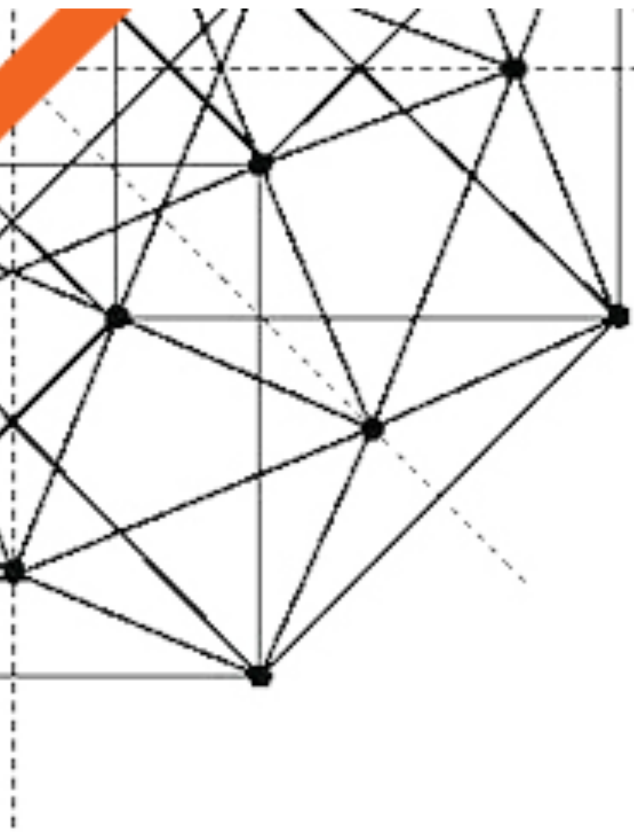
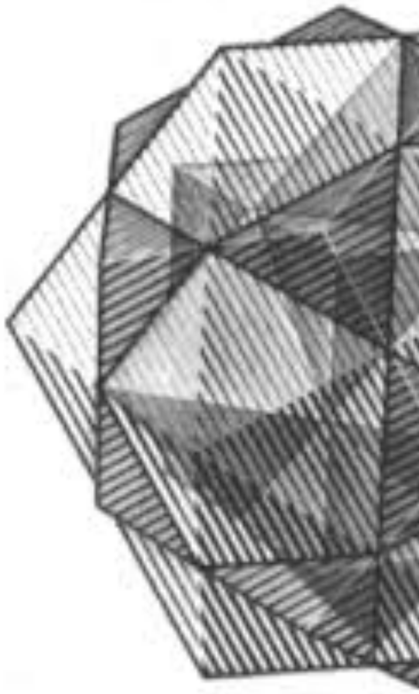


Matrix Applications: Hill Cipher



The Hill Cipher is a method of encipherment that transforms plaintext to ciphertext. This method hides letter frequencies, making it more difficult to de-encrypt than typical encryption methods.

It uses matrix multiplication as well as the association of the alphabet with a numerical system in order to encrypt a message.

A simple way of using the Hill Cipher is to restrict the Alphabet to capital letters and associate it with the numbers 0 through to 25 respectively. We can then group plaintext letters into blocks of 2 letters and encrypt the word/ message one block at a time. This is carried out using 2x2 matrix multiplication as well as calculating modulo 26.

To de-encrypt a message, the key matrix needs to be known and the inverse of the key matrix needs to be found.

As you can see, many matrix skills are applied when the Hill Cipher is used.

The equation:

$$Y = Axmod26$$

Is used to encrypt the message.

Y is a 2x1 matrix that represents the numbers associated with the ciphertext.
A is a 2x2 (key) matrix
x is a 2x1 matrix that represents the numbers associated with the plaintext.

$$\begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} mod26$$

Our key matrix A needs to be invertible modulo26 in order to be appropriate for the hill cipher – we wouldn't be able to de-encrypt messages if not. Finding modulo 26 means we can equate the numbers to the 26 letters in the alphabet. The basic principle is that we divide a number by 26 and use the remainder for numerical encipherment.

