DIRECCIÓN ACADÉMICA
VICERRECTORADO ACADÉMICO

Facultad de Ingeniería

Carrera de Ciencia de Datos e Inteligencia Artificial

Informe de Actividad de Investigación Formativa

Periodo Académico

2024-2S

Contenido

1. Autor

Ordoñez Yaguana Luis Gonzalo

2. Personal Académico

2.1.Director de Carrera

Mgs. Milton Paúl López Ramos

2.2.Profesor de Asignatura

Dr. Daniel Alejandro Lagos Llaguno

3. Resultados de aprendizaje de la asignatura:

- ✓ Resuelve problemas de aplicación que se pueden representar a través de sistemas de ecuaciones aplicando las definiciones y teoremas de matrices.
- ✓ Aplica las transformaciones lineales y sus propiedades para la solución de ejercicios y problemas de ingeniería

4. Tema de la actividad de la investigación formativa:

Cifrado de Hill y su aplicación práctica.

5. Objetivos de la(s) actividad(es):

5.1.Objetivo General

Demostrar el funcionamiento del Cifrado de Hill a través de una implementación práctica en Octave, explicando su proceso de cifrado y descifrado mediante el uso de matrices como claves.

5.2.Objetivos específicos

5.2.1. Primer objetivo específico: Explicar los principios matemáticos que sustentan el Cifrado de Hill, con un enfoque en las operaciones matriciales necesarias para su implementación.

5.2.2. Segundo objetivo específico: Diseñar un programa en Octave que permita a los usuarios cifrar y descifrar mensajes utilizando el Cifrado de Hill.

5.2.3. Tercer objetivo específico: Implementar una interfaz básica en Octave que facilite la interacción del usuario con el programa de cifrado y descifrado, permitiendo la introducción de mensajes y claves de forma intuitiva.

6. Fecha de la ejecución

9 de febrero de 2025

7. Desarrollo del Informe

7.1.Introducción

El cifrado de Hill fue inventado, basándose en el álgebra lineal, por el matemático norteamericano Lester S. Hill en 1929, y aparece explicado en su artículo *Cryptography in an Algebraic Alphabet*, publicado en *The American Mathematical Monthly*. [1,2]

Lester S. Hill es conocido por ser uno de los primeros en usar principios algebraicos y operaciones matriciales para el cifrado de mensajes basado en la sustitución poligráfica la principal innovación del cifrado de Hill fue su capacidad para operar con más de tres símbolos a la vez, lo que lo diferenciaba de otros cifrados poligráficos de la época.

Este algoritmo represento un gran avance en su tiempo en términos de criptografía y seguridad en la transmisión de datos, siendo un sistema de cifrado por bloques que utiliza operaciones matriciales para encriptar texto plano y convertirlo en texto cifrado. Este enfoque matemático no solo introdujo un alto nivel de sofisticación en su época, sino que también sentó las bases para comprender el potencial de las matrices en la criptografía.

Aunque hoy en día existen algoritmos más avanzados como RSA, AES el cifrado de Hill es un ejemplo clásico que ilustra como el algebra lineal puede ser usada en problemas prácticos. [3,4]

Lester Hill introdujo su método en un contexto donde la criptografía estaba evolucionando continuamente, pasando técnicas de cifrados manuales como el cifrado de sustitución simple a enfoques más complejos basados en matemáticas.

Por ejemplo, si un mensaje como "HOLA" se convierte en valores numéricos según el alfabeto (H=7, O=14, L=11, A=0), y se utiliza una matriz clave para multiplicar estos valores, el resultado es un texto cifrado que solo puede descifrarse conociendo la inversa de la matriz clave.

