UNIVERSIDAD TECNOLÓGICA EMILIANO ZAPATA DEL ESTADO DE MORELOS

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN E INNOVACIÓN DIGITAL
TSU DESARROLLO DE SOFTWARE MULTIPLATAFORMA

FUNDAMENTOS MATEMÁTICOS

TAREA INTEGRADORA: CRIPTOGRAFÍA

PROFESORA

MARÍA MAGDALENA CASAS SAUCEDO

---

04 DE NOVIEMBRE, 2024

Criptografía

Según la Real Academia Española **criptografía** (Del gr. $\kappa\rho\upsilon\pi\tau o\zeta$-kryptós 'oculto' y $\gamma\rho\alpha\phi\eta$-'grafía'.) Se define como el arte de escribir con clave secreta o de un modo enigmático. La criptografía tiene una amplia historia, ha existido desde los inicios de la civilización y se ha utlizado para distintos fines.

Básicamente, la criptografía es la técnica que protege documentos y datos. Actualmente podemos apreciar su funcionamiento a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

A partir de la evolución de las computadoras, la criptografía fue ampliamente divulgada, empleada y modificada, y se constituyó luego con algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

Cifrar un texto en claro para generar un texto cifrado no tiene sentido alguno si no se dispone del proceso inverso, es decir, del proceso que nos permita conocer el texto en claro a partir del texto cifrado. Este proceso se conoce como *descifrado*, y permite al receptor legítimo del mensaje conocer lo que el emisor quería decirle. El proceso completo sería tan sencillo como este:

1. El emisor toma el texto en claro y lo cifra o encripta con un determinado método.
2. El mensaje cifrado se envía al destinatario, e idealmente, si un tercero se hace con el mensaje, no podrá conocer el texto en claro al no conocer el método de cifrado, la clave usada... Es importante la palabra *idealmente* de la frase anterior, ya que hay una parte del arte de la criptografía que trata justo de leer los mensajes sin ser el destinatario legítimo.
3. El receptor legítimo recibe el mensaje cifrado y lo descifra, volviendo así al texto en claro y siendo capaz de leer sin problema lo que el emisor quería comunicarle.

Codificando y descodificando mensajes utilizando matrices

En esta sección se explicará cómo cifrar(codificar) y descifrar (descodificar) mensajes utilizando algunas de las operaciones que se pueden realizar entre matrices.

Vamos a considerar A una matriz invertible de dimensiones $n \times n$, y M será un mensaje con forma de matriz de dimensiones $n \times m$. Entonces, el producto de las matrices A y M será el mensaje cifrado, si llamamos C al mensaje cifrado lo anterior queda representado por

$$C = AM.$$

La matriz A será nuestra clave con la cual podremos tanto cifrar como descrifrar el mensaje que estará dado en la matriz M.

Luego para poder descifrar el mensaje solo multiplicamos por la matriz inversa A^{-1} a C para obtener el mensaje original. En términos matemáticos sería lo siguiente:

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

Veamos un ejemplo.

Ejemplo de cifrado

Consideremos que somos el emisor y que queremos enviar el siguiente mensaje:

"HOLA MUNDO"

cuya clave de cifrado está dada por la matriz A

$$A = \begin{pmatrix} 1 & 1 & 3 \\ -1 & 4 & 0 \\ 3 & 0 & 6 \end{pmatrix}.$$

Nuestro primer paso será 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	

Buscamos codificar el mensaje en matrices de tres renglones, así que separamos nuestro mensaje en partes de tres caracteres:

H	O	L
8	15	12

A	_	M
1	27	13

U	N	D
21	14	4

O	_	_
15	27	27

notemos que el último bloque está conformado por la letra "O", en situaciones como esta en la que el último bloque contenga una o dos letras solamente, los espacios restantes se completan con un espacio. Con esto procedemos a formar la matriz M del mensaje como sigue: colocamos como columnas de la matriz M a los números obtenidos de cada bloque. Notemos también que la matriz resultante es una matriz de 3×4.

$$M = \begin{pmatrix} 8 & 1 & 21 & 15 \\ 15 & 27 & 14 & 27 \\ 12 & 13 & 4 & 27 \end{pmatrix}.$$

Finalmente, para obtener el cifrado multiplicamos las matrices A y M:

$$AM = \begin{pmatrix} 1 & 1 & 3 \\ -1 & 4 & 0 \\ 3 & 0 & 6 \end{pmatrix} \begin{pmatrix} 8 & 1 & 21 & 15 \\ 15 & 27 & 14 & 27 \\ 12 & 13 & 4 & 27 \end{pmatrix} = \begin{pmatrix} 59 & 67 & 47 & 123 \\ 52 & 107 & 35 & 93 \\ 96 & 81 & 87 & 207 \end{pmatrix}$$

Así, el mensaje cifrado que enviaremos a nuestro receptor será

$$C = \begin{pmatrix} 59 & 67 & 47 & 123 \\ 52 & 107 & 35 & 93 \\ 96 & 81 & 87 & 207 \end{pmatrix}.$$