To encode a block of plaintext, we need to first break the word into blocks of 2 letters then write them as column vectors of the corresponding numbers.

For the word: MATHEMATICAL

$$\begin{bmatrix} M \\ A \end{bmatrix} \begin{bmatrix} T \\ H \end{bmatrix} \begin{bmatrix} E \\ M \end{bmatrix} \begin{bmatrix} A \\ T \end{bmatrix} \begin{bmatrix} I \\ C \end{bmatrix} \begin{bmatrix} A \\ L \end{bmatrix} = \begin{bmatrix} 12 \\ 0 \end{bmatrix} \begin{bmatrix} 19 \\ 7 \end{bmatrix} \begin{bmatrix} 4 \\ 12 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \begin{bmatrix} 8 \\ 2 \end{bmatrix} \begin{bmatrix} 0 \\ 11 \end{bmatrix}$$

Using the column matrices, we multiply each one by the key matrix, perform modulo 26 calculations on the resulting column matrix and equate it to ciphertext in blocks of 2 letters. An example of this is shown here:

$$\begin{bmatrix} M \\ A \end{bmatrix} = \begin{bmatrix} 12 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix}\begin{bmatrix} 12 \\ 0 \end{bmatrix} = \begin{bmatrix} 22x12 + 13x0 \\ 11x12\ +\ 5x0 \end{bmatrix} = \begin{bmatrix} 264 \\ 132 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix} mod26 \begin{bmatrix} M \\ A \end{bmatrix} = \begin{bmatrix} E \\ C \end{bmatrix}$$

Continuing to do this with the other column matrices gives the ciphertext: **ECPKKANRUUND**

$$\begin{bmatrix} E \\ C \end{bmatrix}\begin{bmatrix} P \\ K \end{bmatrix}\begin{bmatrix} K \\ A \end{bmatrix}\begin{bmatrix} N \\ R \end{bmatrix}\begin{bmatrix} U \\ U \end{bmatrix}\begin{bmatrix} N \\ D \end{bmatrix}$$

To de-encrypt ciphertext, we need to find the inverse of the key matrix. The determinant of A also needs to be relatively prime to 26 (not 13 or even) to make A invertible modulo 26. For the key matrix used previously:

$$detA = 22x5\ -\ 13x11 = -33\ =\ 19$$

As we have a negative determinant, we add 26 to it (twice in this case) to make it positive and in the range of 0-25.
19 is relatively prime to 26, so the inverse of A exists. We can now follow the rule:

As long as A^{-1} exists, $x = A^{-1}Ymod26$

$\mathbf{19^{-1}} \boldsymbol{mod26} = \mathbf{11}$ because 11x19 = 209mod26 = 1mod26

$$A^{-1} = \frac{1}{19}\begin{bmatrix} 22 & 13 \\ 11 & 5 \end{bmatrix} mod26 = 11\begin{bmatrix} 5 & -13 \\ -11 & 22 \end{bmatrix} mod26 = \begin{bmatrix} 3 & 13 \\ 9 & 8 \end{bmatrix} mod26$$

Using this inverse we can start the de-encryption:

$$x = A^{-1}Ymod26$$

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 & 13 \\ 9 & 8 \end{bmatrix}\begin{bmatrix} 4 \\ 2 \end{bmatrix} mod26 = \begin{bmatrix} 3x4 + 13x2 \\ 9x4 + 8x2 \end{bmatrix} = \begin{bmatrix} 38 \\ 52 \end{bmatrix} mod26 = \begin{bmatrix} 12 \\ 0 \end{bmatrix} = \begin{bmatrix} M \\ A \end{bmatrix}$$

And hence we can de-encrypt the message to reveal the word MATHEMATICAL again.