Practical Number 2

Aim: To implement Playfair Cipher.

Theory:

Playfair cipher was invented by Charles Wheatstone in 1854, and was used by US and British army during World War I. It is a Polyalphabetic cipher in which the relationship between a character in the plaintext to a character in the ciphertext is one-to-many; each occurrence of a character in the plaintext may have a different substitute. They have the advantage of hiding the letter frequency of the underlying language. Each ciphertext character depends on both the corresponding plaintext character and the position of the plaintext character in the message. Playfair is a block cipher in which the block size is fixed as two.

The secret key is made of 25 alphabet letters arranged in a 5 x 5 matrix. The letters I and J are considered the same when encrypting/decrypting. The plaintext is divided into blocks of two characters each. The algorithm works as follows:

1. If a pair is a repeated letter, insert a filler like 'X', example "balloon" encrypts as "ba lx lo on".
2. If both letters fall in the same row, replace each with letter to right (wrapping back to start from end).
3. If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom).
4. Otherwise each letter is replaced by the one in its row in the column of the other letter of the pair.

Cryptanalysis of Playfair cipher: The size of the key domain is 25! , hence a brute force attack is very difficult. It hides the single letter frequency of the character. However, the frequencies of the diagrams are preserved; have 26 x 26 = 676 diagrams. A ciphertext only attack based on the diagram frequency test can be carried out.

Example: Encrypt the plaintext “hello” using the following key matrix

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

The plaintext hello is divided into 3 blocks of size 2 as he lx lo

he → **EC**
lx → **QZ**
lo → **BX**

hello → ECQZBX

Reversing the process to decrypt the ciphertext we get **ECQZBX → hello**

Conclusion: Playfair cipher has been studied and implemented