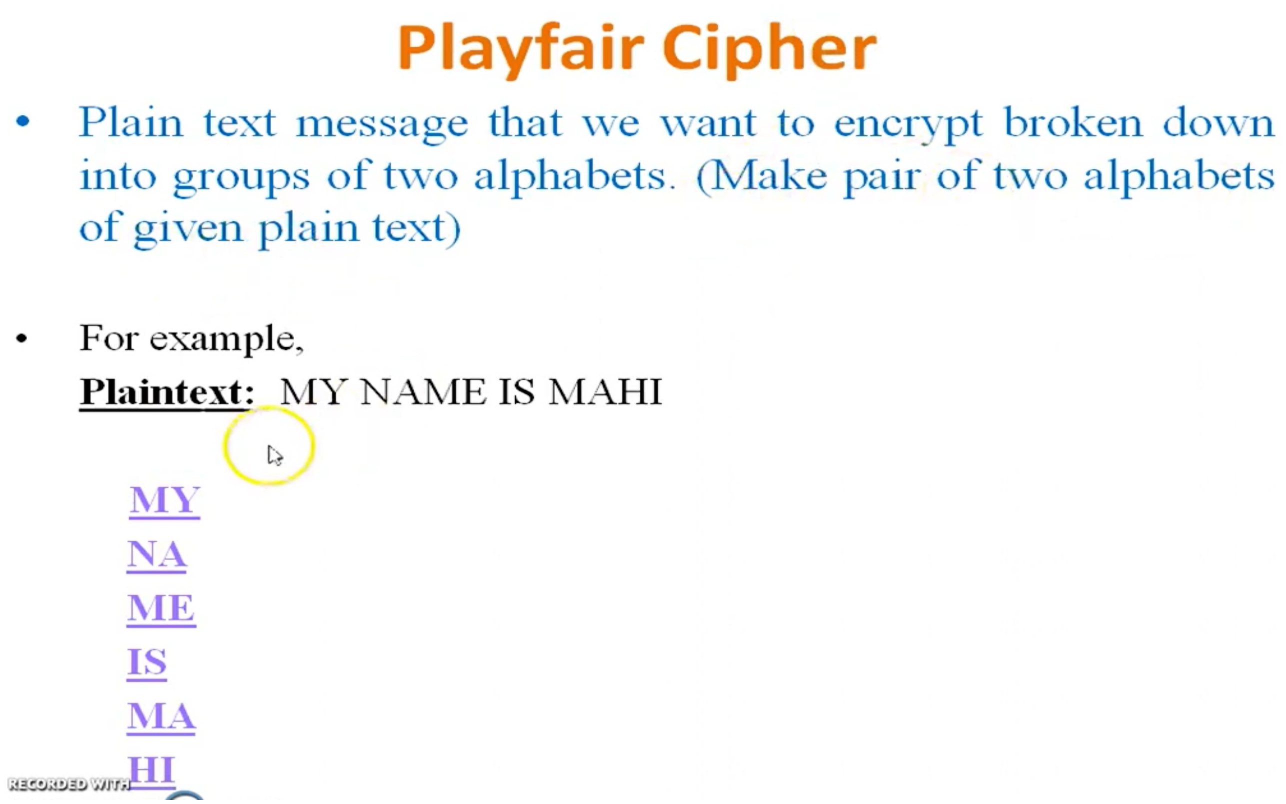
- If any characters are to be repeated in given keyword, used it only once during matrix filling.

