Pre Lab:-

1. What is the basic principle behind the Hill cipher?
The Hill cipher is a polyalphabetic cipher that uses linear algebra and matrix multiplication to encrypt and decrypt blocks of letters from the plaintext.

2. How does the key matrix affect encryption and decryption in the Hill cipher?
The key matrix is multiplied by the plaintext vector to produce the ciphertext; decryption involves using the inverse of the key matrix to retrieve the original plaintext.

3. What are the advantages of the Hill cipher over monoalphabetic substitution ciphers?
The Hill cipher provides more security by encrypting multiple letters at once, making frequency analysis attacks harder compared to monoalphabetic ciphers that encrypt each letter individually.

4. What are the key requirements for a key matrix in the Hill cipher?
The key matrix must be invertible, meaning its determinant should be non-zero and relatively prime to the size of the alphabet, ensuring decryption is possible.

5. How does the Hill cipher handle spaces and punctuation in plaintext?
Typically, spaces and punctuation are removed or encoded as special characters before encryption, as the Hill cipher primarily operates on alphabetic characters.

VIVA:-

1. What are the vulnerabilities of the Hill cipher?
The Hill cipher is vulnerable to known-plaintext attacks and frequency analysis due to its linear nature, which can be exploited if enough plaintext-ciphertext pairs are known.

2. Can the Hill cipher be used for encryption of digital data like images or files?
Yes, the Hill cipher can be adapted for digital data by treating data blocks as vectors, but it is not practical for large data due to its susceptibility to modern cryptanalysis.

3. How does the Hill cipher compare in terms of computational complexity with modern encryption algorithms like AES?
The Hill cipher is less complex than AES, which uses advanced algorithms and key management for robust security. AES provides higher security and efficiency for modern encryption needs.

4. What are some practical applications of the Hill cipher today?
The Hill cipher is mostly used for educational purposes to demonstrate matrix operations and cryptographic principles rather than for practical encryption.

5. What improvements or modifications can be made to enhance the security of the Hill cipher?
Enhancements can include using larger matrices for increased security and combining the Hill cipher with other cryptographic techniques to strengthen overall encryption.