LINEAR ALGEBRA AND ITS APPLICATIONS

Hill Cipher

By:-

- Susmita Kypa PES2UG20CS361
- Vinti Agrawal PES2UG20CS385
- Vishwa Mehul Mehta PES2UG20CS389
- Vismaya R PES2UG20CS391

Hill Cipher

Hill cipher is a polygraphic substitution cipher based on linear algebra.

Encryption and Decryption

Suppose we have an invertible matrix A (the encoding matrix) and a text we want to encrypt. Transform the text to a sequence of numbers by giving each character a unique numerical value, then split the numbers to form a matrix by grouping the numbers into columns according to the order of the matrix A (the amount of elements in each column must be equal to the order of the matrix). Let's call this matrix B (the plain matrix). Multiply the matrix A by the matrix B:

$C = A \cdot B$

The matrix C is the cipher matrix. To decrypt the message, just multiply $Inv(A) \cdot C$, where $Inv(A)$ is the inverse matrix of A.

$Inv(A) \cdot C = Inv(A) \cdot A \cdot B = I \cdot B = B$

Example:

The password is: NCS-2014

First, we must assign each letter a numeric equivalent. As state above, we'll use the Unicode number for each character. For the message to encrypt, we get the following sequence of numbers:

84 104 101 32 112 97 115 115 119 111 114 100 32 105 115 58 32 78 67 83 45 50 48 49 52

Coding matrix:

We choose the following 4x4 invertible matrix A:

$$A = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 2 & -3 & -5 & 4 \\ -2 & -1 & -2 & 2 \\ 3 & -3 & -1 & 2 \end{bmatrix}$$

Example:

Encrypting the message:
We convert the sequence of numbers related to plaintext into a matrix, splitting it into column vectors of 4 elements (the order of the encoding matrix). We fill out the last column with zeros as necessary to complete the 4 elements.

$$B = \begin{bmatrix} 84 & 112 & 119 & 32 & 32 & 45 & 52 \\ 104 & 97 & 111 & 105 & 78 & 50 & 0 \\ 101 & 115 & 114 & 115 & 67 & 48 & 0 \\ 32 & 115 & 100 & 58 & 83 & 49 & 0 \end{bmatrix}$$

Example:

We now encode the message by multiplying the encoding matrix A by the above matrix B. The result is the cipher matrix C:

$$C = A \cdot B = \begin{bmatrix} -89 & 15 & -6 & -130 & -30 & -4 & 52 \\ -521 & -182 & -265 & -594 & -173 & -104 & 104 \\ -410 & -321 & -377 & -283 & -110 & -138 & -104 \\ -97 & 160 & 110 & -218 & -39 & 35 & 156 \end{bmatrix}$$

The columns of this matrix give the encoded message. The message could be transmitted in the following linear form:

-89 -521 -410 -97 15 -182 -321 160 -6 -265 -377
110 -130 -594 -283 -218 -30 -173 -110 -39 -4
-104 -138 35 52 104 -104 156

Example:

Decrypting the message:

To decode the message, write the sequence of numbers you received as a matrix, by splitting the numbers into column vectors of 4 elements. The resulting matrix from this process will be equal to the cipher matrix C. You must know the inverse of the encoding matrix:

$$\mathrm{Inv}(A) = \begin{bmatrix} 6 & -1 & 0 & -1 \\ 22 & -4 & 1 & -4 \\ 14 & -3 & 1 & -2 \\ 31 & -6 & 2 & -5 \end{bmatrix}$$

Multiply that matrix (decoding matrix) by the cipher matrix C. Form back the resulting matrix (it'll be equal to matrix B) into a continuous sequence of numbers and map the numbers to their corresponding characters, to get the original message.

Applications

1. cash withdrawal from an ATM
2. secure web browsing
3. email and file storage using Pretty Good Privacy (PGP) freeware

THANK YOU!!