- For example,
  Keyword: PLAYFAIR

P	L	A	Y	F
I	R			

→

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



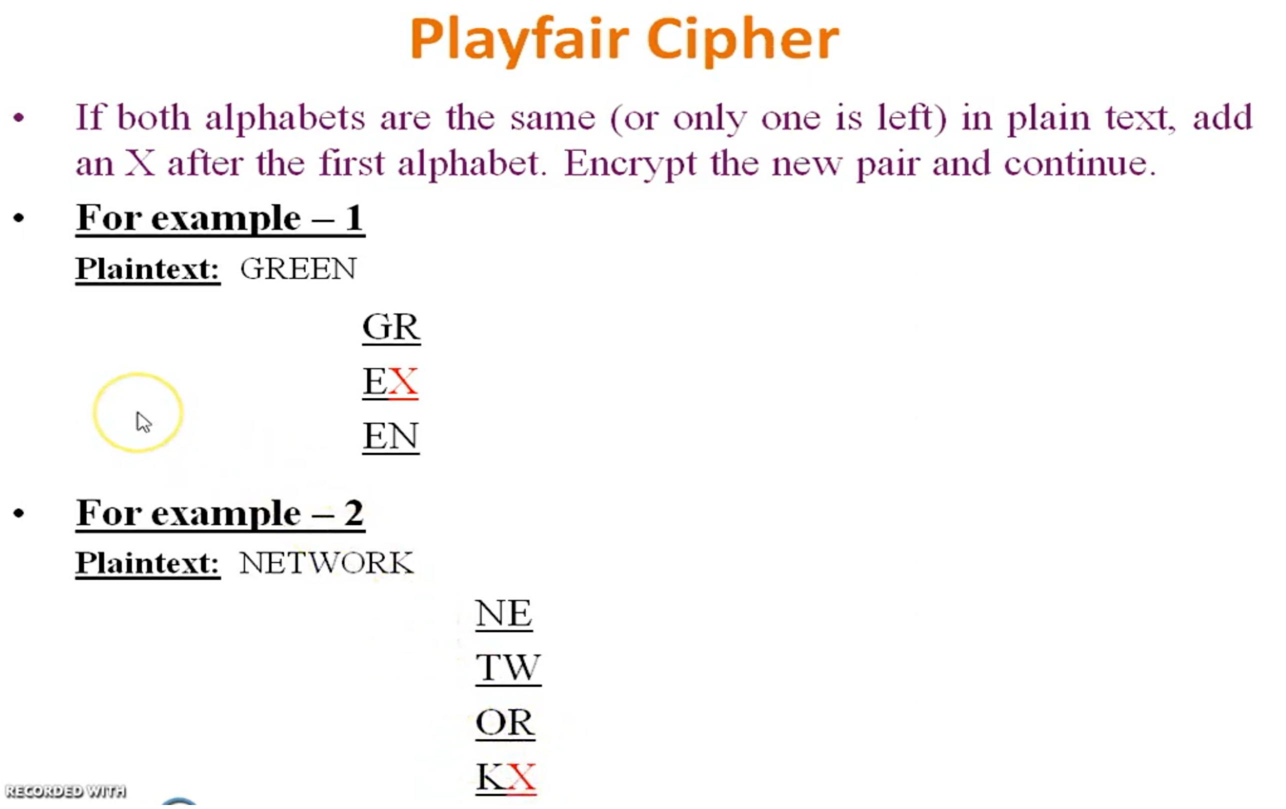
Playfair Cipher

- Plain text message that we want to encrypt broken down into groups of two alphabets. (Make pair of two alphabets of given plain text)

- For example,

  Plaintext: MY NAME IS MAHI

  MY
  NA
  ME
  IS
  MA
  HI



Playfair Cipher

- If both alphabets are the same (or only one is left) in plain text, add an X after the first alphabet. Encrypt the new pair and continue.
- **For example – 1**

