TRABAJO COLABORATIVO

ÁLGEBRA LINEAL

Integrantes:
SUBGRUPO 22
SANTIAGO ZAQUE BUSTOS (1911981780)
YEIMY ANDREA PATIÑO RODRIGUEZ
EDUAR ALEXANDER VILLADA
ANGY NATALIA PUERTO

Instructor:

JOSELIN MONTEALEGRE
Docente - Politécnico Grancolombiano.

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
INGENIERIA INDUSTRIAL
2019

TABLA DE CONTENIDO

INTRODUCCIÓN

Desde que la humanidad invento el lenguaje escrito, ha tratado de compartir información de manera secreta. Este es, básicamente, el objetivo de la criptografía, él estudio de las técnicas para proteger las comunicaciones sensibles por medio de la encriptación de datos y posterior descifrado. El cifrado es la transformación de los datos de una forma ilegible, de manera que, incluso aquellos que puedan ver los datos cifrados, no podrán entender la información oculta. El descifrado es el proceso inverso, es la transformación de los datos cifrados de nuevo en una forma comprensible. Hay algunos conceptos básicos relativos a la criptografía.

- **Cifrado:** El procedimiento que generará un mensaje ininteligible para el receptor.

También se usa para recrear el mensaje original, según el mecanismo de cifrado que se utilice.

- **Texto plano:** El mensaje o información que se va a codificar.

- **Texto cifrado:** El mensaje o información que se obtiene después que se ha utilizado el

OBJETIVO GENERAL

- Investigar e identificar una de las aplicaciones del álgebra lineal la cual consiste en la criptografía mediante matrices, sus conceptos, procedimientos y métodos que dan solución a un sistema de cifrado y descifrado de palabras.

OBJETIVOS ESPECIFICOS

- Investigar sobre el método de cifrado de Hill y plantear posibles soluciones a las actividades indicadas en el trabajo colaborativo.

- Identificar las ideas y procedimientos del álgebra lineal para poderlas trasladar y desarrollar a situaciones problema.

SÍNTESIS IDEAS PRINCIPALES DEL FORO

De acuerdo a la investigación, el desarrollo y los aportes que dio cada uno de los integrantes del grupo utilizando diferentes métodos y recursos de aprendizaje como lo fueron los videos, tutoriales, lecturas, etc. Se evidencia el conocimiento que cada uno de los integrantes iba adquiriendo de acuerdo a su investigación y a sus diferentes consultas, esto nos llevó a la participación e información que poco a poco se iba desarrollando gracias a que cada uno realizaba sus aportes de una manera diferente, creando un dialogo lleno de ideas y puntos de vista distintos, retroalimentando la información si era necesario y corrigiendo la participación de algún compañero.

En cuanto a la participación del foro, se logra evidenciar la consulta sobre el sistema de Hill, sus aplicaciones, y el método para poder desarrollar el cifrado y descifrado de una palabra planteada en la actividad del trabajo colaborativo, esto se logra dar a entender mediante videos, lecturas y desarrollos individuales que cada uno de los integrantes del grupo compartía, aportando así posibles soluciones a las actividades. Se investiga también acerca del método de eliminación de Gauss Jordán, este método lo utilizamos para poder hallar la inversa de nuestra matriz clave, compartiendo videos y lecturas que nos decían el paso a paso para poder hallar la matriz inversa mediante este método.

POSIBLES SOLUCIONES

De acuerdo a la actividad 1.2 que dice:

A partir de la consulta anterior, con sus propias palabras, describa el paso a paso

Para cifrar la palabra DEDICACION empleando la matriz clave.

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	28

Tenemos como posible solución el siguiente procedimiento:

Para cifrar la palabra **DEDICACIÓN** lo primero que realizamos fue analizar el módulo con el cual se iba a trabajar, cabe resaltar que en la información investigada el sistema de cifrado de Hill se trabaja con módulo 26 es decir es un sistema de cifrado poli alfabético. Esto quiere decir que a cada letra del alfabeto se le asigna un número. Pero en nuestro caso iba a ser diferente al tener la siguiente asignación numérica dada en la actividad del trabajo colaborativo.

