



Nombre del Alumno	Diego Joel Zuñiga Frago	Grupo	511																																																												
Fecha de la Práctica	23/09/2022	No. Práctica	6																																																												
Nombre de la Práctica	Criptografía																																																														
Unidad	Matrices Inversas																																																														
CONOCIMIENTOS PREVIOS Operaciones con matrices. Multiplicación de matrices e inversa de una matriz																																																															
OBJETIVO Reconocer diversas formas de representar datos utilizando matrices, realizar operaciones de multiplicación de matrices para la resolución de problemas. Elaborar una hoja de cálculo que realice multiplicación de matrices																																																															
EQUIPO Y MATERIALES Computadora y office																																																															
DESARROLLO																																																															
<p>Con frecuencia los gobiernos, agencias nacionales de seguridad y las empresas se interesan en la transmisión de mensajes codificadas que sean difíciles de descifrar por otros pero que se decodifiquen con facilidad por quienes los reciben. Hay muchas formas interesantes de cifrar o codificar un mensaje, y en su mayor parte usan la teoría de los números o el álgebra lineal.</p>																																																															
<p>1. Método Matriz Invertible con Elementos Enteros.</p>																																																															
<p>a. Codificar</p>																																																															
<p>i. Transformar el mensaje en números asignando un número a cada letra. $A \rightarrow 1, B \rightarrow 2 \dots$ espacio $\rightarrow 0$</p>																																																															
<table border="1"> <tr> <td><i>A</i></td><td><i>B</i></td><td><i>C</i></td><td><i>D</i></td><td><i>E</i></td><td><i>F</i></td><td><i>G</i></td><td><i>H</i></td><td><i>I</i></td><td><i>J</i></td><td><i>K</i></td><td><i>L</i></td><td><i>M</i></td><td><i>N</i></td><td><i>O</i></td></tr> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr> <tr> <td><i>P</i></td><td><i>Q</i></td><td><i>R</i></td><td><i>S</i></td><td><i>T</i></td><td><i>U</i></td><td><i>V</i></td><td><i>W</i></td><td><i>X</i></td><td><i>Y</i></td><td><i>Z</i></td><td>_</td><td>,</td><td>.</td><td>□</td></tr> <tr> <td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>0</td><td>27</td><td>28</td><td>□</td></tr> </table>				<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>L</i>	<i>M</i>	<i>N</i>	<i>O</i>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>	<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>	_	,	.	□	16	17	18	19	20	21	22	23	24	25	26	0	27	28	□
<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>L</i>	<i>M</i>	<i>N</i>	<i>O</i>																																																	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15																																																	
<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>	<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>	_	,	.	□																																																	
16	17	18	19	20	21	22	23	24	25	26	0	27	28	□																																																	
<p>ii. Elegir la matriz cuadrada código C, debe ser una matriz invertible</p>																																																															
<p>iii. Formar la matriz de mensaje M con el mismo número de renglones que la matriz código acomodando los números del mensaje en columnas</p>																																																															
<p>iv. Codificar el mensaje multiplicando la matrices de mensaje por la matriz código $C \cdot M = X$</p>																																																															
<p>b. Enviar</p>																																																															
<p>i. Los valores de la matriz X se convierten en un listado de números y se envían</p>																																																															
<p>c. Decodificar</p>																																																															
<p>i. Decodificación del mensaje. Para recuperar la información del mensaje original, acomodar los números del mensaje en matrices cuadradas del mismo tamaño que la matriz código</p>																																																															
<p>ii. Multiplicar la matriz mensaje por la izquierda por la matriz inversa del código</p>																																																															
$C^{-1}X = C^{-1}C \cdot M$																																																															
$C^{-1}X = M$																																																															
<p>iii. Transformar los números de la matriz obtenida nuevamente en letras</p>																																																															

Ejercicio.

I. Cifra un mensaje

Utiliza el matriz código C para cifrar el siguiente mensaje: **Sin matemáticas no puedes hacer nada, todo a tu alrededor son matemáticas.**

a. Transforma el mensaje a números

19 9 14 0 13 1 20 5 13 1 20 9 3 1 19 0 14 15 0 16 21 5 4 5 19 0 8 1 3 5 18 0 14 1 4 1 27 0 20 15 4 15 0 1 0 20 21
0 1 12 18 5 4 5 4 15 18 0 19 15 14 0 13 1 20 5 13 1 20 9 3 1 19 28

b. Ordena los números en una matriz de 3 x n verticalmente para obtener la matriz del mensaje M

$$M = \begin{pmatrix} 19 & 0 & 20 & 1 & 14 & 16 & 4 & 0 & 3 & 0 & 4 & 0 & 4 & 1 & 21 & 12 & 4 & 15 & 19 & 0 & 20 & 1 & 3 & 28 \\ 9 & 13 & 9 & 19 & 15 & 21 & 5 & 8 & 5 & 14 & 1 & 20 & 15 & 0 & 0 & 18 & 5 & 18 & 15 & 13 & 5 & 20 & 1 & 0 \\ 14 & 1 & 3 & 0 & 0 & 5 & 19 & 1 & 18 & 1 & 27 & 15 & 0 & 20 & 1 & 5 & 4 & 0 & 14 & 1 & 13 & 9 & 19 & 0 \end{pmatrix}$$

