HACETTEPE UNIVERSITY DEPARTMENT OF

COMPUTER ENGINEERING

BBM 456 HOMEWORK 4

Mehmet Taha USTA – 21527472

Subject: What is Hill Cipher ? How does it work ? Give an example

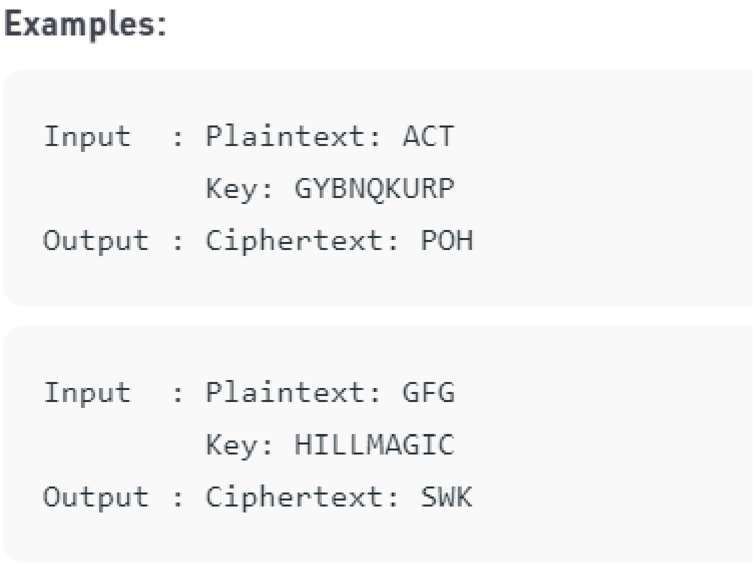
Hill Cipher Definition & Working Principle

Hill cipher is one of the primitive encryption algorithms. In this method, block cipher is used. In other words, the plain text to be encrypted is divided into blocks of plain text and the block is encrypted. The character value in the text is multiplied with the key given for each block. The new results are obtained by adding the obtained results.

Places the text to be encrypted in the matrix and creates a random element matrix. Then it multiplies these two matrices and by searching the formed matrix in the alphabet sequence, the encrypted text is obtained.

Invented by Lester S. Hill in 1929, the Hill cipher is a **polygraphic substitution cipher** based on linear algebra. Hill used matrices and matrix multiplication to mix up the plaintext. To counter charges that his system was too complicated for day to day use, Hill constructed a cipher machine for his system using a series of geared wheels and chains. However, the machine never really sold.

Hill's major contribution was the use of mathematics to design and analyse cryptosystems. It is important to note that the analysis of this algorithm requires a branch of mathematics known as number theory. Many elementary **number theory** text books deal with the theory behind the Hill cipher, with several talking about the cipher in detail.



Examples:

```
Input  : Plaintext: ACT
         Key: GYBNQKURP
Output : Ciphertext: POH
```

```
Input  : Plaintext: GFG
         Key: HILLMAGIC
Output : Ciphertext: SWK
```

Encryption

We have to encrypt the message ‘ACT’ (n=3).The key is ‘GYBNQKURP’ which can be written as the nxn matrix:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

The message ‘ACT’ is written as vector:

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \pmod{26}$$

which corresponds to cipher text of ‘POH’

Decryption

To decrypt the message, we turn the cipher text back into a vector, then simply multiply by the inverse matrix of the key matrix (IFKVIVVMI in letters). The inverse of the matrix used in the previous example is:

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \pmod{26}$$

For the previous Cipher text ‘POH’:

$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

which gives us back ‘ACT’.

Assume that all the alphabets are in upper case.

Below is the implementation of the above idea for n=3.