Al analizar nuestra asignación numérica notamos que no es módulo 26, puesto que, aunque en ella se tiene 26 letras del alfabeto cada una con una asignación numérica, también encontramos el signo ‘’ _ ‘’ y el signo ‘’. ‘’ Los cuales también tiene una asignación numérica que corresponde a 27 y 28 respectivamente. ¿Pero porque hablamos de módulo 29?, porque en este caso el numero 0 sería el 29.

Al tener ya definido nuestro modulo, procedemos a separar la palabra a cifrar en silabas, es decir**: DE, DI, CA, CI, ÓN** y así multiplicar cada pareja por nuestra matriz clave de la siguiente manera:

$$\begin{pmatrix}1 & 7\\0 & 1\end{pmatrix} * \begin{pmatrix}3\\4\end{pmatrix} = \begin{pmatrix}1*3+7*4\\0*3+1*4\end{pmatrix} = \begin{pmatrix}31\\4\end{pmatrix} \boldsymbol{modulo\ 29} = \begin{pmatrix}2\\4\end{pmatrix}$$

$$\begin{pmatrix}1 & 7\\0 & 1\end{pmatrix} * \begin{pmatrix}3\\8\end{pmatrix} = \begin{pmatrix}1*3+7*8\\0*3+1*8\end{pmatrix} = \begin{pmatrix}59\\8\end{pmatrix} \boldsymbol{modulo\ 29} = \begin{pmatrix}1\\8\end{pmatrix}$$

$$\begin{pmatrix}1 & 7\\0 & 1\end{pmatrix} * \begin{pmatrix}2\\0\end{pmatrix} = \begin{pmatrix}1*2+7*0\\0*2+1*0\end{pmatrix} = \begin{pmatrix}2\\0\end{pmatrix} \boldsymbol{modulo\ 29} = \begin{pmatrix}2\\0\end{pmatrix}$$

$$\begin{pmatrix}1 & 7\\0 & 1\end{pmatrix} * \begin{pmatrix}2\\8\end{pmatrix} = \begin{pmatrix}1*2+7*8\\0*2+1*8\end{pmatrix} = \begin{pmatrix}58\\8\end{pmatrix} \boldsymbol{modulo\ 29} = \begin{pmatrix}0\\8\end{pmatrix}$$

$$\begin{pmatrix}1 & 7\\0 & 1\end{pmatrix} * \begin{pmatrix}15\\13\end{pmatrix} = \begin{pmatrix}1*15+7*13\\0*15+1*13\end{pmatrix} = \begin{pmatrix}106\\13\end{pmatrix} \boldsymbol{modulo\ 29} = \begin{pmatrix}19\\13\end{pmatrix}$$

Que corresponderían a las siguientes letras de acuerdo a nuestra asignación numérica modulo 29.

- $\binom{2}{4} = \binom{C}{E}$
- $\binom{1}{8} = \binom{B}{I}$
- $\binom{2}{0} = \binom{C}{A}$
- $\binom{0}{8} = \binom{A}{I}$
- $\binom{19}{13} = \binom{S}{N}$

Obtenemos como resultado la palabra **CEBICAAISN** que seria nuestra palabra cifrada.

. **De acuerdo a la actividad 1.3 que dice:**

Describir el proceso (paso a paso) para desencriptar el mensaje obtenido en el punto anterior.

Tenemos como posible solución el siguiente procedimiento:

Teniendo en cuenta que el método de cifrado de Hill nos dice que la matriz de la transformación lineal utilizada, la clave, que sea una matriz inversa, teniendo en cuenta que la determinante de nuestra matriz sea ≠ 0, si es igual a 0 la matriz no tiene inversa. Sumándole también que la matriz debe ser cuadrada, si no es cuadrada no hay matriz inversa.

Teniendo claro estas condiciones procedemos a hallar la det de nuestra matriz clave $\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$, además de esto podemos observar que es una matriz cuadrada de 2x2.

Para hallar la det de nuestra matriz clave $\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$, utilizamos la ley de sarrus, la cual solo aplica para matrices de 2x2 o 3x3, en nuestro caso por tener una matriz de 2x2 nos permite poder utilizar este procedimiento.