c. Multiplica las matrices CM

$$CM = \begin{pmatrix} 52 & 1 & 43 & 2 & 28 & 37 & 27 & 1 & 24 & 1 & 35 & 15 & 8 & 22 & 43 & 29 & 12 & 30 & 52 & 1 & 53 & 11 & 25 & 56 \\ 51 & 27 & 41 & 39 & 44 & 63 & 33 & 17 & 31 & 29 & 33 & 55 & 34 & 21 & 22 & 53 & 18 & 51 & 63 & 27 & 43 & 50 & 24 & 28 \\ 94 & 15 & 75 & 22 & 57 & 79 & 55 & 10 & 50 & 16 & 67 & 50 & 27 & 43 & 65 & 64 & 25 & 63 & 100 & 15 & 91 & 41 & 48 & 84 \end{pmatrix}$$

d. Ordena los números en lista horizontal.

52 51 94 1 27 15 43 41 75 2 39 22 28 44 57 37 63 79 27 33 55 1 17 10 24 31 50 1 29 16 35 33 67 15 55 50 8 34 27 22 21
43 43 22 65 29 53 64 12 18 25 30 51 63 52 63 100 1 27 15 53 43 91 11 50 41 22 24 48 56 28 84

¡Felicidades! Lograste cifrar el mensaje

$$C = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

II. Descifra un mensaje

Utiliza la matriz inversa para descifrar el siguiente mensaje:
43,33,75,1,27,15,53,43,91,11,50,41,25,24,48,15,43,44,9,35,31,30,53,69,10,33,29,24,42,51,39,64,82,1,17,10,69,
44,113,30,43,59,29,58,66,35,57,77,1,27,15,53,43,91,11,50,41,25,52,62,5,31,23,37,63,80,55,67,107,30,53,64.

a. Ordena los números en una matriz de 3 x n verticalmente para obtener la matriz del mensaje codificado X

$$X = \begin{pmatrix} 43 & 1 & 53 & 11 & 25 & 15 & 9 & 30 & 10 & 24 & 39 & 1 & 69 & 30 & 29 & 35 & 1 & 53 & 11 & 25 & 5 & 37 & 55 & 30 \\ 33 & 27 & 43 & 50 & 24 & 43 & 35 & 53 & 33 & 42 & 64 & 17 & 44 & 43 & 58 & 57 & 27 & 43 & 50 & 52 & 31 & 63 & 67 & 53 \\ 75 & 15 & 91 & 41 & 48 & 44 & 31 & 69 & 29 & 51 & 82 & 10 & 113 & 59 & 66 & 77 & 15 & 91 & 41 & 62 & 23 & 80 & 107 & 64 \end{pmatrix}$$

b. Calcula la inversa de la matriz C

$$C^{-1} = \begin{pmatrix} 3 & 1 & -2 \\ 1 & 1 & -1 \\ -5 & -2 & 4 \end{pmatrix}$$

c. Multiplica las matrices $C^{-1}X$

$$C^{-1}X = \begin{pmatrix} 12 & 0 & 20 & 1 & 3 & 0 & 0 & 5 & 5 & 12 & 17 & 0 & 25 & 15 & 13 & 8 & 0 & 20 & 1 & 3 & 0 & 14 & 18 & 15 \\ 1 & 13 & 5 & 20 & 1 & 14 & 13 & 14 & 14 & 15 & 21 & 8 & 0 & 14 & 21 & 15 & 13 & 5 & 20 & 15 & 13 & 20 & 15 & 19 \\ 19 & 1 & 13 & 9 & 19 & 15 & 9 & 20 & 0 & 0 & 5 & 1 & 19 & 0 & 3 & 19 & 1 & 13 & 9 & 19 & 5 & 9 & 19 & 0 \end{pmatrix}$$

d. Transforma los números en letras:

$$C^{-1}X = \begin{pmatrix} L & \square & T & A & C & \square & \square & E & E & L & Q & \square & Y & O & M & H & \square & T & A & C & \square & N & R & O \\ A & M & E & T & A & N & M & N & N & O & U & H & 0 & N & U & O & M & E & T & O & M & T & O & S \\ S & A & M & I & S & O & I & T & \square & \square & E & A & S & \square & C & S & A & M & I & S & E & I & S & \square \end{pmatrix}$$

¿Qué dice el mensaje?

