PES UNIVERSITY

LINEAR ALGEBRA PROJECT

TITLE: CRACKING THE CODE USING HILL CIPHER

Description

TEAM MEMBERS:

NAMES:	SRN:
Sanath N Bhargav	PES1UG20CS372
Sarang J Chilkund	PES1UG20CS387
Sathwick P	PES1UG20CS388
Samarth Rajendra	PES1UG20CS370

HILL CIPHER

Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The stages of the Hill Cipher encryption algorithm are as follows :

1. Organize character alphabetically with numeric A → 1, B → 2, ..., Z → 26 or in ASCII (256 characters)

2. Create a key matrix measuring m x m

$$K_{mxm} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

3. Matrix K is an invertible matrix that has multiplicative inverse K−1 so that K. K−1 = 1

4. Plaintext P = p1 p2 ... pn, blocked with the same size as the row or column column K

$$P_{qxm} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ p_{q1} & p_{q2} & \cdots & p_{qm} \end{bmatrix}$$

5. Transpose matrix P and became

$$P^{t}_{mxq} = \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{1q} \\ p_{12} & p_{22} & \cdots & p_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1m} & p_{2m} & \cdots & p_{qm} \end{bmatrix}$$

6. Multiply matrix K with transposed P in modulo 26 or 256

$$C^t = K_{m \times m} P^t_{m \times q}$$

$$C^t = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix} \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{1q} \\ p_{12} & p_{22} & \cdots & p_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1m} & p_{2m} & \cdots & p_{qm} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{21} & \cdots & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ c_{1q} & c_{2q} & \cdots & c_{mq} \end{bmatrix}$$

7. Then transpose to

$$C = (C^t)^t = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1q} \\ c_{21} & c_{22} & \cdots & c_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mq} \end{bmatrix}$$

8. Change the result of step 7 into the alphabet using alphabetical correspondence with numeric in step 1 to obtain the ciphertext