$\underline{o}\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$

=1x1-0x7

=1-0

=1

det =1

Esto quiere decir que la determinante de nuestra matriz clave

$^{o}\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$es ≠0

Al tener la determinante de nuestra matriz clave y que sea ≠0 procedemos a hallar la matriz inversa, porque como ya sabemos que la det ≠0 esto quiere decir que nuestra matriz tiene inversa.
Lo siguiente que procedemos a realizar fue hallar la matriz inversa de nuestra matriz clave, por medio del método Gauss Jordan de la siguiente manera:

Lo primero que debemos hacer según el método de Gauss Jordan es tener nuestra matriz aumentada de la siguiente manera, de la siguiente manera,

$$\left(\begin{array}{cc:cc} 1 & 7 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right)$$

El método de eliminación de Gauss Jordan nos dice que, a la matriz aumentada la llevamos en forma escalonada reducida por filas, esto quiere decir que todos sus elementos que están fuera de la diagonal principal deben ser 0 y sus pivotes deben ser 1, esto con el fin de convertirla en una matriz identidad. Nuestra matriz clave es la siguiente:

$$\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$$

Este 7 lo debemos convertir en 0, para que de esta manera los elementos que están por fuera

$$\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$$

Diagonal principal

Procedemos a resolver utilizando operaciones entre filas, las cuales pueden ser cuatro:

- Intercambiar la fila *i* y la fila *j*, $Fi \leftrightarrow Fj$
- Multiplicar la fila *i* por un α no nulo
- Reemplazar la fila *j* por el resultado obtenido al sumar la fila *j* y la fila *i* F*i*+F*j*
- Combinaciones de las operaciones anteriores α $Fi \leftrightarrow Fj$.

De esta manera obtenemos:

- $\left(\begin{array}{cc|cc} 1 & 7 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right) \rightarrow$ F1 F1+ (-7) F2

- $\left(\begin{array}{cc|cc} 1 & 0 & 1 & -7 \\ 0 & 1 & 0 & 1 \end{array}\right)$ Esta seria nuestra matriz inversa

Porque decimos que nuestra matriz inversa seria $\begin{pmatrix} 1 & -7 \\ 0 & 1 \end{pmatrix}$. Porque una manera de comprobar que es cierto, es realizando la operación de la multiplicación entre la matriz clave $\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$ y la matriz inversa $\begin{pmatrix} 1 & -7 \\ 0 & 1 \end{pmatrix}$, el resultado entre estas dos matrices nos debe dar la matriz identidad, es decir una matriz que tiene ceros (0) excepto en la posición de la diagonal principal en donde tiene unos (1).

- $\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$ A nuestra matriz clave la llamaremos **A**

- $\begin{pmatrix} 1 & -7 \\ 0 & 1 \end{pmatrix}$ A nuestra matriz clave la llamaremos **B**

- A= $\begin{pmatrix} 1 & 7 \\ 0 & 1 \end{pmatrix}$XB=$\begin{pmatrix} 1 & -7 \\ 0 & 1 \end{pmatrix}$ En esta operación multiplicaremos filas x columnas.

- **= 1+0 7-7 0+0 0+1**

- **=** $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ siendo esta nuestra matriz **identidad.**

Con nuestra matriz inversa hallada $\begin{pmatrix} 1 & -7 \\ 0 & 1 \end{pmatrix}$, podemos realizar la misma operación que hicimos en el momento de cifrar nuestra palabra, que es multiplicar nuestra matriz inversa por las parejas de letras que obtuvimos en el momento de cifrar la palabra **DEDICACION.**

Las cuales son las siguientes:

- **CEBICAAISN**

Realizamos el mismo ejercicio que es dejarla e forma matricial, y asignarle el numero correspondiente según nuestra asignación numérica modulo 29, de la siguiente manera:

- $\begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} C \\ E \end{pmatrix}$
- $\begin{pmatrix} 1 \\ 8 \end{pmatrix} = \begin{pmatrix} B \\ I \end{pmatrix}$
- $\begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} C \\ A \end{pmatrix}$
- $\begin{pmatrix} 0 \\ 8 \end{pmatrix} = \begin{pmatrix} A \\ I \end{pmatrix}$
- $\begin{pmatrix} 19 \\ 13 \end{pmatrix} = \begin{pmatrix} S \\ N \end{pmatrix}$

