MENSAJES OCULTOS

Objetivos de aprendizaje:

1. Identificar los conceptos y procesos del álgebra lineal involucrados en un sistema de cifrado y descifrado de mensajes.
2. Utilizar apropiadamente procedimientos para cifrar y descifrar mensajes.
3. Transferir adecuadamente las ideas o conceptos del álgebra lineal a un contexto particular, para resolver situaciones problema.

Indicaciones generales:

- *Para cada semana (3, 4 y 5) se plantean unas actividades a desarrollar.*
- *Todo aporte debe quedar directamente registrado en el foro.*
- *Se debe registrar todos los procesos matemáticos empleados para dar solución a las actividades propuestas.*
- *Sólo se debe entregar consolidado grupal de las actividades propuestas para la semana 5.*

OCULTANDO MENSAJES

Una de las aplicaciones del Álgebra Lineal es la criptografía, parte de la Criptología (estudio de lo oculto), que trata del diseño e implementación de sistemas secretos para cifrar mensajes. Existen diversas técnicas para cifrar y descifrar mensajes cuya complejidad depende de las herramientas matemáticas que se empleen en el diseño de los algoritmos de cifrado. Un sistema clásico es el Sistema de Hill o Cifrado en Bloques que fue diseñado por el matemático Lister Hill en 1929 basado en ideas de algebra lineal, en particular, en el álgebra de matrices.

SEMANA 3.

De manera individual realizar lo que se plantea a continuación.

1. Consultar y estudiar el método de Hill para encriptar y desencriptar mensajes, luego:
   - A través de un esquema, describir *con sus propias palabras* el proceso que se realiza para encriptar un mensaje. Escribir la bibliografía revisada, empelando normas APA.
   - Elegir una frase que tenga entre 3 y 4 palabras y encriptarla con el método consultado y la matriz clave $\begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}$ y publíquelo en el foro para que sus compañeros lo puedan descifrar.
2. Revisar, por lo menos, los aportes de un compañero del grupo y desencriptar el mensaje propuesto, describiendo el proceso empleado, teniendo en cuenta la matriz clave empleada. Si no le es posible realizarlo, indicar cuál fue la dificultad, por ejemplo, *falta información*, *no se llega a un mensaje coherente*, entre otros.
   Si necesita alguna información adicional, puede registrar respetuosamente en el foro, comentarios a su(s) compañero(s). Comentarios como “Felicitaciones” o “Estoy de acuerdo”, no se considera un aporte académico.

SEMANA 4.

De manera individual realizar lo que se plantea a continuación. Registrar todos los procedimientos empleados.

Usando el método de Hill, realizar lo siguiente:

1. Elegir una frase de tres palabras, la cual debe cifrar teniendo en cuenta la siguiente información.
   - Se cuenta con la siguiente matriz clave.
   $$\begin{pmatrix} 4 & 3 & x \\ 2 & 2 & 1 \\ x & 1 & 1 \end{pmatrix}$$
   - Se sabe que el determinante de la matriz es 1 y que el valor de x es un entero positivo.
   - La asignación numérica se debe realizar con el siguiente recuadro (en él, el símbolo "_" representa el espacio entre las palabras).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

2. Revisar, por lo menos, los aportes de un compañero del grupo y desencriptar el mensaje propuesto describiendo el proceso empleado. Si no le es posible realizarlo, indicar cuál fue la dificultad, por ejemplo, falta información, no llega a un mensaje coherente, entre otros. Al iniciar el aporte, escribir el nombre del compañero sobre el que realizará lo indicado.
   Si necesita alguna información adicional, puede registrar respetuosamente en el foro comentarios a su(s) compañero(s).

SEMANA 5. ACTIVIDADES PARA EL CONSOLIDADO GRUPAL

Cada integrante del equipo debe proponer una solución a las tres actividades; luego, revisar, comentar o complementar los aportes de sus compañeros y aportar a la consolidación de la respuesta grupal. Todo debe estar registrado en el foro.

Suponga que se intercepta el mensaje IZFORVKGRWVXMJJMUBLOVGXHOKE y que de él se sabe lo siguiente.

a. Las tres primeras letras del mensaje oculto son DEM y las tres últimas son LES.
b. La matriz clave es de la forma $\begin{pmatrix} a & b & c \\ -2 & 1 & 0 \\ -1 & -1 & 1 \end{pmatrix}$.
c. El determinante de la matriz clave es 1.

A partir de esta información:

Actividad 1. Planteen un sistema de ecuaciones que permita hallar las incógnitas a, b, c.
Actividad 2. Resolver el sistema de ecuaciones planteado.
Actividad 3. Empleando la matriz clave, descifre el mensaje oculto.