- Cada letra del mensaje se convierte en un número según su posición en el alfabeto (A=0, B=1, ..., Z=25).
- El mensaje se divide en bloques del mismo tamaño que la matriz clave. Si el mensaje no tiene suficientes letras para completar un bloque, se agregan caracteres de relleno.
- Cada bloque de texto plano se representa como un vector y se multiplica por la matriz clave. Los resultados se toman módulo 26 para asegurarse de que los valores resultantes correspondan a letras del alfabeto.
- Los vectores resultantes se convierten nuevamente en letras, produciendo el mensaje cifrado.
- Para recuperar el mensaje original, se multiplica cada bloque cifrado por la inversa de la matriz clave, aplicando también el módulo 26. [5]

El Cifrado de Hill representa un puente entre las técnicas criptográficas tradicionales y los sistemas modernos. Su enfoque basado en matrices no solo demuestra la aplicación práctica de conceptos matemáticos, sino que también inspira nuevas formas de proteger información en un mundo digital en constante cambio. En este proyecto, se busca demostrar el funcionamiento del Cifrado de Hill mediante una implementación práctica en Octave, un entorno computacional ampliamente utilizado para el cálculo matricial y el análisis numérico. Esta demostración incluirá el desarrollo de un programa capaz de cifrar y descifrar mensajes, mostrando cada etapa del proceso de transformación del texto. Este trabajo ofrece una comprensión detallada del Cifrado de Hill desde una perspectiva técnica y aplicada, destacando su contribución a la seguridad de la información y su utilidad como recurso didáctico. La implementación en Octave permitirá visualizar cómo las operaciones matemáticas subyacentes se traducen en un sistema funcional de cifrado, fomentando así un mayor entendimiento de los fundamentos criptográficos y su aplicabilidad en la protección de datos.

7.2.Descripción de la metodología

La metodología de la investigación se basó en un enfoque teórico-práctico para implementar el Cifrado de Hill. Primero, se realizó una revisión teórica de los fundamentos matemáticos, como matrices, determinantes e inversas modulares, apoyada en bibliografía especializada. Luego, se diseñó y desarrolló un programa en Octave que permite cifrar y descifrar mensajes utilizando una matriz clave, incorporando una interfaz gráfica para facilitar la interacción del usuario. Se implementaron las operaciones matemáticas necesarias, como la multiplicación de matrices y el cálculo de la inversa modular, y se validó el programa mediante pruebas con diferentes mensajes y claves. Finalmente, se documentó el proceso y se presentaron los resultados, demostrando la aplicabilidad del Cifrado de Hill como herramienta didáctica en criptografía.

7.3.Descripción de la(s) acción(es) realizadas

El cifrado de Hill opera sobre la base de un marco matemático específico, cuyos componentes se describirán a continuación. Este marco se fundamenta en el álgebra lineal, particularmente en el manejo de matrices y aritmética modular.

1. Representación de Texto en Criptografía:

El Cifrado de Hill trabaja con bloques de texto representados numéricamente. Cada carácter se asigna a un número según el alfabeto:

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
0	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

El texto se organiza en vectores columna de tamaño n, según la dimensión de la matriz clave.

2. La Matriz Clave:

La matriz clave K es una matriz cuadrada de dimensiones $n \times n$, utilizada para cifrar los bloques de texto. Sus características principales son:

- Debe ser invertible en aritmética modular (mod 26 en el caso de cifrado alfabético).
- El determinante de K debe tener un inverso modular.

3. Operaciones Clave:

- Multiplicación Matricial: Se utiliza para transformar el mensaje original (P) en el texto cifrado (C):

$$C = (K \cdot P) mod 26$$

- Determinante de una Matriz: El determinante $(\det(K))$ es esencial para verificar si K es invertible. Para este proyecto usaremos la ley de cofactores para un uso más generalizado y practico a matrices de tamaño $n \times n$ donde:

La ley de cofactores establece que el determinante de una matriz cuadrada A puede calcularse como la suma de los productos de los elementos de una fila o columna por sus respectivos cofactores. [6]

El menor M_{ij} de un elemento a_{ij} es el determinante de la sub matriz que se obtiene al eliminar la fila i y la columna j de la matriz original.

El cofactor C_{ij} de un elemento a_{ij} está dado por:

$$C_{ij} = (-1)^{i+j} M_{ij}$$

$(-1)^{i+j}$ introduce un signo positivo o negativo dependiendo de la posición del elemento en la matriz.

M_{ij} es el determinante del menor asociado al elemento a_{ij}.