Separando nuestras letras en forma matricial, procedemos a multiplicar cada pareja por la matriz inversa $\begin{pmatrix} 1 & -7 \\ 0 & 1 \end{pmatrix}$ los resultados obtenidos nos deben dar nuevamente la palabra **DEDICACION.**

TRABAJO COLABORATIVO ALGEBRA LINEAL

De acuerdo a la actividad 2 que dice:

Suponga que se intercepta el mensaje **NQÑTIJIQKSSEWNHRÑTYPIWADPHYEVNUHZEMQTEKHJQLLP**

Junto con este mensaje encriptado, solo se logró obtener la matriz clave $\begin{pmatrix} 9 & 5 & 2 \\ 5 & 4 & 3 \\ 1 & 1 & 1 \end{pmatrix}$

La misión del grupo es:

1. Descifrar tal mensaje

2. detallar organizadamente todos los procedimientos que se realizaron para descifrar el mensaje

Posible soluciones.

1. Primero optamos por asignar un número a cada letra del mensaje interceptado teniendo en cuenta el sistema Hill y quedo de la siguiente manera:

N	**Q**	**Ñ**	**T**	**I**	**J**	**I**	**Q**	**K**	**S**	**S**	**E**	**W**	**N**	**H**
13	17	14	20	8	9	8	17	10	19	19	4	23	13	7
R	**Ñ**	**T**	**Y**	**P**	**I**	**W**	**A**	**D**	**P**	**H**	**Y**	**E**	**V**	**N**
18	14	20	25	16	8	23	0	3	16	7	25	4	22	13
U	**H**	**Z**	**E**	**M**	**Q**	**T**	**E**	**K**	**H**	**J**	**Q**	**L**	**L**	**P**
21	7	26	4	12	17	20	4	10	7	9	17	11	11	16

2. Continuamos con agrupar los números dados y formamos ternas de 3 dígitos

$$\begin{matrix} 13 & 20 & 8 & 19 & 23 & 18 & 25 & 23 & 16 & 4 & 21 & 4 & 20 & 7 & 11 \\ 17 & 8 & 17 & 19 & 13 & 14 & 16 & 0 & 7 & 22 & 7 & 12 & 4 & 9 & 11 \\ 14 & 9 & 10 & 4 & 7 & 20 & 8 & 3 & 25 & 13 & 26 & 17 & 10 & 17 & 16 \end{matrix}$$

3. Debemos hallar el determinante de nuestra matriz clave.

$\begin{pmatrix} 9 & 5 & 2 \\ 5 & 4 & 3 \\ 1 & 1 & 1 \end{pmatrix}$ Δ=1 $A^{-1} = \left|\frac{1}{A}\right|$.Adj (A')

lAl= 36+15+10-(8+27+25)

61-60

=1

4. A continuación tomamos la matriz clave y le sacamos su matriz inversa:

$\begin{pmatrix} 9 & 5 & 2 \\ 5 & 4 & 3 \\ 1 & 1 & 1 \end{pmatrix}$= matriz inversa $\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix}$

4.Con la matriz inversa de la matriz clave y las ternas ya podemos pasar a operar la matriz inversa con todas las ternas y el resultado lo pasamos a modulo 29 para poder asignar las letras a cada número que nos de:

$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 13 \\ x17 \\ 14 \end{matrix} = \begin{matrix} (1*13)+ & (-3*17)+ & (7*14) \\ (-2*13)+ & (7*17)+ & (-17*14) \\ (1*13)+ & (-4*17)+ & (11*14) \end{matrix} = \begin{matrix} 60 \\ -145 \\ 99 \end{matrix} \text{mod}29 \begin{matrix} 2 & \mathbf{C} \\ 0 = & \mathbf{A} \\ 12 & \mathbf{M} \end{matrix}$

$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 20 \\ x\ 8 \\ 9 \end{matrix} = \begin{matrix} (1*20)+ & (-3*8)+ & (7*9) \\ (-2*20)+ & (7*8)+ & (-17*9) \\ (1*20)+ & (-4*8)+ & (11*9) \end{matrix} = \begin{matrix} 59 \\ -137 \\ 87 \end{matrix} \text{mod}29 \begin{matrix} 1 & \boldsymbol{B} \\ 8= & \boldsymbol{I} \\ 0 & \boldsymbol{A} \end{matrix}$