Ejemplo de descifrado

Pasemos ahora al proceso de descrifrado. Si ahora jugamos el papel de receptor, recibiremos un mensaje en código que debemos descifrar. Consideremos que hemos recibido em mensaje C dado por la matriz

$$C = \begin{pmatrix} 59 & 67 & 47 & 123 \\ 52 & 107 & 35 & 93 \\ 96 & 81 & 87 & 207 \end{pmatrix},$$

y que nuestra clave para descrifrarlo es la matriz A

$$A = \begin{pmatrix} 1 & 1 & 3 \\ -1 & 4 & 0 \\ 3 & 0 & 6 \end{pmatrix}.$$

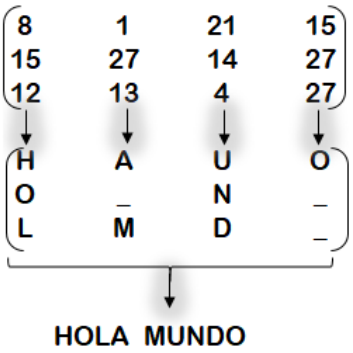
Para descifrar el mensaje simplemente se calcula la inversa de la matriz A, viene dada por

$$A^{-1} = \begin{pmatrix} -4 & 1 & 2 \\ -1 & \frac{1}{2} & \frac{1}{2} \\ 2 & -\frac{1}{2} & -\frac{5}{6} \end{pmatrix}.$$

Como se mencionó en párrafos anteriores, para descodificar el mensaje recibido basta con hacer la multiplicación $A^{-1}C$:

$$A^{-1}C = \begin{pmatrix} -4 & 1 & 2 \\ -1 & \frac{1}{2} & \frac{1}{2} \\ 2 & -\frac{1}{2} & -\frac{5}{6} \end{pmatrix} \begin{pmatrix} 59 & 67 & 47 & 123 \\ 52 & 107 & 35 & 93 \\ 96 & 81 & 87 & 207 \end{pmatrix} = \begin{pmatrix} 8 & 1 & 21 & 15 \\ 15 & 27 & 14 & 27 \\ 12 & 13 & 4 & 27 \end{pmatrix}$$

lo cual si observamos con cuidado es justo la matriz que contiene el mensaje original ‘M”. Para traducir el mensaje numérico que hemos recibido, ahora escribiremos la letra correspondiente al número indicado en cada componente de la matriz M leyendo éstos por columna.



Planteamiento del proyecto

Como proyecto final se te proporcionará una clave y algunos mensajes que en base a lo explicado anteriormente deberás descifrar.

Trabajando con C++

Como pudiste observar, el proceso de cifrado y descifrado de mensajes mostrado en este texto involucra operaciones con matrices. Con ayuda del programa **C++** lleva a cabo las operaciones necesarias para lograr el objetivo de descrifrar los mensajes propuestos. En dicho software deberás desarrollar el código que te permita realizar las operaciones entre matrices de manera exitosa.

En el código:

- Deberás definir la matriz clave A.
- Definirás su inversa.
- Le pedirás al usuario que introduzca el mensaje cifrado C, es decir, la matriz de dimensiones de $3 \times n$, siendo n el número de columnas que tiene la matriz del mensaje que se te ha enviado para descifrar.
- Posteriormente, lleva a cabo la multiplicación $A^{-1}C$ para descubrir el mensaje enviado.
- Finalmente el usuario debe ver en pantalla el mensaje descifrado ya sea la matriz expuesta término a término o bien, el mensaje mostrado letra por letra.

Entrega del proyecto

En este apartado se te indicará cómo deberás entregar el proyecto realizado.

- Entrega un reporte escrito que contenga lo siguiente:

  i) Portada.

  ii) Introducción al tema de criptografía (Puedes usar la que se utiliza en este documento).

  iii) Desarrollo del proyecto.

  iv) Conclusiones del proyecto.

  v) Descripción breve de tus impresiones de la clase en cuanto a contenido y cómo se ha impartido éste (en una sección aparte).

- El archivo se deberá entregar en formato **PDF**.
- Entrega el código que generaste para concluir esta actividad.
- Fecha de entrega: Lunes 2 de diciembre del 2024.

La portada debe llevar la estructura que se indicará en el apartado de googleclasroom llamada **Tarea Integradora**.

Las referencias en las cuales está basado el proyecto se encontrarán disponibles en el apartado de googleclassroom **Bibliografía** de la tarea integradora.

En la parte desarrollo del proyecto, debes presentar de manera general los cálculos en los cuales están basados tus resultados; cómo defines una matriz, cómo defines su matriz inversa, cómo se define el producto de matrices, no es necesario que expongas todos los cálculos para cada ejemplo, puedes indicar los productos así como en el ejemplo que se muestra en este documento y mostrar el resultado final de ellos, fíjate que no se muestran explícitamente los cálculos para determinar cada entrada de cada matriz. Deberás mostrar también tus resultados finales, **el mensaje descifrado**, como matriz y como texto. Puedes añadir el código de tu programa, recuerda que el programa lo debes entregar a parte.

Un integrante del equipo deberá mandar el reporte escrito y el programa a mi correo electrónico:

mariacasas@utez.edu.mx

con el **asunto**: Tarea Integradora Criptografía.

En el texto del mensaje indicará el nombre de los integrantes del proyecto, el grupo al que pertenecen y la materia en la cual están presentando el proyecto.