Si seleccionas la fila i, el determinante de A se calcula como:

$$\det(A) = \sum_{i=1}^{n} a_{ij} C_{ij}$$

Si seleccionas la fila j, el determinante de A se calcula como:

$$\det(A) = \sum_{j=1}^{n} a_{ij} C_{ij}$$

- Inversa Modular de una Matriz: La matriz clave invertida (K^{-1}) se obtiene mediante la fórmula:

$$K^{-1} = \big(det(K^{-1}) \cdot Adj(K)\big) mod\ 26$$

Donde:

$\det(K)^{-1}$ es el inverso modular del determinante.

$Adj(K)$ es la matriz adjunta de K.

4. Cifrado y Descifrado:

Cifrado: Para cifrar un bloque de texto P:

$$C = (K \cdot P)\ mod\ 26$$

Descifrado: Para recuperar el mensaje original P, se utiliza la inversa de la matriz clave:

$$P = (K^{-1} \cdot C)\ mod\ 26$$

Ahora revisaremos un ejemplo práctico para poder comprender los fundamentos matemáticos que respaldan el cifrado de Hill.

Para la encriptación usaremos la palabra “CODIGO” eliminando signos ortográficos.

- Seleccionamos una matriz clave de tamaño 2x2:

$$k = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

- La matriz clave debe ser invertible en módulo 26. Su determinante es:

$$\det(K) = (3 \cdot 5 - 3 \cdot 2)$$

$$\det(K) = 15 - 6$$

$$\det(K) = 9$$

El determinante 9 es válido porque tiene un inverso módulo 26, lo que permite descifrar el mensaje después.

- Asignamos a cada letra un valor numérico según su posición en el alfabeto:

$$C = 2, O = 14, D = 3, I = 8, G = 6, O = 14$$

- En este caso rompemos la estructura en bloques de 2 caracteres:

$$Bloques: [C, O], [D, I], [G, O]$$

$$Bloques\ numéricos: \begin{bmatrix} 2 \\ 14 \end{bmatrix}, \begin{bmatrix} 3 \\ 8 \end{bmatrix}, \begin{bmatrix} 6 \\ 14 \end{bmatrix}$$

- La fórmula para cifrar es:

$$C = (K \cdot P)\ mod\ 26$$

$$C = bloque\ de\ cifrado, K = matriz\ clave, P = Bloque\ del\ mensaje\ orginal$$

- Cifrado del primer bloque [2,14]:

$$C = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 14 \end{bmatrix}\ mod\ 26$$

Multiplicamos:

$$C = \begin{bmatrix} (3 \cdot 2 + 3 \cdot 14) \\ (2 \cdot 2 + 5 \cdot 14) \end{bmatrix} = \begin{bmatrix} 6 + 42 \\ 4 + 70 \end{bmatrix} = \begin{bmatrix} 48 \\ 74 \end{bmatrix}\ mod\ 26$$

Reducimos módulo 26:

$$C = \begin{bmatrix} 48\ mod\ 26 \\ 74\ mod\ 26 \end{bmatrix} = \begin{bmatrix} 22 \\ 22 \end{bmatrix}$$

El bloque cifrado es:

$$c_1 = [22, 22] \qquad (W, W)$$

- Cifrado del segundo bloque [3, 8]:

$$C = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 8 \end{bmatrix}\ mod\ 26$$

Multiplicamos:

$$C = \begin{bmatrix} (3 \cdot 3 + 3 \cdot 8) \\ (2 \cdot 3 + 5 \cdot 8) \end{bmatrix} = \begin{bmatrix} 9 + 24 \\ 6 + 40 \end{bmatrix} = \begin{bmatrix} 33 \\ 46 \end{bmatrix}\ mod\ 26$$

Reducimos módulo 26:

$$C = \begin{bmatrix} 33\ mod\ 26 \\ 46\ mod\ 26 \end{bmatrix} = \begin{bmatrix} 7 \\ 20 \end{bmatrix}$$

El bloque cifrado es:

$$c_2 = [7, 20] \qquad (H, U)$$

- Cifrado del tercer bloque [6, 14]:

$$C = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ 14 \end{bmatrix}\ mod\ 26$$

