USO DEL SOFTWARE MATEMÁTICO APLICADO A LA INGENIERÍA, EL CASO DE LA CRIPTOGRAFÍA

María del Carmen López Chávez, Carlos Oropeza Legorreta
Facultad de Estudios Superiores Cuautitlán México
i.a.maria.lopez.chavez@gmail.com, carlos_oropezamx@yahoo.com.es
Campo de investigación: Uso de las Nuevas Tecnologías en la Enseñanza de las Matemáticas Nivel: Superior

Resumen. *En el presente trabajo se reporta la aplicación del concepto de transformación vectorial y matricial, que forma parte de la currícula en el curso de Algebra Lineal que se imparte en la Facultad de Estudios Superiores Cuautitlán. Ésta experiencia centra su atención fundamentalmente en dos aspectos, por una parte, en el concepto mismo y por otra, la articulación de éste con el uso de la tecnología a través del software matemático, como una estrategia metodológica complementaria. En dicha asignatura, la mayor parte de los conceptos se construyen formalmente, esto hace que los estudiantes la perciban demasiado abstracta y declaran que "estudiar conceptos como los que se muestran, carecen de aplicación en la realidad"; con éste trabajo se pretende entre otros objetivos romper con ésta idea tradicional provocando la reflexión y el desarrollo en la adquisición del concepto, a su vez confrontando el aprovechamiento de los estudiantes.*

Palabras clave: criptografía, software, matrices, tecnología

Introducción

Una de las muchas aplicaciones del Álgebra Lineal es el uso de matrices para desarrollar códigos, proceso que involucra la transformación vectorial y matricial, en conjunto con un software para representar graficas, evaluación de datos, y/o simplificación de procesos. A dicho estudio se le denomina Criptografía. La criptografía es la ciencia de crear y descifrar códigos. Durante siglos, los códigos se han utilizado en la diplomacia, los servicios de inteligencia, y las comunicaciones militares. Hoy en día, con tantos datos secretos almacenados en las computadoras, ocultar la información computarizada con códigos se ha convertido en algo muy importante para la industria. A menudo, se utilizan matrices para desarrollar sistemas de códigos. Dentro de éste trabajo pretendemos exponer uno de los diversos usos de la Criptografía, que se basa en la transformación de una gráfica en R^3 a un código matricial, transformándolos a valores específicos haciendo uso de un codificador y su inverso decodificador. Basándonos en los principios básicos de la Criptografía, transformaremos una gráfica de bloques simulando edificios, ubicándolos en el plano tridimensional como vectores, y posteriormente como matrices. Dicho proceso involucra un codificador que nos dará como resultado un código numérico de nuestra gráfica. A su vez

utilizaremos un decodificador para revertir el proceso y obtener una réplica exacta de la gráfica original.

Snyder (1988), explica que la educación matemática desarrolla un aspecto del pensamiento que la lengua verbal no aborda: la *experiencia de la solución*. El niño hace un cálculo y encuentra la solución que puede verificar objetivamente si es la correcta o no. Como Lima (1994), entendemos que la evolución del concepto coincide con la síntesis de la evolución histórica significativa de su creación. Por lo tanto, el concepto matemático es un movimiento de diferenciación y combinación acumulativa de ideas y de superación de transformaciones permanentes del lenguaje verbal en lenguaje operacional y del lenguaje operacional en leguaje verbal, cada salto es significativo para el aprendizaje y acontece a partir de las síntesis anteriores más simples. En este sentido, la *experiencia de la solución* pierde significado si no está comprometida con un contexto determinado, con una problematización que puede ser realizada a través de la asociación de ideas e imágenes, del lenguaje verbal.

Observamos en Kopnin (1978), que el lenguaje es un movimiento evolutivo que parte de las reflexiones y correspondencias más simples, creando redes y nexos crecientemente más amplios, abarcativos y profundos. El aprendizaje de una operación matemática a que se reduce el concepto, necesita apenas de entrenamiento y se realiza como simple sumatoria fragmentada de habilidades y *competencias*.

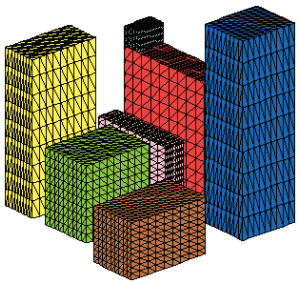
En una educación conceptual, la educación para el lenguaje matemático es intencional y organizada, no es aleatoria ni espontánea.

Análisis

En esta primera etapa se proporciona parte de la información y se da evidencia del uso y manejo del software matemático. Consideramos pertinente mostrar algunas instrucciones que se utilizaron para el desarrollo de la propuesta.

