Codificación por Matrices

Ana Paola Carreón Hernández

21 de junio de 2022

Introducción

La forma mas sencilla y común de codificar mensajes es asignandole un número a cada letra de el alfabeto y escribir tu mensaje con los valores asignados por ejemplo el mensaje:

ENVIA MEME

Puede estar codificado como:

3,20,16,5,4 11,3,11,3

En el ejemplo la codificacion es una al azar que invente en cinco minutos donde la E esta representada por el 3 la N por el 20 y asi progresivamente. Desafortunadamente este tipo de código es generalmente fácil de decifrar y romper. En un mensaje largo podremos ser capaces de descubrir que letra esta representada por que número. Por ejemplo si el número 3 es el que aparece con más frecuencia eso solo significaría que es la letra E que es la que es mas usada en el Español, igualmente podríamos ir ubicando las otras vocales he aqui una tabla de las letras mas usadas del español.

Cuadro 1: Concurrencia letras

E	A	O	S	R	N	I
13.68 %	12.53 %	8.68 %	7.98 %	6.87 %	6.71 %	6.25 %

Por lo que una manera en la que puedes ocultar o codificar mas tus mensajes sería a traves de **multiplicaciones de matrices**.

Desarrollo

Los pasos para codificar a traves de matrices son los siguientes:

1. Para iniciar debes de escoger una palabra que está limitada a tener exactamente la misma cantidad de letras que los elementos de tu matriz codificadora no mas no menos

   `En este ejemplo nuestra matriz codificadora tiene 9 valores por lo que escogemos una frase o palabra que tenga 9 caracteres donde los espacios no importan; en este caso haremos uso de la ejemplificación de la introducción asi que nuestra frase será ENVIA MEME`

2. Cambiar las letras de tu mensaje a los valores que decidiste asignarle. `En el ejemplo el resultado es 3,20,16,5,4,11,3,11,3`

Cuadro 2: Codificación Ejemplo

A	B	C	D	E	F	G	H	I	J	K	L	M	
4	13	26	12	3	17	6	14	5	25	30	7	11	
N	ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
20	1	10	19	24	18	15	9	0	16	21	2	8	22

3. Una vez cambiado tu mensaje debes hacer una matriz cuadrada con tu mensaje codificado donde vas acomodando los valores por columna(verticalmente) `En el ejemplo el 3 va en la posición (1,1), el 20 en la posición (2,1) y asi sucesivamente`

$$B = \begin{pmatrix} 3 & 5 & 3 \\ 20 & 4 & 11 \\ 16 & 11 & 3 \end{pmatrix}$$

4. Para mejorar la codificación multiplicaremos la matriz de la codificación sencilla nuestra B con una matriz A que mas adelante veremos que requisitos debe cumplir esta para que sea valida:

   `La matriz resultante AB es tu matriz codificada de manera mucho mas segura`

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 5 & 3 \\ 2 & 3 & 2 \end{pmatrix} \quad AB = \begin{pmatrix} 59 & 24 & 28 \\ 154 & 63 & 70 \\ 98 & 44 & 45 \end{pmatrix}$$

5. Para regresar a tu matriz B y decodificar el mensaje lo único que tienes que hacer es multiplicar tu matriz AB con la inversa de A

$$A^{-1} = \begin{pmatrix} 1 & -1 & 1 \\ 2 & 0 & -1 \\ -4 & 1 & 1 \end{pmatrix} \quad A^{-1} \cdot AB = \begin{pmatrix} 3 & 5 & 3 \\ 20 & 4 & 11 \\ 16 & 11 & 3 \end{pmatrix}$$

6. Terminamos reemplazando los valores de la matriz decodificada por sus valores equivalentes del alfabeto en el mismo orden que los insertamos osea se por columna

$$3,20,16,5,4,11,3,11,3 = \text{ENVIA MEME}$$

Como mencionamos con anterioridad tu puedes escoger la longitud de tu cadena pero a cambio tienes que crear tu propia matriz codificadora la cual debe cumplir los siguiente requisitos:

- Que sea cuadrada
- Que su determinante sea diferente de cero
- Que tenga el mismo numero de elementos que tu mensaje (sin contar los espacios)

La razón por la que necesitamos que sea cuadrada y que su determinante sea diferente de cero es porque si no los cumple eso implicaría que la matriz no tiene inversa entonces no habría manera de decodificar nuestro mensaje y la razón por la que necesitamos que sea de el mismo tamaño que nuestro mensaje es porque si no lo son no podríamos hacer ninguna multiplicación porque el tamaño de las matrices no coincidirían.

Conclusión

Es una manera interesante de ver alguna aplicación de la algebra lineal sin embargo tiene muchas restricciones a la hora de ponerlo en marcha las cuales son el restringir el tamaño de tus mensajes o tener que estar buscando y creando matrices codificadoras de la longitud que tu quieres.

Bibliografía

[1] Leon, Steve J. *Linear Algebra with Applications*, octava edición, Pearson.