Multiplicamos:

$$C = \begin{bmatrix} (3 \cdot 6 + 3 \cdot 14) \\ (2 \cdot 6 + 5 \cdot 14) \end{bmatrix} = \begin{bmatrix} 18 + 42 \\ 12 + 70 \end{bmatrix} = \begin{bmatrix} 60 \\ 82 \end{bmatrix}\ mod\ 26$$

Reducimos módulo 26:

$$C = \begin{bmatrix} 60\ mod\ 26 \\ 82\ mod\ 26 \end{bmatrix} = \begin{bmatrix} 8 \\ 4 \end{bmatrix}$$

El bloque cifrado es:

$$c_3 = [8, 4] \qquad (I, E)$$

- Resultado final del mensaje cifrado:

$$C_1 = WW \qquad C_2 = HU \qquad C_3 = IE$$

Mensaje cifrado: "WWHUIE".

Hemos cifrado el mensaje "CODIGO" utilizando el Cifrado de Hill con una matriz clave de2×2. Este proceso demuestra cómo las herramientas matemáticas, como matrices se aplican en criptografía para garantizar la seguridad de la información. [7]

Ahora vamos a descifrar el mensaje:

$$Inversa = \frac{1}{determinante} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$determinante = 9$$

$$9 \cdot x \equiv mod\ 26$$

$$9 \cdot 3 = 27 \equiv mod\ 26$$

$$inverso\ de\ 9\ modulo\ 26\ es = 3$$

La matriz inversa es:

$$\frac{1}{9} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} = 3 \cdot \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix}$$

$$\begin{bmatrix} 5 \cdot 3 & -3 \cdot 3 \\ -2 \cdot 3 & 3 \cdot 3 \end{bmatrix} = \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} mod\ 26$$

Tomando los resultados módulo 26:

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

$$inversa = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

Multiplicamos la matriz inversa por cada par de la siguiente manera:

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 22 \\ 22 \end{bmatrix} = \begin{bmatrix} 704 \\ 638 \end{bmatrix} \text{ mod } 26$$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 7 \\ 20 \end{bmatrix} = \begin{bmatrix} 445 \\ 320 \end{bmatrix} \text{ mod } 26$$

$$\begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 8 \\ 4 \end{bmatrix} = \begin{bmatrix} 188 \\ 196 \end{bmatrix} \text{ mod } 26$$

Tomamos los resultados de módulo 26:

$$704\ mod\ 26 = 2\ y\ 638\ mod\ 26 = 14$$

$$445\ mod\ 26 = 3\ y\ 320\ mod\ 26 = 8$$

$$188\ mod\ 26 = 3\ y\ 196\ mod\ 26 = 14$$

Entonces tenemos los pares:

$$[2,14], [3,8], [3,14]$$

Finalmente desciframos el mensaje:

$$2 = C, 14 = O, 3 = D, 8 = I, 3 = G, 14 = O - - - -> \text{“CODIGO”}$$

El descifrado en el cifrado de Hill consiste en revertir el proceso de cifrado utilizando la matriz inversa de la clave. Se toma el texto cifrado, se agrupa en pares de letras como en el cifrado, y se multiplica cada grupo por la matriz inversa de la clave, aplicando una operación modular para garantizar que los resultados se mantengan dentro del rango del alfabeto. Finalmente, los valores obtenidos se convierten nuevamente en letras para reconstruir el mensaje original. Este método garantiza que, con la matriz inversa correcta, el texto cifrado se transforme de vuelta al texto claro original. [8,9]

Ahora veremos la aplicación del cifrado de Hill presentando el código desarrollado en Octave. Este programa permite cifrar y descifrar mensajes utilizando operaciones matriciales y una interfaz gráfica sencilla, diseñada para facilitar su uso. Además, se han incorporado comentarios en el código para explicar cada paso del proceso.

