Cryptography : Playfair Cipher

Tutorial Problem

Generate the key Square(5×5):

The key square is a 5×5 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, then it is replaced by I.

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:

The key is "monarchy"

Thus the initial entries are

'm', 'o', 'n', 'a', 'r', 'c', 'h', 'y'

followed by remaining characters of

a-z(except 'j') in that order.

Key Square

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

Algorithm to encrypt the plain text

The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

If a character is repeated, include ‘x’ for second occrrence of that character.

For example:

PlainText: "instruments"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

Rules for Encryption:

If both the 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

e -> l

Rules Contd...

If both the 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

t -> l

Rules Contd..

If neither of the above rules is true: 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

t -> q

Example

For example:
Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx
Encryption:

i -> g
n -> a
s -> t
t -> l
r -> m
u -> z
m -> c
e -> l
n -> r
t -> q
s -> t
z -> x