Semester : VI Subject : CSS Academic Year: 2023-2024

## PLAYFAIR CIPHER :-

* The Playfair Cipher was the first practical digraph substitution cipher.

* The technique encrypts pair of letters (digraphs), instead of single letters as in the simple substitution cipher.

* The playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. (Frequency analysis = 25 x 25 = 625).

* 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.

Playfair Cipher Encryption Rules:

* It creates a key-table of 5x5 matrix.

* The matrix contain alphabets that act as the key for encryption of the plaintext.

Note: Any alphabets should not be repeated. There are only 25 blocks but we have 26 alphabets, so J is always combined with I.

Rules for plain Text:

* Split the plaintext into digraphs.

* If plaintext is odd numbers of letters, append the letter Z at the end of the plaintext Make the plain text even.

* If any letter appears (twice), put X at the place of the second occurrence.

Rules for matrix :-

- If a pair of letters appears in the same row, replace each letter of the digraph with the letters immediately to their right. If there is no letter to the right, consider the first letter of the same row as the right letter.
- If a pair of letters appear in the same coloumn, replace each letter of the digraph with the letters immediately below them. If there is no letter below, wrap around to the top of the same coloumn.
- If the letters are in different rows and coloumns, replace the pair with the letters on the same row respectively but at the other pair of concerns of the rectangle defined by the original pair.

Example

Encrypt "COMMUNICATE" with Playfair Cipher using key "COMPUTER".

Solution

First, split the plaintext into digraph as

CO MX MU NI CA TE

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

5x5 key matrix.

CO → CO will be replaced with OM

MX → MX will be replaced with RM.

MU → MU will be replaced with PC.

NI → NI will be replaced with SG.

CA → CA will be replaced with PT.

TE → TE will be replaced with ER.

The encryptext text is OMRMPCSGPTER.

Semester : VI  Subject : CSS  Academic Year: 2023-2024.

Example - 2 :-

Encrypt "THIS IS THE FINAL EXAM" with Playfair Cipher using the key "GUIDANCE".

Solution :-

First, split the plaintext into digraph as:

TH IS IS TH EF IN AL EX AM.

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

5x5 key matrix.

TH → TH is encrypted to PO.

IS → JS is encrypted to DR.

IS → JS is encrypted to DR.

TH → TH is encrypted to PO.

EF → EF is encrypted to BN.

IN → IN is encrypted to GE.

AL → AL is encrypted to IO

EX → EX is encrypted to LI.

AM → AM is encrypted to DO.

The encrypted text is PODRDRPOBNGEIOLIDO.