Código:

```
% Función principal
function hill_cipher_gui()
    % Crear la ventana de la interfaz gráfica
    fig = figure('Name', 'Cifrado Hill', 'Position', [500, 300, 400, 400]);

    % Etiquetas y campos de texto para el mensaje y la clave
    uicontrol('Style', 'text', 'Position', [50, 290, 300, 20], 'String', 'Mensaje a cifrar:',
'HorizontalAlignment', 'left');
```

```
    inputMessage = uicontrol('Style', 'edit', 'Position', [50, 260, 300, 25]);
    uicontrol('Style', 'text', 'Position', [50, 220, 300, 20], 'String', 'Clave 2x2
Ejemplo:(0,0;0,0)', 'HorizontalAlignment', 'left');
    inputKey = uicontrol('Style', 'edit', 'Position', [50, 190, 300, 25]);
    % Botones para cifrar y descifrar
    uicontrol('Style', 'pushbutton', 'Position', [50, 130, 120, 30], 'String', 'Cifrar', 'Callback',
@(~, ~) cifrarCallback());
    uicontrol('Style', 'pushbutton', 'Position', [200, 130, 120, 30], 'String', 'Descifrar',
'Callback', @(~, ~) descifrarCallback());
    % Área de resultado para mostrar el cifrado o descifrado
    resultBox = uicontrol('Style', 'text', 'Position', [50, 50, 300, 40], 'String', '',
'HorizontalAlignment', 'left');
    % Mostrar el crédito al final de la interfaz
    uicontrol('Style', 'text', 'Position', [50, 10, 300, 20], 'String', 'Desarrollado por Luis
Ordoñez', 'HorizontalAlignment', 'center');
    % Función de cifrado
    function cifrarCallback()
        % Obtener el mensaje y la clave ingresados por el usuario
        mensaje = get(inputMessage, 'String');
        claveStr = get(inputKey, 'String');
        clave = str2num(['[', claveStr, ']']); %#ok<ST2NM>
        % Validar entrada del usuario
        if isempty(mensaje) || isempty(clave) || ~isequal(size(clave), [2, 2])
            set(resultBox, 'String', 'Por favor ingresa un mensaje y una clave válida.');
            return;
        end
        % Realizar el cifrado
        mensajeCifrado = cifrarHill(mensaje, clave);
        % Mostrar el resultado cifrado
        set(resultBox, 'String', ['Cifrado: ', mensajeCifrado]);
    end
    % Función de descifrado
    function descifrarCallback()
        % Obtener el mensaje y la clave ingresados por el usuario
        mensaje = get(inputMessage, 'String');
        claveStr = get(inputKey, 'String');
        clave = str2num(['[', claveStr, ']']);
        % Validar entrada del usuario
        if isempty(mensaje) || isempty(clave) || ~isequal(size(clave), [2, 2])
            set(resultBox, 'String', 'Por favor ingresa un mensaje y una clave válida.');
            return;
        end
        % Intentar descifrar el mensaje
        try
            mensajeDescifrado = descifrarHill(mensaje, clave);
            % Mostrar el resultado descifrado
            set(resultBox, 'String', ['Descifrado: ', mensajeDescifrado]);
        catch
            % Mostrar error si la clave no tiene inversa modular
            set(resultBox, 'String', 'Error: la clave no tiene inversa modular.');
```

