Topic- 8

__/__/__

* Playfair Cipher

→ It was the first practical digraph substitution cipher.
(a Pair of two letters)

→ It is an encryption algorithm to encrypt or encode an message.

→ It is same as traditional cipher. The only difference is that it encrypts a pairs of Letters instead of single Letters.

• Encryption Technique:- for the encryption process let us consider the following example:-

Key :- mon

PlainText :- instruments

→ The algorithm consists of 2 steps :-

1. Generate the key Square (5x5) :-

In Playfair cipher, initially a key table is created. The key table 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)

→ If the Plaintext contains J, it is replaced by I.

(ii) Algorithm to encrypt the Plain Text:-

→ The Plaintext is split into pairs of two letters.

→ If there is an odd numbers of letter, a Z is added to last letter.

For example:-

Plain Text: "jpweb"
After Split:- 'jp' 'we' 'bz'

① Pair cannot be made with same letters. break the letters in single and add 'x' to the previous letter.

↑ bogus letter

For example:-

plain Text:- "hello"
After Split:- 'he' 'lx' 'lo'
→ x is bogus letter.

② If the letter is standing alone in the process of pairing, then add an extra bogus letter (z) with the alone letter.

for example :- plainText :- "helloe"
After Split :- 'he' 'lx' 'lo' 'lz'

→ z is the bogus letter.

• Rules for Encryption :-

(1) If both the letters are in the same column :- It replace them with alphabets immediatly below them.

For example :-

Diagraph : "me"
Encrypted Tet : 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

___/___/___

(II) If both the letters are in the same row:-

→ It replace them with alphabets to their immediate right.

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

(iii) If not in Same row/ Column :- It replace them with alphabets in same row respectively,

→ form a rectangle with the two letters and take the letters on the horizental opposite corner of the rectangle..

for example:-

Diagraph : "nt"

Encrypted Text: rq

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