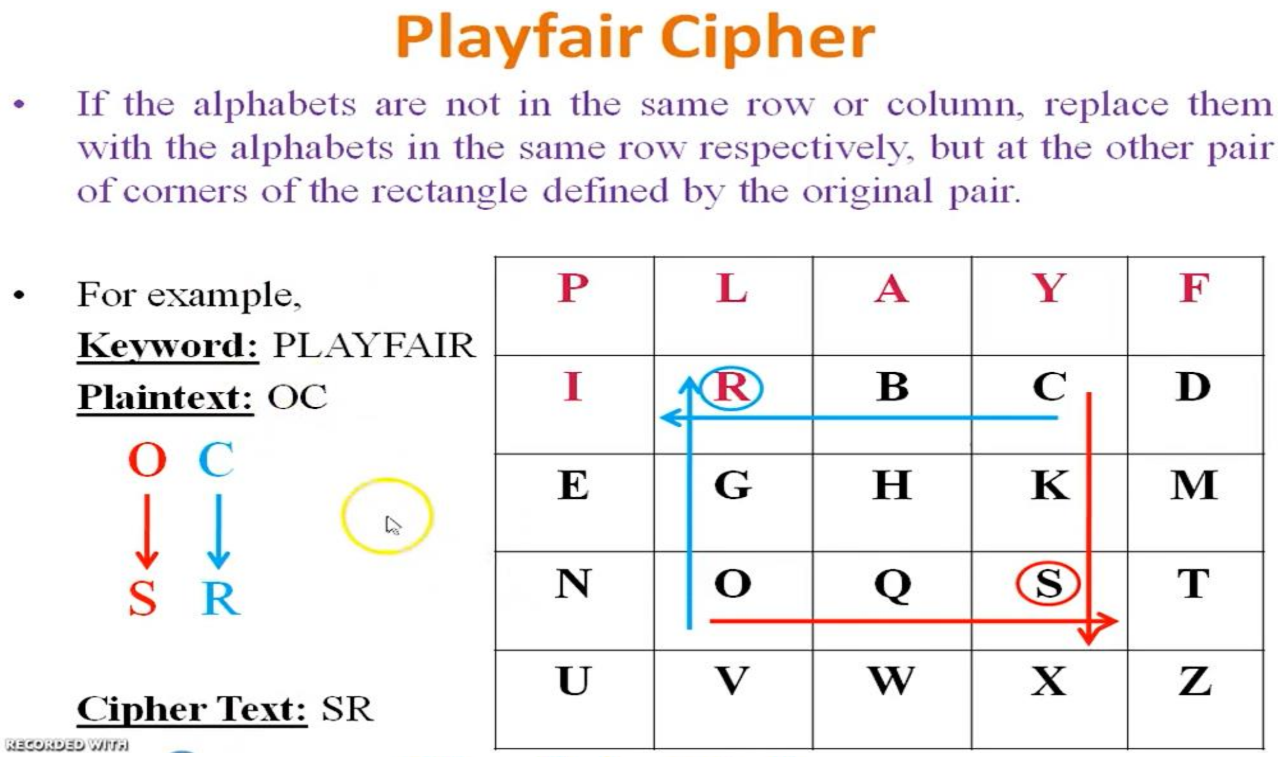
  Plaintext: GREEN

  GR
  EX
  EN

- **For example – 2**

  Plaintext: NETWORK

  NE
  TW
  OR
  KX



Playfair Cipher

- If the alphabets are not in the same row or column, replace them with the alphabets in the same row respectively, but at the other pair of corners of the rectangle defined by the original pair.