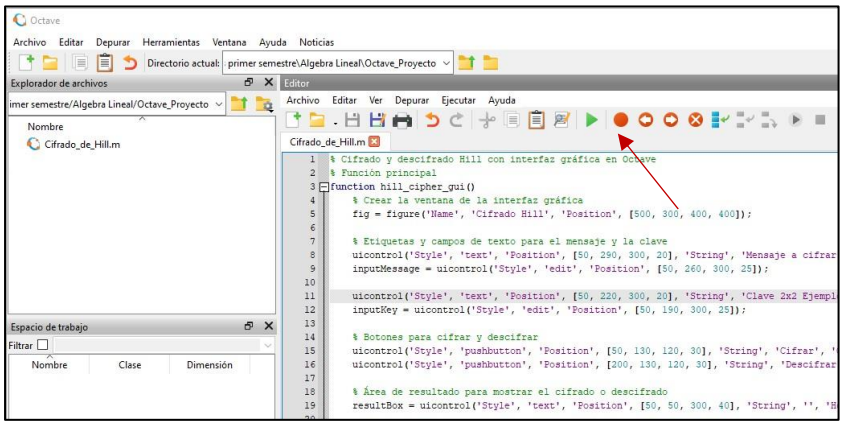
```
        end
    end
end
% Función para cifrar usando el cifrado de Hill
function mensajeCifrado = cifrarHill(mensaje, clave)
    % Preprocesar el mensaje para eliminar caracteres no válidos y completar con X
    mensaje = preprocessMessage(mensaje);
    % Convertir el mensaje a formato numérico (A=0, B=1, ..., Z=25)
    mensajeNumerico = charToNum(mensaje);
    % Aplicar la matriz clave para cifrar el mensaje
    mensajeCifradoNumerico = mod(clave * reshape(mensajeNumerico, 2, []), 26);
    % Convertir el mensaje cifrado a formato de texto
    mensajeCifrado = numToChar(mensajeCifradoNumerico(:)');
end
% Función para descifrar usando el cifrado de Hill
function mensajeDescifrado = descifrarHill(mensaje, clave)
    % Preprocesar el mensaje para eliminar caracteres no válidos y completar con X
    mensaje = preprocessMessage(mensaje);
    % Convertir el mensaje a formato numérico (A=0, B=1, ..., Z=25)
    mensajeNumerico = charToNum(mensaje);
    % Calcular la inversa modular de la clave
    detClave = mod(det(clave), 26); % Determinante de la matriz clave mod 26
    inversaDetClave = modInverse(detClave, 26); % Inversa modular del determinante
    adjClave = round(det(clave) * inv(clave)); % Matriz adjunta de la clave
    claveInversa = mod(inversaDetClave * adjClave, 26); % Clave inversa mod 26

    % Aplicar la matriz inversa para descifrar el mensaje
    mensajeDescifradoNumerico = mod(claveInversa * reshape(mensajeNumerico, 2, []), 26);
    % Convertir el mensaje descifrado a formato de texto
    mensajeDescifrado = numToChar(mensajeDescifradoNumerico(:)');
end
% Convertir caracteres a números (A=0, B=1, ..., Z=25)
function nums = charToNum(chars)
    nums = double(upper(chars)) - double('A');
end
% Convertir números a caracteres (0=A, 1=B, ..., 25=Z)
function chars = numToChar(nums)
    chars = char(mod(nums, 26) + double('A'));
end
% Preprocesar el mensaje (convertir a mayúsculas y completar con X si es necesario)
function mensaje = preprocessMessage(mensaje)
    % Convertir el mensaje a mayúsculas y eliminar caracteres no alfabéticos
    mensaje = upper(regexprep(mensaje, '[^A-Z]', ''));
    % Completar el mensaje con 'X' si su longitud no es múltiplo de 2
    if mod(length(mensaje), 2) ~= 0
        mensaje = [mensaje, 'X'];
    end
end

% Calcular la inversa modular
```

```
function inv = modInverse(a, m)
    % Utilizar el algoritmo extendido de Euclides para calcular la inversa modular
    [g, x, ~] = gcd(a, m);
    if g ~= 1
        error('No existe inversa modular.');
    end
    inv = mod(x, m);
end
```

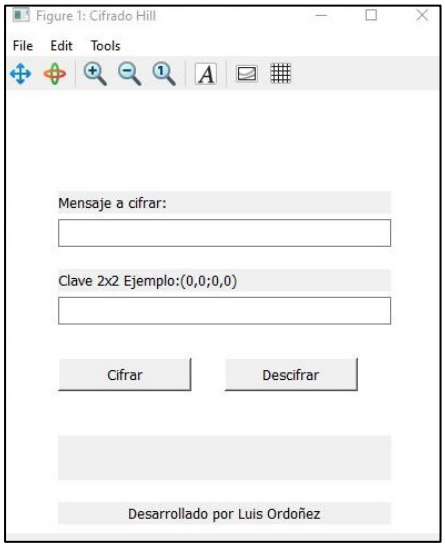
La aplicación incluye una interfaz gráfica (GUI) que facilita la interacción del usuario, mostrando opciones para cifrar, descifrar. El mensaje de entrada se convierte en valores numéricos según su posición en el alfabeto, y la matriz clave de 2x2 se utiliza para cifrar los valores del mensaje, realizando las operaciones en módulo 26. Para el descifrado, se calcula la matriz inversa modular de la clave y se aplica al mensaje cifrado para recuperar el texto original.

