Sai Ram
20181CSE0621

02/06/2021

20181CSE0621
Sai Ram.K
6-CSE-10

Part-B

Q.2] **PLAY-FAIR CIPHER:-**

- It is the best known multi-letter encryption cipher which treats diagrams in the plaintext as single units and translates these units into ciphertext diagrams.
- It is based on 5x5 matrix of ~~two~~ letters constructed using a keyword.
- For example, Keyword : Security
  Plaintext : Pattern

In this case the keyword is security. The matrix is constructed by filling in the letters (no duplicates) from left to right & top to bottom, & filling the remaining with the other alphabets

NOTE: Letters i & j count as one letter.

--> **MATRIX:-**

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

The rules for encryption is that two letters are paired together according to the following rule

BALLOON => BA LX LO ON

* We add the letter 'x' as a filler in case of repeating letters

20181CSE0621
Sai Ram

→ SENARIO OF 3 Cases:-

1] Repeating plaintext letters that are in the same pair are seperated with a filler letter such as 'x' so that pattern will be treated as "pa tx te rn".

2] Two plaintext letters that fall in the same row of the matrix are replaced by a letter to the right, with the first element of the row circularly following the last. For Eg:

OP is encrypted as PL

3] Two plaintext letters that fall in the same column are replaced by the letter beneath, with top element circularly following the last. For Eg:

MV is encrypted as VE.