Proyecto de Álgebra Lineal
II Término 2017

Facultad de Ciencias Naturales y Matemáticas

Guayaquil, Agosto de 2017

1. Introducción

Criptografía es la ciencia de escribir o descifrar claves. A pesar de que esta materia se asocia frecuentemente con asuntos militares, la criptografía llegó a ser un área importante en los negocios. Las grandes empresas, que procesan enormes cantidades de datos computarizados, deben protegerse constantemente contra lo que se llama espionaje industrial, esto es, el robo de información importante por ser competidores.

Actualmente, hay muchas técnicas extremadamente complejas desarrolladas para garantizar la posibilidad de transmitir grandes cantidades de información en forma confidencial. A esto se llegó después de investigación altamente elaborada hecha por criptógrafos modernos.

Un criptograma común es el siguiente:

KI ZPIIC VPJLP PI PUPJKVG

Esto se puede descifrar usando la tabla decodificadora:

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

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

Notando que K está en el lugar de E, que I sustituye a L, que Z reemplaza a G, etcétera, se llega al mensaje siguiente:

EL GALLO CANTA AL AMANECER

Ahora se verá cómo se pueden usar matrices para crear una clave mucho más difícil de descifrar. Entonces se empieza asignando a cada letra su lugar en el alfabeto ordenado.

(1)

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
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

Supóngase que queremos codificar el mensaje

LAS MATRICES SON AMIGABLES

Descomponemos el mensaje en unidades de igual longitud. Si se escogen longitudes de dos letras se obtiene

$$\text{LA} \quad \text{SM} \quad \text{AT} \quad \text{RI} \quad \text{CE} \quad \text{SS} \quad \text{ON} \quad \text{AM} \quad \text{IG} \quad \text{AB} \quad \text{LE} \quad \text{SX} \tag{2}$$

La X al final simplemente llena el espacio. Si usamos nuestro código numérico (1), podemos escribir (2) como el conjunto de vectores de dos componentes

$$\begin{pmatrix}12\\1\end{pmatrix}\begin{pmatrix}19\\13\end{pmatrix}\begin{pmatrix}1\\20\end{pmatrix}\begin{pmatrix}18\\9\end{pmatrix}\begin{pmatrix}3\\5\end{pmatrix}\begin{pmatrix}19\\19\end{pmatrix}\begin{pmatrix}15\\14\end{pmatrix}\begin{pmatrix}1\\13\end{pmatrix}\begin{pmatrix}9\\7\end{pmatrix}\begin{pmatrix}1\\2\end{pmatrix}\begin{pmatrix}12\\5\end{pmatrix}\begin{pmatrix}19\\24\end{pmatrix} \tag{3}$$

Escogemos una matriz A de 2×2, inversible y entera, con determinante ± 1. Esto asegurará que A^{-1} también tiene sólo componentes enteras. Una matriz con esas condiciones es

$$A = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}.$$

Para continuar, multiplicamos cada uno de los vectores de dos componentes en (3), a la izquierda, por A. Por ejemplo,

$$\begin{pmatrix}12\\1\end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}\begin{pmatrix}12\\1\end{pmatrix} = \begin{pmatrix}15\\16\end{pmatrix}.$$

Así obtenemos el nuevo conjunto de vectores

$$\begin{pmatrix}15\\16\end{pmatrix}\begin{pmatrix}58\\71\end{pmatrix}\begin{pmatrix}61\\81\end{pmatrix}\begin{pmatrix}45\\54\end{pmatrix}\begin{pmatrix}18\\23\end{pmatrix}\begin{pmatrix}76\\95\end{pmatrix}\begin{pmatrix}57\\71\end{pmatrix}\begin{pmatrix}40\\53\end{pmatrix}\begin{pmatrix}30\\37\end{pmatrix}\begin{pmatrix}7\\9\end{pmatrix}\begin{pmatrix}27\\32\end{pmatrix}\begin{pmatrix}91\\115\end{pmatrix} \tag{4}$$

Por último, escribimos (4) así:

$$15\ 16\ 58\ 71\ 61\ 81\ 45\ 54\ 18\ 23\ 76\ 95\ 57\ 71\ 40\ 53\ 30\ 37\ 7\ 9\ 27\ 32\ 91\ 115 \tag{5}$$

Este es nuestro nuevo mensaje codificado, que sería muy difícil de descifrar si no se sabe cuál es la matriz A. Conociendo A,en cambio, es relativamente sencillo. Empezamos rearreglando los números en (5) en grupo de vectores de 2 componentes. Ya que, por ejemplo,

$$\begin{pmatrix}15\\16\end{pmatrix} = A\begin{pmatrix}12\\1\end{pmatrix}$$

tenemos que

$$\begin{pmatrix}12\\1\end{pmatrix} = A^{-1}\begin{pmatrix}15\\16\end{pmatrix}$$

Para comprobar esto, observamos que

$A^{-1} = \begin{pmatrix} 4 & -3 \\ -1 & 1 \end{pmatrix}$ por lo que $A^{-1}\begin{pmatrix} 15 \\ 16 \end{pmatrix} = \begin{pmatrix} 4 & -3 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 15 \\ 16 \end{pmatrix} = \begin{pmatrix} 12 \\ 1 \end{pmatrix} = \begin{pmatrix} \mathrm{L} \\ \mathrm{A} \end{pmatrix}$.

Multiplicando cada uno de los vectores en (4) por A^{-1} se obtendrán los vectores en (3), que se pueden convertir directamente por medio de (1) en el mensaje (2). En este contexto, la matriz A se denomina **matriz codificadora**, y la matriz A^{-1} recibe el nombre de **matriz decodificadora**.

2. El problema

Problema 1.

Codifique el mensaje

MOZART CONQUISTA A TODOS

usando la matriz de codificación

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 4 & -2 & 3 \\ 2 & 1 & 5 \end{pmatrix}$$

y usando la matriz, descífrese lo siguiente

$$8 \quad 63 \quad 66 \quad 2 \quad 106 \quad 161 \quad -2 \quad 1 \quad 10 \quad -6 \quad 19 \quad 53 \quad -6 \quad 96 \quad 180$$

Problema 2.

Utilizando una matriz 7x7 cuyas entradas sean distintas de ceros al menos en un 75 % del total de ellas, codifique y muestre que es posible decodificar el siguiente párrafo.

> Euclides se encontraba impartiendo una clase en Alejandría cuando, uno de sus alumnos, le preguntó que para qué servían todas aquellas demostraciones tan extensas y complejas que explicaba el matemático. Pausadamente, Euclides, se dirigió a otro de los estudiantes presentes y le dijo: Dele una moneda y que se marche. Lo que éste busca no es el saber, es otra cosa.

3. Entregables

Se necesita que su grupo de trabajo elabore un reporte con su solución a este problema. El reporte es un documento con introducción, fundamento teórico, solución, conclusiones, recomendaciones.

Para la sección solución usted deberá presentar:

- El planteamiento matricial del problema
- Resolución del problema
- Resultados numéricos
- Interpretación de los resultados.

Todo lo anterior debe estar escrito de una manera secuencial y con sentido completo. Usted puede (y probablemente debe) ayudarse utilizando herramientas de software para resolver este problema, los mismos que deben ser descritos, y detallar su uso, en el reporte.