- For example,

  Keyword: PLAYFAIR

  Plaintext: OC

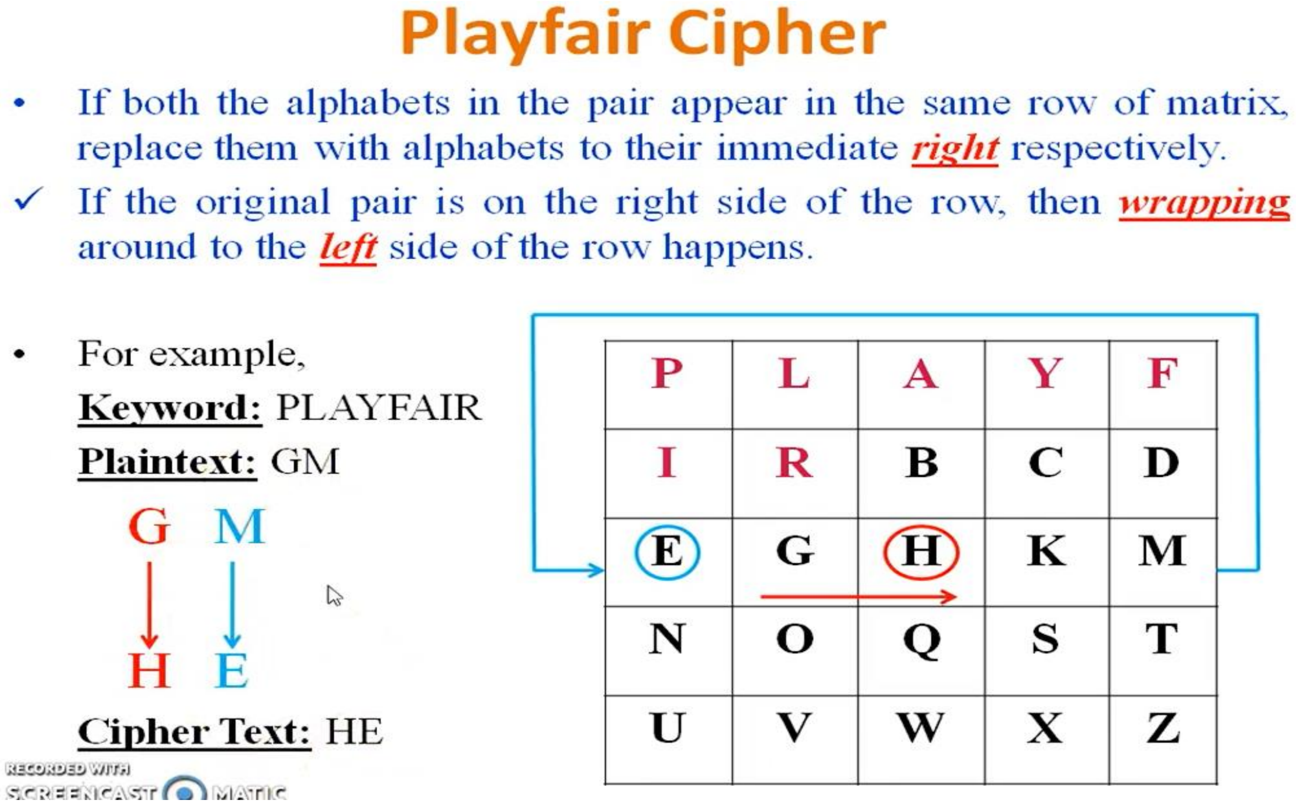
  O C

  ↓ ↓

  S R

  Cipher Text: SR

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



Playfair Cipher

- If both the alphabets in the pair appear in the same row of matrix, replace them with alphabets to their immediate ***right*** respectively.

✓ If the original pair is on the right side of the row, then ***wrapping*** around to the ***left*** side of the row happens.

- For example,

  Keyword: PLAYFAIR

  Plaintext: GM

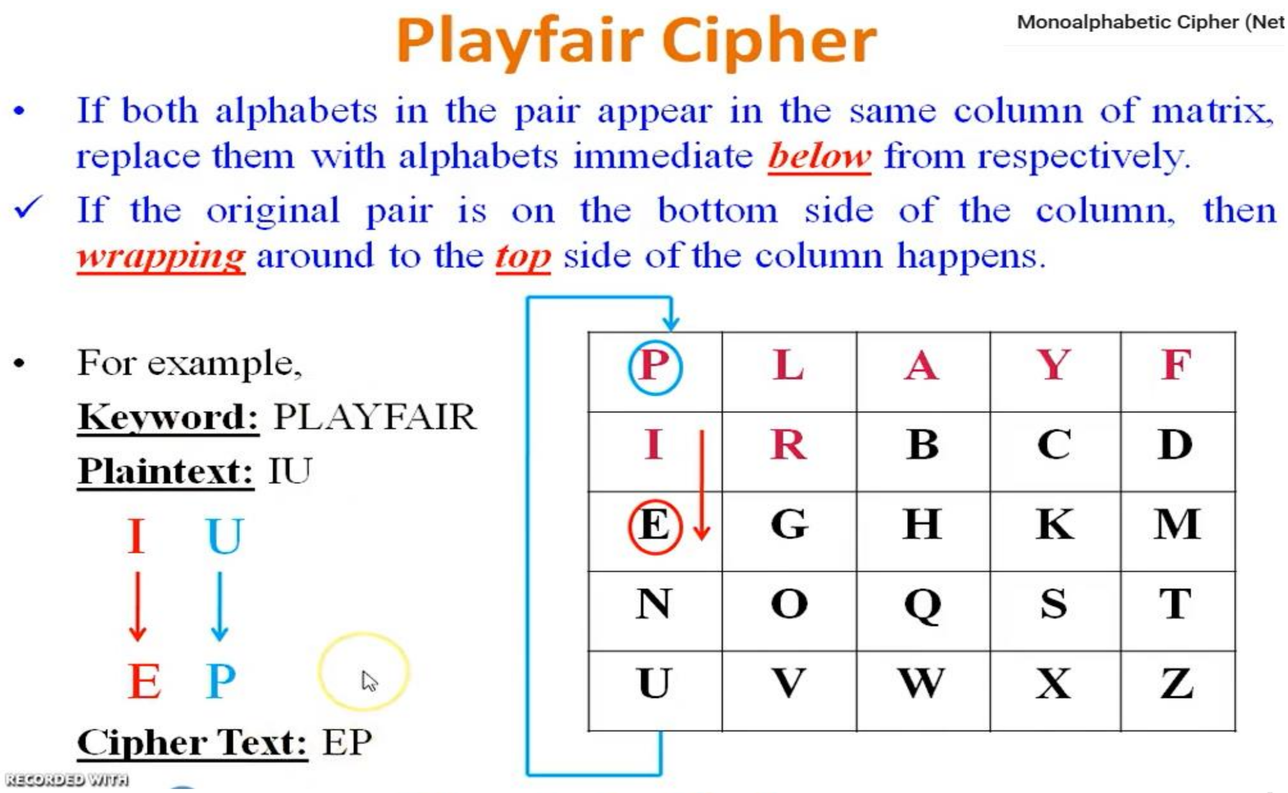
  G M

  ↓ ↓

  H E

  Cipher Text: HE

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



Monoalphabetic Cipher (Net

Playfair Cipher

- If both alphabets in the pair appear in the same column of matrix, replace them with alphabets immediate ***below*** from respectively.