$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 8 \\ x17 \\ 10 \end{matrix} = \begin{matrix} (1*8)+ & (-3*17)+ & (7*10) \\ (-2*8)+ & (7*17)+ & (-17*10) \\ (1*8)+ & (-4*17)+ & (11*10) \end{matrix} = \begin{matrix} 27 \\ -67 \\ 50 \end{matrix} \text{mod}29 \begin{matrix} 27 & \_ \\ 20= & \mathbf{T} \\ 21 & \mathbf{U} \end{matrix}$

$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 19 \\ x19 \\ 4 \end{matrix} = \begin{matrix} (1*19)+ & (-3*19)+ & (7*4) \\ (-2*19)+ & (7*19)+ & (-17*4) \\ (1*19)+ & (-4*19)+ & (11*4) \end{matrix} = \begin{matrix} -10 \\ 27 \\ -13 \end{matrix} \text{mod}29 \begin{matrix} 19 & \mathbf{S} \\ 27= & \_ \\ 16 & \mathbf{P} \end{matrix}$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 23 \\ x13 \\ 7 \end{matrix} \begin{matrix} (1*23)+ \\ =(-2*23)+ \\ (1*23)+ \end{matrix} \begin{matrix} (-3*13)+ \\ (7*13)+ \\ (-4*13)+ \end{matrix} \begin{matrix} (7*7) \\ (-17*7) \\ (11*7) \end{matrix} \begin{matrix} 33 \\ =-74 \\ 48 \end{matrix} \begin{matrix} 4 \\ \mathrm{mod}29 \\ 19 \end{matrix} \begin{matrix} \mathbf{E} \\ 13=\mathbf{N} \\ \mathbf{S} \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 18 \\ x14 \\ 20 \end{matrix} \begin{matrix} (1*18)+ \\ =(-2*18)+ \\ (1*18)+ \end{matrix} \begin{matrix} (-3*14)+ \\ (7*14)+ \\ (-4*14)+ \end{matrix} \begin{matrix} (7*20) \\ (-17*20) \\ (11*20) \end{matrix} \begin{matrix} 116 \\ =-278 \\ 182 \end{matrix} \begin{matrix} 0 \\ \mathrm{mod}29 \\ 8 \end{matrix} \begin{matrix} \mathbf{A} \\ 12=\mathbf{M} \\ \mathbf{I} \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 25 \\ x16 \\ 8 \end{matrix} \begin{matrix} (1*25)+ \\ =(-2*25)+ \\ (1*25)+ \end{matrix} \begin{matrix} (-3*16)+ \\ (7*16)+ \\ (-4*16)+ \end{matrix} \begin{matrix} (7*8) \\ (-17*8) \\ (11*8) \end{matrix} \begin{matrix} 33 \\ =-74 \\ 49 \end{matrix} \begin{matrix} 4 \\ \mathrm{mod}29 \\ 20 \end{matrix} \begin{matrix} \mathbf{E} \\ 13=\mathbf{N} \\ \mathbf{T} \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 23 \\ x\ 0 \\ 3 \end{matrix} \begin{matrix} (1*23)+ \\ =(-2*23)+ \\ (1*23)+ \end{matrix} \begin{matrix} (-3*0)+ \\ (7*0)+ \\ (-4*0)+ \end{matrix} \begin{matrix} (7*3) \\ (-17*3) \\ (11*3) \end{matrix} \begin{matrix} 44 \\ =-97 \\ 56 \end{matrix} \begin{matrix} 15 \\ \mathrm{mod}29 \\ 27 \end{matrix} \begin{matrix} \boldsymbol{O} \\ 19=\boldsymbol{S} \\ \_\_ \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 16 \\ x\ 7 \\ 25 \end{matrix} \begin{matrix} (1*16)+ \\ =(-2*16)+ \\ (1*16)+ \end{matrix} \begin{matrix} (-3*7)+ \\ (7*7)+ \\ (-4*7)+ \end{matrix} \begin{matrix} (7*25) \\ (-17*25) \\ (11*25) \end{matrix} \begin{matrix} 170 \\ =-408 \\ 263 \end{matrix} \begin{matrix} 25 \\ \mathrm{mod}29 \\ 2 \end{matrix} \begin{matrix} \mathbf{Y} \\ 27=\_\_ \\ \mathbf{C} \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 4 \\ x22 \\ 13 \end{matrix} \begin{matrix} (1*4)+ \\ =(-2*4)+ \\ (1*4)+ \end{matrix} \begin{matrix} (-3*22)+ \\ (7*22)+ \\ (-4*22)+ \end{matrix} \begin{matrix} (7*13) \\ (-17*13) \\ (11*13) \end{matrix} \begin{matrix} 29 \\ =-75 \\ 59 \end{matrix} \begin{matrix} 0 \\ \mathrm{mod}29 \\ 1 \end{matrix} \begin{matrix} \mathbf{A} \\ 12=\mathbf{M} \\ \mathbf{B} \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 21 \\ x\ 7 \\ 26 \end{matrix} \begin{matrix} (1*21)+ \\ =(-2*21)+ \\ (1*21)+ \end{matrix} \begin{matrix} (-3*7)+ \\ (7*7)+ \\ (-4*7)+ \end{matrix} \begin{matrix} (7*26) \\ (-17*26) \\ (11*26) \end{matrix} \begin{matrix} 182 \\ =-435 \\ 279 \end{matrix} \begin{matrix} 8 \\ \mathrm{mod}29 \\ 18 \end{matrix} \begin{matrix} \mathbf{I} \\ 0=\mathbf{A} \\ \mathbf{R} \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 4 \\ x12 \\ 17 \end{matrix} \begin{matrix} (1*4)+ \\ =(-2*4)+ \\ (1*4)+ \end{matrix} \begin{matrix} (-3*12)+ \\ (7*12)+ \\ (-4*12)+ \end{matrix} \begin{matrix} (7*17) \\ (-17*17) \\ (11*17) \end{matrix} \begin{matrix} 87 \\ =-213 \\ 143 \end{matrix} \begin{matrix} 0 \\ \mathrm{mod}29 \\ 27 \end{matrix} \begin{matrix} \mathbf{A} \\ 19=\mathbf{S} \\ \_\_ \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 20 \\ \text{x } 4 \\ 10 \end{matrix} = \begin{matrix} (1*20)+ \\ (-2*20)+ \\ (1*20)+ \end{matrix} \begin{matrix} (-3*4)+ \\ (7*4)+ \\ (-4*4)+ \end{matrix} \begin{matrix} (7*10) \\ (-17*10) \\ (11*10) \end{matrix} \begin{matrix} 78 \\ -182 \mod 29 \\ 114 \end{matrix} \begin{matrix} 20 \\ 21 \\ 27 \end{matrix} \begin{matrix} \mathbf{T} \\ \mathbf{U} \\ \_\_ \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 7 \\ \text{x } 9 \\ 17 \end{matrix} = \begin{matrix} (1*7)+ \\ (-2*7)+ \\ (1*7)+ \end{matrix} \begin{matrix} (-3*9)+ \\ (7*9)+ \\ (-4*9)+ \end{matrix} \begin{matrix} (7*17) \\ (-17*17) \\ (11*17) \end{matrix} \begin{matrix} 99 \\ -240 \mod 29 \\ 158 \end{matrix} \begin{matrix} 12 \\ 21 \\ 13 \end{matrix} \begin{matrix} \mathbf{M} \\ \mathbf{U} \\ \mathbf{N} \end{matrix}$$

