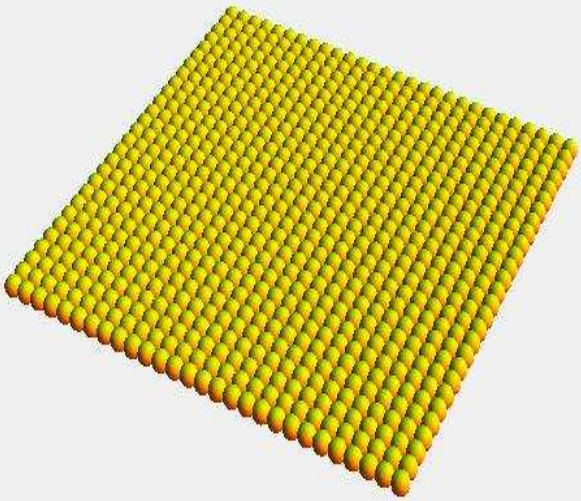
MathCon

The Mathematics Firm

Criptografía

Ejercicios de cifrado usando matrices



www.math.com.mx

José de Jesús Angel Angel
jjaa@math.com.mx

Contenido

Capítulo 1

Criptografía

1.1. Introducción

La criptografía es la ciencia que se encarga de diseñar métodos para mantener confidencial a la información que es enviada por un medio inseguro.

Casi todos los medios de comunicación son inseguros, es decir, un espía siempre puede intervenir una comunicación, y en tal caso conocer su contenido, alterar el contenido, borrar el contenido, etc.

La criptografía entonces usa un algoritmo de cifrado con una clave. Para que el emisor de un mensaje pueda estar seguro que éste sea confidencial, y solo el receptor autorizado pueda saber en contenido aplicando un método de descifrado con su respectiva clave.

La criptografía tiene una amplia historia, ha existido desde los inicios de la civilización.

1.2. Sistema Criptográfico usando Matrices

Sea A una matriz invertible $n \times n$, y M un mensaje con forma de matrix $n \times m$. Entonces, $C = AM$ es el mensaje cifrado. Para poder descifrar el mensaje solo multiplicamos por la matriz inversa A^{-1} a C para obtener el mensaje original.

$$A^{-1}C = A^{-1}AM = IM = M$$

1.2.1. Ejemplo 1

Proceso de preparación.
Para cifrar un mensaje se hace lo siguiente: si el mensaje original es

"HOY ES EL PRIMER DIA"

el primer paso es codificar el mensaje con números de acuerdo a la siguiente tabla:

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
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	

De tal forma que el mensaje queda codificado como:

H	O	Y	_	E	S	_	E	L	_	P	R	I	M	E	R	_	D	I	A
8	15	25	27	5	19	27	5	12	27	16	18	9	13	5	18	27	4	9	1

Dada la clave:

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

Proceso de cifrado.

Como la clave tiene tamaño 3×3, entonces el primer paso para cifrar el mensaje es separar este de 3 letras en tres, completando el mensaje a un múltiplo de 3 con blancos.

H	O	Y	_	E	S	_	E	L	_	P	R	I	M	E	R	_	D	I	A	
8	15	25	27	5	19	27	5	12	27	16	18	9	13	5	18	27	4	9	1	27

El segundo paso es construir la matriz M del mensaje, colocando como columnas cada grupo de 3 letras.

$$M = \begin{pmatrix} 8 & 27 & 27 & 27 & 9 & 18 & 9 \\ 15 & 5 & 5 & 16 & 13 & 27 & 1 \\ 25 & 19 & 12 & 18 & 5 & 4 & 27 \end{pmatrix}$$

Finalmente para obtener el mensaje cifrado, realizamos el producto AM.

$$\begin{aligned} AM &= \begin{pmatrix} -1 & 1 & 1 \\ -2 & -3 & 1 \\ 3 & 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 8 & 27 & 27 & 27 & 9 & 18 & 9 \\ 15 & 5 & 5 & 16 & 13 & 27 & 1 \\ 25 & 19 & 12 & 18 & 5 & 4 & 27 \end{pmatrix} \\ &= \begin{pmatrix} 32 & -3 & -10 & 7 & 9 & 13 & 19 \\ -36 & -50 & -57 & -84 & -52 & -113 & 6 \\ -11 & 48 & 62 & 61 & 30 & 73 & -26 \end{pmatrix} \end{aligned}$$

Proceso de descifrado.