✓ If the original pair is on the bottom side of the column, then ***wrapping*** around to the ***top*** side of the column happens.

- For example,

Keyword: PLAYFAIR

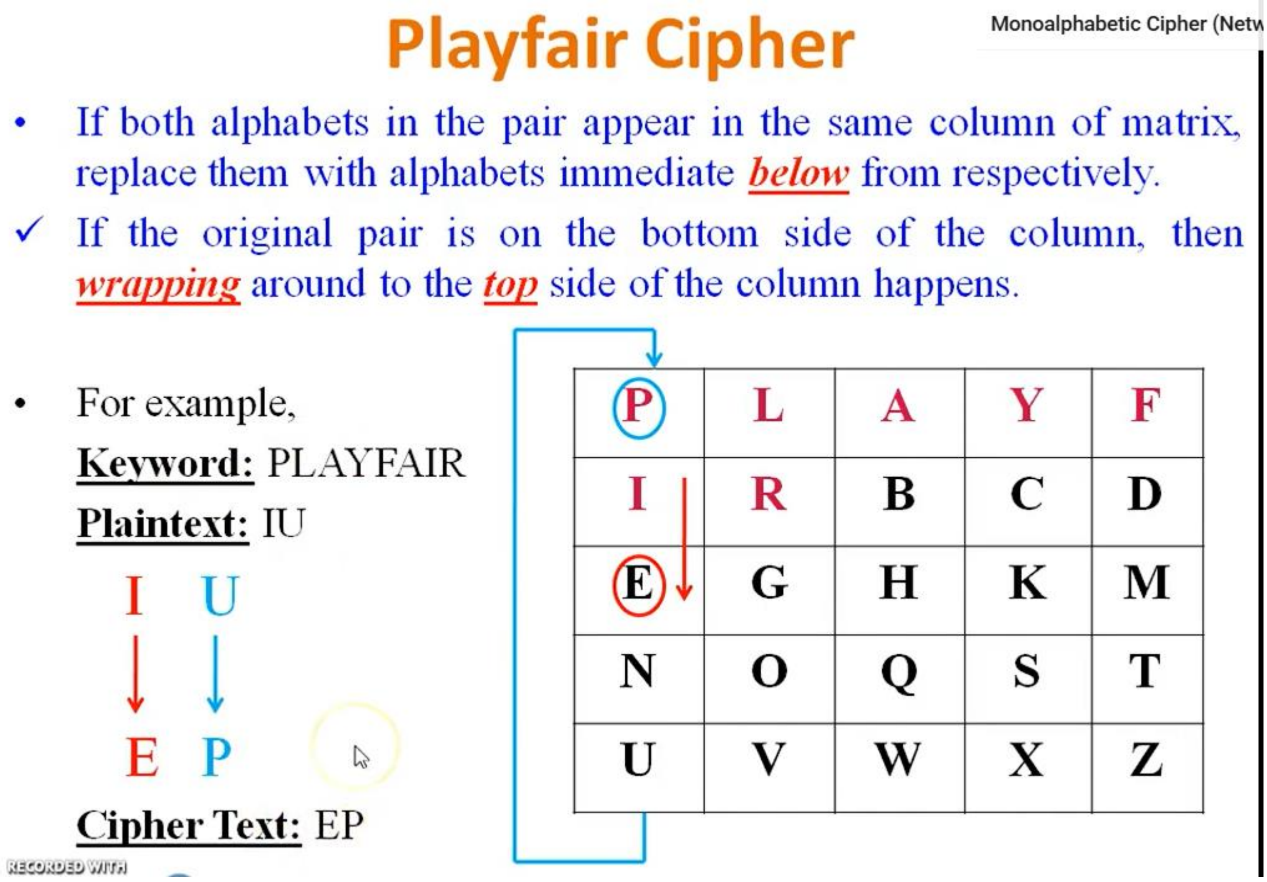
Plaintext: IU

I → E

U → P

Cipher Text: EP

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



Monoalphabetic Cipher (Netw

Playfair Cipher

- If both alphabets in the pair appear in the same column of matrix, replace them with alphabets immediate ***below*** from respectively.