$$\begin{pmatrix} 1 & -3 & 7 \\ -2 & 7 & -17 \\ 1 & -4 & 11 \end{pmatrix} \begin{matrix} 11 \\ \text{x}11 \\ 16 \end{matrix} = \begin{matrix} (1*11)+ \\ (-2*11)+ \\ (1*11)+ \end{matrix} \begin{matrix} (-3*11)+ \\ (7*11)+ \\ (-4*11)+ \end{matrix} \begin{matrix} (7*16) \\ (-17*16) \\ (11*16) \end{matrix} \begin{matrix} -251 \\ -217 \mod 29 \\ 143 \end{matrix} \begin{matrix} 3 \\ 15 \\ 27 \end{matrix} \begin{matrix} \mathbf{D} \\ \mathbf{O} \\ \_\_ \end{matrix}$$

Al desencriptar el mensaje interceptado nos da como resultado la frase:

CAMBIA_TUS_PENSAMIENTOS_Y_CAMBIARAS_TU_MUNDO_

ANALISIS DEL FORO

A partir del foro del trabajo colaborativo se pudo analizar varias de las opiniones, participaciones y procesos individuales que cada uno de los integrantes del grupo compartía de acuerdo a la investigación del método de Cifrado de Hill, resaltando así el conocimiento e investigación que cada uno de los integrantes del grupo iba aportando, retroalimentando la información y corrigiendo algunos temas si esto era necesario.

Se analizo el método de cifrado de Hill, el cual nos dice que se trabaja con módulo 26, al principio no teníamos clara la idea ya que nuestra asignación numérica era diferente, según lo investigado y la información que cada uno tenia sobre el tema, se llego a la conclusión de trabajar nuestra primera actividad con modulo 29. Este análisis se ve evidenciado en el foro del grupo, quizás fue la primera de los muchos interrogantes que teníamos hasta ese momento, pero que poco a poco iban tomando su rumbo, gracias a que cada participante se informaba y a su vez la información documentada la hacía visible para todo el grupo.

También analizamos las operaciones que se procedían a realizar de acuerdo al sistema, teniendo en cuanta que nuestra matriz clave era de 2x2, y que para realizar las operaciones teníamos que trabajar de forma matricial, lo cual al principio no se tenia claro. Hallar la inversa de nuestra matriz clave también fue un tema que se analizo y se trabajo de manera individual, teniendo en cuenta los aportes que cada uno de los integrantes iba desarrollando y a su vez iba compartiendo en el foro, se iban analizando los desarrollos y los procedimientos que cada uno tenía, creando así un dialogo lleno de opiniones y puntos de vista distintos, esto nos llevó a definir las posibles soluciones que podrían darle solución a las actividades dadas en el trabajo colaborativo.

MARCO TEÓRICO

Cifrado de Hill: Es un sistema criptográfico de sustitución poli alfabético, es decir, un mismo signo, en este caso una misma letra, puede ser representado en un mismo mensaje con más de un carácter. Así, en el ejemplo que vamos a analizar a continuación, la letra A del mensaje original aparece representada en el mensaje codificado de tres formas distintas, como C, K e I.

Cifrado: es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo. Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica), distintas (criptografía asimétrica) o de ambos tipos (criptografía híbrida).

Como el producto de matrices, en mayor generalidad se dice que son elementos de un anillo. Una matriz se representa por medio de una letra mayúscula (A, B...) y sus elementos con la misma letra en minúscula (a, b...), con un doble subíndice donde el primero indica la fila y el segundo la columna a la que pertenece.

Determinante: como una forma matrilineal alternada de un cuerpo. Esta definición indica una serie de propiedades matemáticas y generaliza el concepto de determinante haciéndolo aplicable en numerosos campos. Sin embargo, el concepto de determinante o de volumen orientado fue introducido para estudiar el número de soluciones de los sistemas de ecuaciones lineales.

Matriz: es un arreglo bidimensional de números. Dado que puede definirse tanto la suma ese caso se dice que la matriz es de orden n.

Matriz Cuadrada: Es aquella que tiene igual número n de filas que de columnas (n=m).

CONCLUSIONES

En el desarrollo del trabajo nos dimos cuenta de que implementando el Sistema de cifrado Hill podemos Encriptar o desencriptar datos que se quieren proteger y que si no se conoce el procedimiento no será posible descifrar los mensajes ocultos.

Se investigó y aplicó el método de Hill para el desarrollo de los problemas planteados, los cuales fueron resueltos de una manera ordenada y especifica con aportes de los integrantes del equipo ya que se siguió cada paso que correspondía al procedimiento llegando así a un resultado final con un mensaje descifrado que era lo que se buscaba.

BIBLIOGRAFÍA

Criptografia con matrices https://culturacientifica.com/2017/01/11/criptografia-matrices-cifrado-hill/

Cifrado de Hill http://blog.andresed.me/2015/07/cifrado-de-hill.html

Video de cifrado por matrices https://www.youtube.com/watch?v=3X29bcufrOM