SSN College of Engineering,
Department of Computer Science and Engineering
CS6711 Security Laboratory

Exercise 2a:

To implement the substitution technique: Hill Cipher

Hints:

Encryption Procedure for Hill Cipher:

E: C= KP mod 26

1. Read the plain text message
2. Read the key (a square matrix, say order of $n \times n$)
3. Split the plain text into chunks of size n, convert them into their numerical equivalent and form a columnar matrix.
4. Perform matrix multiplication on K and plain text vector mod 26.
5. Generate cipher text by decoding the outcome of step 4 into equivalent alphabets.
6. Display the cipher text.

Decryption Procedure for Hill Cipher:

D: P= K^{-1}C mod 26

1. Use the cipher text as input
2. Compute the inverse matrix of K, that is K^{-1}
3. Encode the cipher text into their numerical equivalent and form a columnar matrix with respect to the order of K^{-1}.
4. Perform matrix multiplication on K^{-1} and cipher text vector mod 26.
5. Retrieve plain text by decoding the outcome of step 4 into equivalent alphabets.
6. Display the plain text.