Códigos

Un método de codificación eficaz, es si se usa una matriz invertible de gran tamaño, se describa a continuación. Sea una matriz *M* invertible, que sólo conocen quienes la transmiten y quienes la reciben.

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

Supóngase que se desea codificar el mensaje:

ATTACK NOW

Se reemplaza cada letra con el número que le corresponde a su posición en el alfabeto. Un espacio se representa por 0.

A	T	T	A	C	K		N	O	W
1	20	20	1	3	11	0	14	15	23

El mensaje se ha convertido a la sucesión de números 1, 20, 20, 1, 3, 11, 0, 14, 15, 23. Que agrupamos como una sucesión de vectores columna,

$$\begin{bmatrix} 1 \\ 20 \end{bmatrix} \begin{bmatrix} 20 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 11 \end{bmatrix} \begin{bmatrix} 0 \\ 14 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \end{bmatrix}$$

Y multiplicamos por la izquierda a *M*:

$$M \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 77 \\ 39 \end{bmatrix}, \qquad M \begin{bmatrix} 20 \\ 1 \end{bmatrix} = \begin{bmatrix} -56 \\ -18 \end{bmatrix}, \qquad M \begin{bmatrix} 3 \\ 11 \end{bmatrix} = \begin{bmatrix} 35 \\ 19 \end{bmatrix}$$

$$M \begin{bmatrix} 0 \\ 14 \end{bmatrix} = \begin{bmatrix} 56 \\ 28 \end{bmatrix}, \qquad M \begin{bmatrix} 15 \\ 23 \end{bmatrix} = \begin{bmatrix} 47 \\ 31 \end{bmatrix}$$

Con lo que se obtiene la sucesión de números 77, 39, -56, -18, 35, 19, 56, 28, 47, 31. Éste es el mensaje cifrado. Para decodificarlo, quien lo recibe necesita calcular M^{-1}.

$$M^{-1} = \begin{bmatrix} -1 & 2 \\ -\frac{1}{2} & \frac{3}{2} \end{bmatrix}$$

Y multiplicarla por los vectores $\begin{bmatrix} 77 \\ 39 \end{bmatrix}, \begin{bmatrix} -56 \\ -18 \end{bmatrix}, \begin{bmatrix} 35 \\ 19 \end{bmatrix}, \begin{bmatrix} 56 \\ 28 \end{bmatrix}, \begin{bmatrix} 47 \\ 31 \end{bmatrix}$ para obtener los números originales.

Problema 1

Basado en el método anterior, decodifica el mensaje expresado por los números 17, 15, 29, 15, 17, 29, 16, 31, 47, 6, 19, 20, 35, 24, 39, 14, 19, 19, si

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix}$$

Problema 2

Interceptaste el siguiente mensaje cifrado sobre el mercado accionario: 1156, -203, 624, -84, -228, 95, 1100, -165, 60, 19. Sus fuentes le informan que fue codificado con una matriz simétrica de 2 X 2. Tu intuición te dice que es muy probable que la primera palabra del mensaje sea *sell* o *buy*. Tu misión Jim es descifrar el mensaje.