Pre Lab:-

1. Define diagram with an example.
A diagram in cryptography refers to the grouping of letters, typically pairs (digraphs) for encryption. For example, in the Playfair cipher, the message "HELLO" becomes "HE LL O" and then "HE LX LO" to form digraphs.

2. What is the reason to consider a 5 × 5 matrix in a Playfair cipher technique?
The 5x5 matrix holds 25 letters of the alphabet (combining 'I' and 'J'), ensuring that every letter in the English alphabet is assigned a position in the matrix for encryption.

3. What to do if letters in plaintext reoccur eg: Hello?
If letters in a digraph reoccur (e.g., "LL" in "HELLO"), an extra character like 'X' is inserted between them, turning "LL" into "LX".

4. What are the advantages of Playfair cipher?
The Playfair cipher encrypts digraphs instead of individual letters, making frequency analysis harder. It's simple, easy to implement, and provides more security than monoalphabetic ciphers.

5. Trace what will be the encrypted message by using Playfair cipher if the message is 'balloon' and the key is "Monarchy".
Using the key "Monarchy", the 5x5 matrix is:

M O N A R

C H Y B D

E F G I/J K

L P Q S T

U V W X Z

Message: "BALLOON" becomes "BA LX LO ON".

- BA -> EN (row rule)
- LX -> NA (rectangle rule)
- LO -> MU (rectangle rule)
- ON -> RO (row rule)
  Encrypted message: "EN NAM URO".

VIVA:-

1. Briefly explain the Playfair Cipher and its basic principles.
The Playfair cipher is a digraph substitution cipher that encrypts pairs of letters from the plaintext. It uses a 5x5 matrix of letters created from a key phrase, where letters are substituted based on their positions in the matrix, making cryptanalysis more difficult than monoalphabetic ciphers.

2. How are the Playfair Cipher's key matrix and key phrase related?
The key matrix is constructed from the key phrase by removing duplicate letters and placing them in a 5x5 grid, followed by the remaining letters of the alphabet (combining 'I' and 'J') to fill the matrix.

3. What steps are involved in encrypting a message using the Playfair Cipher?

1. Split the plaintext into digraphs (pairs of letters), adding filler letters like 'X' if necessary.
2. Locate the two letters of each digraph in the matrix.
3. Encrypt according to the Playfair rules: same row (shift right), same column (shift down), or rectangle rule (swap corners).

4. How is the Playfair Cipher decrypted?

Decryption follows the same steps as encryption but shifts left (for same row) and shifts up (for same column) instead. The rectangle rule remains the same, swapping corners.

5. Discuss any limitations or weaknesses of the Playfair Cipher.

The Playfair cipher is vulnerable to frequency analysis of digraphs and patterns in digraphs can reveal information. Also, the use of only 25 letters (merging 'I' and 'J') limits its versatility, and it's less secure against modern cryptanalysis methods.