Encodificación

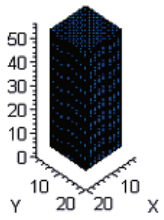
En el desarrollo de la propuesta se plantea mandar un mensaje vía un código en particular, en este caso se trata de un conjunto habitacional el cual se encuentra caracterizado en el espacio de tres dimensiones. El mensaje es el siguiente:



En esta parte se explica la manera de representarlo gráficamente. El desarrollo del primer bloque (azul) se lleva a cabo de la siguiente manera:

```
[> a1:=implicitplot3d({X=1,X=15},X=1..20,Y=1..15,Z=1..50,color=blue):
[> a2:=implicitplot3d({Y=1,Y=15},X=1..15,Y=1..20,Z=1..50,color=blue):
[> a3:=implicitplot3d({Z=1,Z=50},X=1..15,Y=1..15,Z=1..55,color=blue):
```

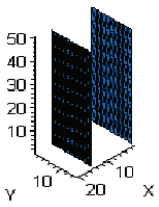
Con los demás bloques, se sigue la misma metodología, cambiando las coordenadas y los colores.



Ya que el objetivo es codificarlo, se necesita saber cómo se va a representar el mensaje en código, se puede tomar como un conjunto de planos con ciertos parámetros; tomando el primer bloque (azul):

```
[> display(a1,a2,a3,scaling=CONSTRAINED,axes=framed);
```

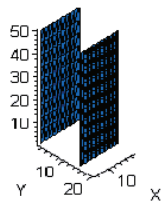
Es un conjunto de 6 planos, divididos en tres los que son perpendiculares al eje *x*:




```
[> display(a1,scaling=CONSTRAINED,axes=framed);
```

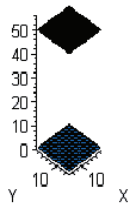
Los que son perpendiculares al eje *y*:

[> display(a2,scaling=CONSTRAINED,axes=framed);



Y los que son perpendiculares al eje *z*:

[> display(a3,scaling=CONSTRAINED,axes=framed);



Podemos observar que en cada parte los planos son iguales, solo varía el valor con respecto al cual son perpendiculares .Ejemplo:

Se observa que los dos valores que se dan con respecto al eje *x* son 1 y 15, además de que se le dan parámetros con respecto a cada eje, con respecto al eje *x* de 1 a 20, con respecto al eje *y* de 1 a 15 y con respecto al eje *z* de 1 a 50, y se tiene éste conjunto de números 1,15 1,20 1,15 1,50 ; los cuales podemos introducir a una matriz de la siguiente manera:

Primero se colocan en una matriz de 3 x 2 los parámetros con respecto a cada eje

$$\begin{bmatrix} 1 & 20 \\ 1 & 15 \\ 1 & 50 \end{bmatrix}$$

Después se convierte a la matriz en una de 3 x 4; colocando el valor que sea con respecto al eje *x* a un lado de los valores de los parámetros con respecto a *x* y se completa la matriz con ceros

$$\begin{bmatrix} 1 & 20 & 1 & 15 \\ 1 & 15 & 0 & 0 \\ 1 & 50 & 0 & 0 \end{bmatrix}$$

Con respecto al eje *y* al eje *z*, se sigue una metodología similar. Lo que permitirá tener tres matrices por un solo un bloque

$$\begin{bmatrix} 1 & 20 & 1 & 15 \\ 1 & 15 & 0 & 0 \\ 1 & 50 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 15 & 0 & 0 \\ 1 & 20 & 1 & 15 \\ 1 & 50 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 15 & 0 & 0 \\ 1 & 15 & 0 & 0 \\ 1 & 55 & 1 & 55 \end{bmatrix}$$

Que transcritas al software se muestran de la siguiente manera:

```
[> M1:=matrix([[1, 20, 1, 15], [1, 15, 0, 0], [1, 50, 0, 0]]):
[> M2:=matrix([[1, 15, 0, 0], [1, 20, 1, 15], [1, 50, 0, 0]]):
[> M3:=matrix([[1, 15, 0, 0], [1, 15, 0, 0], [1, 55, 1, 55]]):
```

Se repite el proceso con cada uno de los bloques. Se asigna una matriz codificadora:

```
[> matriz_de_codificacion:=matrix([[1, 2, 1], [2, 4, 3], [1, 1, 2]]);
```

$$matriz\_de\_codificacion := \begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 3 \\ 1 & 1 & 2 \end{bmatrix}$$

Aplicando la matriz de codificación para cada una de las matrices anteriores se obtiene una nueva serie de matrices que proporcionan el siguiente código tomando en un inicio la primera fila y así sucesivamente:

4,100,1,15 9, 250,2,30 4,135,1,15 4,105,2,30 9,260,4,60 4,135,1,15 4,100,1,50 9,255,3,150
4,140,2,100 28,101,25,55 57,232,50,110 28,123,25,55 28,105,2,16 57,240,4,32 28,125,1,8
28,106,1,30 57,247,3,90 28,133,2,60 82,106,50,55 194,247,100,110 111,133,50,55
82,110,2,16 194,255,4,32 111,135,1,8 82,111,30,35 194,262,90,105 111,143,60,70
72,150,25,40 145,320,50,80 50,130,25,40 72,150,46,80 145,320,92,160 50,125,23,40
72,145,1,20 145,315,3,60 50,130,2,40 92,180,45,55 185,400,90,110 70,180,45,55
92,195,46,80 185,430,92,160 70,185,23,40 92,180,1,40 185,405,3,120 70,185,2,80
51,105,30,55 103,225,60,110 42,105,30,55 51,110,20,30 103,235,40,60 42,105,10,15
51,105,1,15 103,230,3,45 42,110,2,30 52,125,1,15 105,265,2,30 28,95,1,15 52,130,50,90
105,275,100,180 28,95,25,45 52,125,1,15 105,270,3,45 28,100,2,30

Hasta éste punto, ya se tiene el código para mandarlo y decodificarlo.

Decodificación

El código se transforma a matrices obteniendo el siguiente conjunto:

$$\begin{bmatrix} 4 & 100 & 1 & 15 \\ 9 & 250 & 2 & 30 \\ 4 & 135 & 1 & 15 \end{bmatrix}, \begin{bmatrix} 4 & 105 & 2 & 30 \\ 9 & 260 & 4 & 60 \\ 4 & 135 & 1 & 15 \end{bmatrix}, \begin{bmatrix} 4 & 100 & 1 & 50 \\ 9 & 255 & 3 & 150 \\ 4 & 140 & 2 & 100 \end{bmatrix}, \begin{bmatrix} 28 & 101 & 25 & 55 \\ 57 & 232 & 50 & 110 \\ 28 & 123 & 25 & 55 \end{bmatrix},$$

$$\begin{bmatrix} 28 & 105 & 2 & 16 \\ 57 & 240 & 4 & 32 \\ 28 & 125 & 1 & 8 \end{bmatrix}, \begin{bmatrix} 28 & 106 & 1 & 30 \\ 57 & 247 & 3 & 90 \\ 28 & 133 & 2 & 60 \end{bmatrix}, \begin{bmatrix} 82 & 106 & 50 & 55 \\ 194 & 247 & 100 & 110 \\ 111 & 133 & 50 & 55 \end{bmatrix},$$

$$\begin{bmatrix} 82 & 110 & 2 & 16 \\ 194 & 255 & 4 & 32 \\ 111 & 135 & 1 & 8 \end{bmatrix}, \begin{bmatrix} 82 & 111 & 30 & 35 \\ 194 & 262 & 90 & 105 \\ 111 & 143 & 60 & 70 \end{bmatrix}, \begin{bmatrix} 72 & 150 & 25 & 40 \\ 145 & 320 & 50 & 80 \\ 50 & 130 & 25 & 40 \end{bmatrix},$$

$$\begin{bmatrix} 72 & 150 & 46 & 80 \\ 145 & 320 & 92 & 160 \\ 50 & 125 & 23 & 40 \end{bmatrix}, \begin{bmatrix} 72 & 145 & 1 & 20 \\ 145 & 315 & 3 & 60 \\ 50 & 130 & 2 & 40 \end{bmatrix}, \begin{bmatrix} 92 & 180 & 45 & 55 \\ 185 & 400 & 90 & 110 \\ 70 & 180 & 45 & 55 \end{bmatrix},$$

$$\begin{bmatrix} 92 & 195 & 46 & 80 \\ 185 & 430 & 92 & 160 \\ 70 & 185 & 23 & 40 \end{bmatrix}, \begin{bmatrix} 92 & 180 & 1 & 40 \\ 185 & 405 & 3 & 120 \\ 70 & 185 & 2 & 80 \end{bmatrix}, \begin{bmatrix} 51 & 105 & 30 & 55 \\ 103 & 225 & 60 & 110 \\ 42 & 105 & 30 & 55 \end{bmatrix},$$

$$\begin{bmatrix} 51 & 110 & 20 & 30 \\ 103 & 235 & 40 & 60 \\ 42 & 105 & 10 & 15 \end{bmatrix}, \begin{bmatrix} 51 & 105 & 1 & 15 \\ 103 & 230 & 3 & 45 \\ 42 & 110 & 2 & 30 \end{bmatrix}, \begin{bmatrix} 52 & 125 & 1 & 15 \\ 105 & 265 & 2 & 30 \\ 28 & 95 & 1 & 15 \end{bmatrix},$$

$$\begin{bmatrix} 52 & 130 & 50 & 90 \\ 105 & 275 & 100 & 180 \\ 28 & 95 & 25 & 45 \end{bmatrix}, \begin{bmatrix} 52 & 125 & 1 & 15 \\ 105 & 270 & 3 & 45 \\ 28 & 100 & 2 & 30 \end{bmatrix}$$

