CRIPTOGRAFÍA - Encriptar mensajes utilizando matrices.

Un criptograma es un mensaje escrito de acuerdo a un código secreto. Para crear criptogramas por medio de matrices primeramente se debe asignar un número a cada letra del alfabeto (el cero representa espacios en blanco) de la siguiente manera:

a = 1	g = 7	m =13	r=19	x = 25
b = 2	h = 8	n =14	s= 20	y = 26
c = 3	i = 9	ñ = 15	t = 21	z = 27
d = 4	j=10	o = 16	u = 22	_=0
e = 5	k = 11	p = 17	v = 23	. = 28
f = 6	1 = 12	q = 18	w = 24	

Después, el mensaje es convertido a números dividiéndolo en matrices fila sin codificar, cada uno con "n" elementos. Se encripta multiplicando cada matriz fila formada por n elementos por una matriz cuadrada de orden n que sea regular, es decir, que tenga inversa. El resultado es el mensaje encriptado. A la matriz cuadrada utilizada la llamamos matriz clave.

Para aclarar el proceso veamos un ejemplo.

Ejemplo: Vamos a encriptar las palabras Flipped Classroom utilizando matrices filas de tres elementos.

F	1	i	p	p	e	d		С	1	a	s	s	r	О	О	m	
6	12	9	17	17	5	4	0	3	12	1	20	20	19	16	16	13	28

Complicamos el cifrado multiplicando cada 3 elementos por una matriz de orden tres invertible. Por ejemplo:

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 0 & -1 & 3 \\ 2 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 6 & 12 & 9 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 1 \\ 0 & -1 & 3 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 24 & 9 & 42 \end{bmatrix}$$

$$\begin{bmatrix} 17 & 17 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 1 \\ 0 & -1 & 3 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 27 & 22 & 68 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 0 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 1 \\ 0 & -1 & 3 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 10 & 11 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 12 & 1 & 20 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 1 \\ 0 & -1 & 3 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 52 & 43 & 15 \end{bmatrix}$$

$$\begin{bmatrix} 20 & 19 & 16 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 1 \\ 0 & -1 & 3 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 52 & 37 & 77 \end{bmatrix}$$

$$\begin{bmatrix} 16 & 13 & 28 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 1 \\ 0 & -1 & 3 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 72 & 47 & 55 \end{bmatrix}$$

Luego el mensaje cifrado sería:

¿Cómo se decodifica un mensaje cifrado?

Es absolutamente necesario conocer la matriz clave y calcular su matriz inversa. Para descifrar el mensaje oculto se procede multiplicando cada matriz fila de orden tres (formada por tres elementos del mensaje cifrado) por la inversa de la matriz clave A.

Ejemplo: Vamos a descifrar el mensaje anterior

24 9 42 27 22 68 10 11 4 52 43 15 52 37 77 72 47 55

conocida la matriz clave $A = \begin{bmatrix} 1 & 2 & 1 \\ 0 & -1 & 3 \\ 2 & 1 & 0 \end{bmatrix}$.

Calculamos la matriz inversa de A: $A^{-1} = \begin{bmatrix} \frac{-3}{11} & \frac{1}{11} & \frac{7}{11} \\ \frac{6}{11} & \frac{-2}{11} & \frac{-3}{11} \\ \frac{2}{11} & \frac{3}{11} & \frac{-1}{11} \end{bmatrix}$

$$\begin{bmatrix} 24 & 9 & 42 \end{bmatrix} \cdot \begin{bmatrix} \frac{-3}{11} & \frac{1}{11} & \frac{7}{11} \\ \frac{6}{11} & \frac{-2}{11} & \frac{-3}{11} \\ \frac{2}{11} & \frac{3}{11} & \frac{-1}{11} \end{bmatrix} = \begin{bmatrix} 6 & 12 & 9 \end{bmatrix} \longrightarrow \begin{bmatrix} 27 & 22 & 68 \end{bmatrix} \cdot \begin{bmatrix} \frac{-3}{11} & \frac{1}{11} & \frac{7}{11} \\ \frac{6}{11} & \frac{-2}{11} & \frac{-3}{11} \\ \frac{2}{11} & \frac{3}{11} & \frac{-1}{11} \end{bmatrix} = \begin{bmatrix} 17 & 17 & 5 \end{bmatrix} \longrightarrow$$

$$\begin{bmatrix} 10 & 11 & 4 \end{bmatrix} \cdot \begin{bmatrix} \frac{-3}{11} & \frac{1}{11} & \frac{7}{11} \\ \frac{6}{11} & \frac{-2}{11} & \frac{-3}{11} \\ \frac{2}{11} & \frac{3}{11} & \frac{-1}{11} \end{bmatrix} = \begin{bmatrix} 4 & 0 & 3 \end{bmatrix} \longrightarrow \begin{bmatrix} 52 & 43 & 15 \end{bmatrix} \cdot \begin{bmatrix} \frac{-3}{11} & \frac{1}{11} & \frac{7}{11} \\ \frac{6}{11} & \frac{-2}{11} & \frac{-3}{11} \\ \frac{2}{11} & \frac{3}{11} & \frac{-1}{11} \end{bmatrix} = \begin{bmatrix} 12 & 1 & 20 \end{bmatrix} \longrightarrow$$

$$\begin{bmatrix} 52 & 37 & 77 \end{bmatrix} \cdot \begin{bmatrix} \frac{-3}{11} & \frac{1}{11} & \frac{7}{11} \\ \frac{6}{11} & \frac{-2}{11} & \frac{-3}{11} \\ \frac{2}{11} & \frac{3}{11} & \frac{-1}{11} \end{bmatrix} = \begin{bmatrix} 20 & 19 & 16 \end{bmatrix} \longrightarrow \begin{bmatrix} 72 & 47 & 55 \end{bmatrix} \cdot \begin{bmatrix} \frac{-3}{11} & \frac{1}{11} & \frac{7}{11} \\ \frac{6}{11} & \frac{-2}{11} & \frac{-3}{11} \\ \frac{2}{11} & \frac{3}{11} & \frac{-1}{11} \end{bmatrix} = \begin{bmatrix} 16 & 13 & 28 \end{bmatrix}$$

Utilizamos la tabla que asocia los números con el alfabeto y tenemos nuestro mensaje decodificado:

6	12	9	17	17	5	4	0	3	12	1	20	20	19	16	16	13	28
F	1	i	p	p	e	d		C	1	a	S	S	r	О	О	m	

Justificación:

Si a la matriz $X = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}$, formada por tres elementos no codificados, la multiplicamos por A matriz de orden 3 invertible obtenemos $Y = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \cdot A = \begin{bmatrix} y_1 & y_2 & y_3 \end{bmatrix}$ que son los elementos del mensaje codificado. Si a Y lo multiplicamos por la inversa de A:

 $\begin{bmatrix} y_1 & y_2 & y_3 \end{bmatrix} \cdot A^{-1} = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \cdot A \cdot A^{-1} = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}$ Obteniendo así el los elementos no codificados.

Por lo tanto es totalmente necesario conocer la matriz clave para poder decodificar un mensaje por este método.