✓ If the original pair is on the bottom side of the column, then ***wrapping*** around to the ***top*** side of the column happens.

- For example,

Keyword: PLAYFAIR

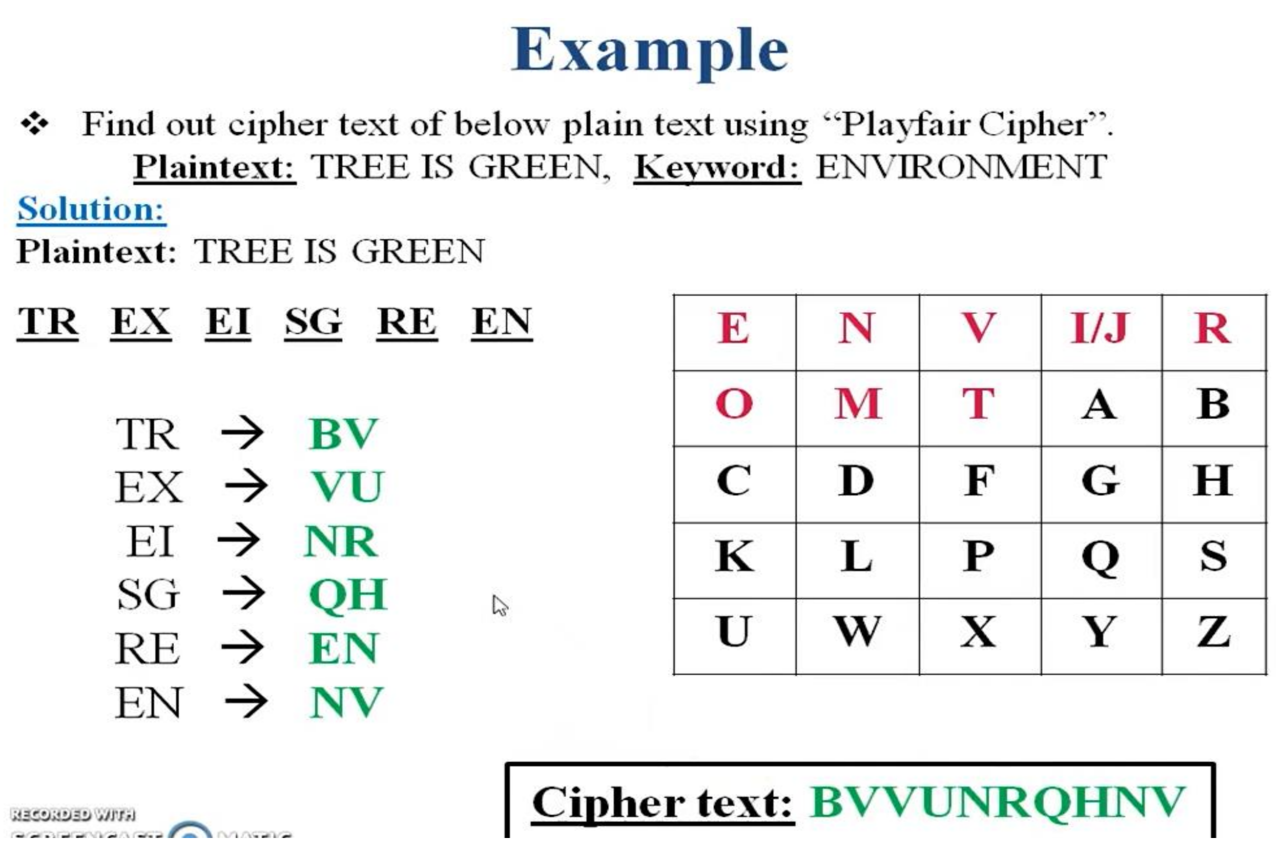
Plaintext: IU

I → E

U → P

Cipher Text: EP

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



Example

- ❖ Find out cipher text of below plain text using “Playfair Cipher”.

  Plaintext: TREE IS GREEN, **Keyword:** ENVIRONMENT

Solution:

Plaintext: TREE IS GREEN

TR **EX** **EI** **SG** **RE** **EN**

TR → **BV**
EX → **VU**
EI → **NR**
SG → **QH**
RE → **EN**
EN → **NV**

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

Cipher text: **BVVUNRQHNV**