LAS MATEMATICAS NO MIENTEN LO QUE HAY SON MUCHOS MATEMATICOS MENTIROPOS

¡Felicidades! Lograste cifrar el mensaje

III. Envía un mensaje codificado a un compañero y dile cuál es la matriz código

Mensaje: LO QUE NO TE MATA, TE HACE MAS FUERTE

Mensaje en codigo: 12 15 0 17 21 5 0 14 15 0 20 5 0 13 1 20 1 27 0 20 5 0 8 1 3 5 0 13 1 19 0 6 21 5 18 20 5 28

$$C = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

$$M = \begin{pmatrix} 12 & 17 & 0 & 0 & 0 & 20 & 0 & 0 & 3 & 13 & 0 & 5 & 5 \\ 15 & 21 & 14 & 20 & 13 & 1 & 20 & 8 & 5 & 1 & 6 & 18 & 28 \\ 0 & 5 & 15 & 5 & 1 & 27 & 5 & 1 & 0 & 19 & 21 & 20 & 0 \end{pmatrix}$$

$$CM = \begin{pmatrix} 24 & 39 & 15 & 5 & 1 & 67 & 5 & 1 & 6 & 45 & 21 & 30 & 10 \\ 42 & 64 & 43 & 45 & 27 & 49 & 45 & 17 & 13 & 34 & 33 & 61 & 61 \\ 51 & 82 & 44 & 30 & 15 & 115 & 30 & 10 & 14 & 78 & 48 & 73 & 43 \end{pmatrix}$$

IV. Decodifica el mensaje que te envíe un, pídele la matriz código

$$C = \begin{pmatrix} 2 & 0 & 1 \\ 1 & 2 & 1 \\ 3 & 1 & 2 \end{pmatrix}$$

$$X = \begin{pmatrix} 28 & 38 & 39 & 15 & 51 & 1 & 24 & 15 & 41 & 40 & 19 & 70 & 25 & 9 & 5 & 21 & 32 & 30 & 24 & 27 & 39 & 3 & 9 & 48 & 34 & 15 & 25 \\ 44 & 29 & 64 & 59 & 26 & 17 & 31 & 21 & 27 & 31 & 18 & 43 & 56 & 47 & 43 & 55 & 27 & 65 & 23 & 62 & 21 & 10 & 35 & 75 & 19 & 10 & 37 \\ 57 & 62 & 82 & 52 & 77 & 10 & 50 & 33 & 68 & 71 & 33 & 113 & 63 & 37 & 29 & 59 & 59 & 70 & 47 & 67 & 60 & 9 & 31 & 103 & 53 & 25 & 50 \end{pmatrix}$$

$$C^{-1}X = \begin{pmatrix} 14 & 19 & 17 & 0 & 25 & 0 & 3 & 0 & 14 & 9 & 9 & 27 & 5 & 0 & 0 & 0 & 5 & 15 & 1 & 9 & 18 & 1 & 0 & 13 & 15 & 5 & 12 \\ 15 & 5 & 21 & 22 & 0 & 8 & 5 & 3 & 0 & 0 & 4 & 0 & 18 & 19 & 19 & 17 & 0 & 25 & 0 & 22 & 0 & 4 & 13 & 20 & 0 & 0 & 12 \\ 0 & 0 & 5 & 15 & 1 & 1 & 18 & 15 & 13 & 22 & 1 & 16 & 15 & 9 & 5 & 21 & 22 & 0 & 22 & 9 & 3 & 1 & 9 & 22 & 4 & 5 & 1 \end{pmatrix}$$

Mensaje: NO SE QUE VOY A HACER CON MI VIDA, PERO SI SE QUE VOY A VIVIR CADA MINUTO DE ELLA

V. Cuestionario

1. ¿Qué significa la palabra encriptar?

También se le dice cifrar datos y sirve para ocultar el contenido de un mensaje a simple vista.

2. ¿Por qué es importante que la matriz código sea cuadrada?

Es importante para que se le pueda sacar la inversa

3. ¿Por qué es importante que la matriz código tenga inversa?

Para poder encontrar la matriz X con el mensaje, es decir, descifrar el mensaje.

4. ¿Puede utilizarse la Ñ en los mensajes?

No se puede utilizar, porque recorre 1 número a todos los demás, y a la hora de asignarle letras a los

números va a cambiar el mensaje.

5. ¿Qué ocurre si el mensaje es interceptado por el “enemigo”?

Al no tener la matriz código, es casi imposible que descifre el mensaje

6. Si no se está en guerra, ¿para qué sirve la criptografía?

En la actualidad, la aplicación WhatsApp lo utiliza para asegurar los mensajes enviados mediante su plataforma de extremo a extremo.

CONCLUSIONES

Hoy en día nuestra información está más comprometida que nunca, por lo que es bien que las aplicaciones implementen cifrados para proteger nuestros datos. En esta práctica aprendí mucho y aunque fue muy elaborada de hacer, la comprendí al 100%.

EVALUACIÓN DE LA PRÁCTICA

Se evaluará la realización de la práctica mostrando la resolución de cada uno de los ejercicios. El documento se enviará utilizando el campus virtual