La matriz decodificadora es la inversa de la codificadora:

```
[> matriz_decodificadora:=inverse(matriz_de_codificacion);
```

$$matriz\_decodificadora := \begin{bmatrix} 5 & -3 & 2 \\ -1 & 1 & -1 \\ -2 & 1 & 0 \end{bmatrix}$$

Se multiplica la matriz decodificadora por cada una de las matrices, y separándolas se obtienen los resultados, dependiendo del eje a manejar; continuando con el ejemplo del bloque azul:

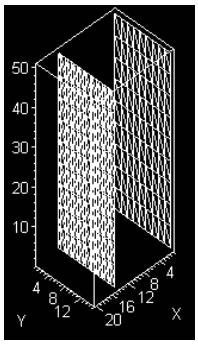
X	Y	Z
1, 20, 1, 15	1, 15, 0, 0	1, 50, 0, 0
25, 55, 25, 55	1, 8, 0, 0	1, 30, 0, 0
50, 55, 50, 55	1, 8, 0, 0	30, 35, 0, 0
25, 50, 25, 40	23, 40, 0, 0	1, 20, 0, 0
45, 60, 45, 55	23, 40, 0, 0	1, 40, 0, 0
30, 60, 30, 55	10, 15, 0, 0	1, 15, 0, 0
1, 20, 1, 15	25, 45, 0, 0	1, 15, 0, 0

Así se obtienen los vectores de la gráfica en R^3, comenzar con el primer renglón:

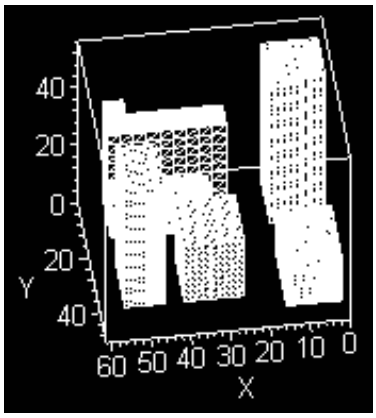
1, 20, 1, 15 1, 15 1, 50

se toman las primeras coordenadas de cada parte en *x* (1, 20), en *y* (1, 15) y en *z* (1, 50), si se grafican solo son puntos en R^2; pero también lo tomamos como parámetros en *x* del 1 al 20, en *y* del 1 al 15 y en *z* del 1 al 50, aunque se tiene otro par de coordenadas en *x* (1,15) y éstos serán los puntos en el eje *x* donde se tomarán los parámetros que se tienen, al graficar se obtiene:

```
[>implicitplot3d({X=1,X=15},X=1..20,Y=1..15,Z=1..50,scaling=CONSTRAINED,axes=boxed,color=white);
```



Se repite el mismo proceso con cada renglón y se obtiene como resultado:



Que como se aprecia, es una réplica de la gráfica original.

Conclusiones

Al hacer uso de la criptografía en el ejemplo mostrado, los estudiantes hacen un reconocimiento de su importancia en el manejo de la codificación y decodificación de señales.

El desarrollo de éste trabajo, generó en la mayoría de los estudiantes participantes la inquietud de continuar con su estudio, para la posible aplicación de la criptografía en el área industrial y en el área mecánica.

Despertó en ellos el interés por el uso del software y comprobaron que con Maple se pueden realizar programas que les proporcionen ventajas en el estudio de conceptos no solamente para la asignatura de Álgebra Lineal, sino en cualquier otra de las que ellos atienden.

Finalmente, reconocieron también que hacer uso del software matemático como una herramienta verificadora, proporciona alternativas en la comprensión de algunos conceptos, que complementa por un lado su formación y por otro acelera la velocidad de respuesta a cuestionamientos que a ellos se les plantea.

Referencias bibliográficas

Antón, H. (2006). *Introducción al álgebra lineal* (3ª edición). México, D. F., México.: Limusa Wiley.

De Burgos, J. (2006). *Álgebra lineal y geometría cartesiana* (3ª edición). Aravaca, Madrid, España.: McGraw-Hill/Interamericana de España, S. A. U.

Grossman, S. I. *Álgebra Lineal* (6ª edición). México, D. F., México.: McGraw-Hill.

Kopnin, P. V. (1978). *A Dialética como Lógica e Teoria del Conhecimento*. Rio de Janeiro: Editora Civilización Brasileira.

Lima, L. (1994). *Momento de criar matemática, contando com coisas.* São Paulo: Cevec, Ciarte.

Poole, D. (2007). *Álgebra lineal una introducción moderna* (2ª edición). México, D. F., México.: Thomson.

Snyder, G. (1998). *Para onde vao as Pedagogias nao-diretivas*. Lisboa: Moraes editores.