Para descifrar el mensaje simplemente se realiza el producto $A^{-1}C = A^{-1}AM = M$.

$$A^{-1}C = \begin{pmatrix} 5 & 3 & 4 \\ -1 & -1 & -1 \\ 7 & 4 & 5 \end{pmatrix} \cdot \begin{pmatrix} 32 & -3 & -10 & 7 & 9 & 13 & 19 \\ -36 & -50 & -57 & -84 & -52 & -113 & 6 \\ -11 & 48 & 62 & 61 & 30 & 73 & -26 \end{pmatrix}$$

$$= \begin{pmatrix} 8 & 27 & 27 & 27 & 9 & 18 & 9 \\ 15 & 5 & 5 & 16 & 13 & 27 & 1 \\ 25 & 19 & 12 & 18 & 5 & 4 & 27 \end{pmatrix}$$

1.3. Ejercicios

1. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} 7 & 4 & -8 \\ -78 & -30 & -81 \\ -60 & -21 & -67 \end{pmatrix}$$

2. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} 9 & 48 & 64 & 32 \\ 14 & 18 & 29 & 20 \\ -48 & -37 & -61 & -67 \end{pmatrix}$$

3. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} 44 & 45 & 32 & 32 \\ 76 & 86 & 49 & 90 \\ -3 & 14 & -11 & 53 \end{pmatrix}$$

4. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} 116 & 111 & 79 & 69 & 138 \\ 98 & 92 & 61 & 66 & 111 \\ -3 & -1 & 8 & -20 & -1 \end{pmatrix}$$

5. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

$$A = \begin{pmatrix} -5 & 0 & 6 \\ -1 & 3 & 8 \\ 1 & 1 & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 24 & -50 & -89 \\ 149 & 87 & 49 \\ 42 & 42 & 40 \end{pmatrix}$$

6. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

$$A = \begin{pmatrix} 1 & 2 & 2 \\ -1 & 7 & -6 \\ 3 & 13 & 3 \end{pmatrix}$$

$$C = \begin{pmatrix} 69 & 34 & 45 & 82 \\ -6 & -1 & 36 & -23 \\ 258 & 128 & 199 & 294 \end{pmatrix}$$

7. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

$$A = \begin{pmatrix} 5 & 5 & -3 \\ 16 & 10 & -7 \\ -7 & -2 & 2 \end{pmatrix}$$

$$C = \begin{pmatrix} 89 & 101 & 118 & 9 \\ 288 & 195 & 257 & 9 \\ -128 & -35 & -65 & 3 \end{pmatrix}$$

8. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} -48 & -79 & -83 & -54 \\ 15 & 6 & -13 & 21 \\ -32 & -48 & -44 & -38 \end{pmatrix}$$

9. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

$$A = \begin{pmatrix} -6 & 8 & 9 \\ -5 & 11 & 2 \\ -8 & 13 & 9 \end{pmatrix}$$

$$C = \begin{pmatrix} -97 & 99 & 67 & 345 \\ -93 & 46 & 89 & 256 \\ -136 & 112 & 107 & 442 \end{pmatrix}$$

10. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} 53 & 40 & 89 & 102 & 44 & 37 \\ 40 & 46 & 43 & 79 & 40 & 35 \\ -52 & -65 & -48 & -106 & -55 & -49 \end{pmatrix}$$

11. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} 32 & 36 & 17 & 32 & 28 & 14 & 37 \\ 24 & -21 & 10 & -20 & 34 & -17 & 15 \\ 5 & -30 & -5 & -33 & 7 & -19 & -4 \end{pmatrix}$$

12. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} -17 & 5 & -55 & -37 & -67 & 0 & -26 & -65 \\ -14 & 10 & -37 & -36 & -42 & 5 & -5 & -46 \\ -16 & -11 & -38 & -28 & -47 & -9 & -22 & -46 \end{pmatrix}$$

13. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

$$A = \begin{pmatrix} -2 & -2 & -1 \\ -1 & 1 & -2 \\ -2 & -1 & -2 \end{pmatrix}$$

$$C = \begin{pmatrix} -80 & -103 & -81 & -79 & -85 & -75 & -34 & -83 \\ -28 & -26 & -12 & -70 & -53 & -68 & -21 & -28 \\ -77 & -95 & -71 & -101 & -97 & -97 & -37 & -83 \end{pmatrix}$$

14. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} 7 & -14 & -13 & 12 & 8 & 26 & -8 & -8 & 23 \\ 56 & 32 & 48 & 74 & 85 & 63 & 56 & 21 & 85 \\ 12 & 5 & 5 & 27 & 27 & 27 & 13 & 4 & 27 \end{pmatrix}$$

15. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

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

$$C = \begin{pmatrix} -3 & 35 & -17 & 49 & 42 & 41 & -10 & 50 & -3 & 39 & 3 \\ 5 & -29 & 12 & -52 & -53 & -16 & 12 & -33 & 5 & -25 & -28 \\ 2 & 41 & -14 & 64 & 61 & 42 & -9 & 55 & 2 & 44 & 23 \end{pmatrix}$$

16. El mensaje M fue cifrado con la clave A, y se obtuvo el mensaje cifrado C. Encontrar M.

$$A = \begin{pmatrix} 9 & 5 & 10 \\ 1 & 2 & -8 \\ 13 & 10 & -3 \end{pmatrix}$$

$$C = \begin{pmatrix} 375 & 347 & 295 & 368 & 313 & 217 & 417 & 109 & 471 & 410 & 383 & 409 \\ -187 & -100 & -75 & -67 & -5 & 4 & -178 & -19 & -172 & -173 & -202 & -190 \\ 104 & 236 & 220 & 325 & 376 & 275 & 173 & 98 & 251 & 174 & 85 & 140 \end{pmatrix}$$