A continuación, se visualizará la ejecución del programa:

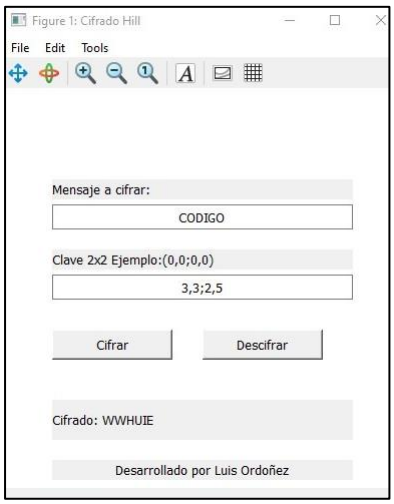
- Ejecutamos el proyecto en Octave:



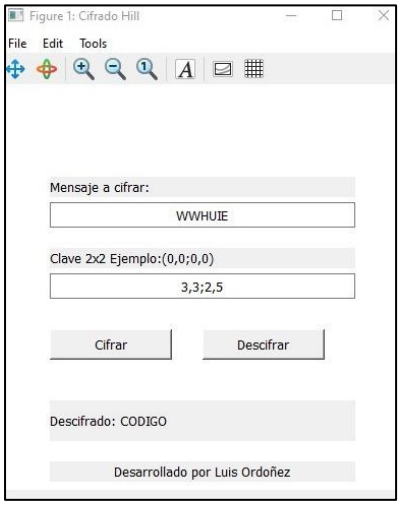
- Contiene una interfaz gráfica básica e intuitiva:



- Ingresar una palabra a cifrar, además una matriz clave 2x2 que debe cumplir con la condición de ser invertible:



- Para descifrar usamos el mensaje ya cifrado y lo escribimos en mensaje a cifrar, debe ser con su matriz clave usada en el cifrado:



Una de las principales enseñanzas que deja este cifrado es la importancia de las matemáticas y las estructuras algebraicas en la criptografía. A través del uso de matrices y operaciones modulares, el cifrado de Hill marco un paso hacia la automatización y sofisticación de los sistemas de cifrado, lo que permitió garantizar una mayor seguridad en los mensajes, incluso ante la posibilidad de ser interceptados.

Hoy en día, sistemas como RSA y AES, que utilizan claves mucho más largas y algoritmos matemáticos complejos, son más efectivos frente a los avances en la capacidad de cómputo y los métodos de criptoanálisis. A pesar de esto, el cifrado de Hill sigue siendo una pieza fundamental en la historia de la criptografía, ayudando a sentar las bases para la evolución de métodos más sofisticados que protegen las comunicaciones modernas.

7.4.Resultados

Los resultados obtenidos en esta investigación formativa demuestran el correcto funcionamiento del Cifrado de Hill a través de su implementación práctica en Octave. El programa desarrollado permitió cifrar y descifrar mensajes de manera eficiente, validando los principios matemáticos y criptográficos que sustentan este método. A continuación, se destacan los principales hallazgos:

- Se logró diseñar y programar un sistema en Octave que realiza las operaciones de cifrado y descifrado utilizando matrices como clave. El programa convierte el texto en valores numéricos, aplica la matriz clave y realiza operaciones en módulo 26 para obtener el texto cifrado o descifrado.
- El proyecto permitió aplicar conceptos de álgebra lineal, como la multiplicación de matrices, el cálculo de determinantes y la obtención de inversas modulares, demostrando su utilidad en problemas prácticos de criptografía.
- La implementación del Cifrado de Hill en Octave sirvió como una herramienta didáctica para comprender los fundamentos de la criptografía clásica y su evolución hacia métodos más avanzados.
- El proyecto destacó la relevancia de las matemáticas en la seguridad de la información, mostrando cómo conceptos teóricos pueden traducirse en aplicaciones prácticas.

En conclusión, los resultados obtenidos confirman que el Cifrado de Hill, aunque simple en comparación con métodos modernos, es una herramienta efectiva para entender los principios básicos de la criptografía y la aplicación de las matemáticas en la protección de datos.

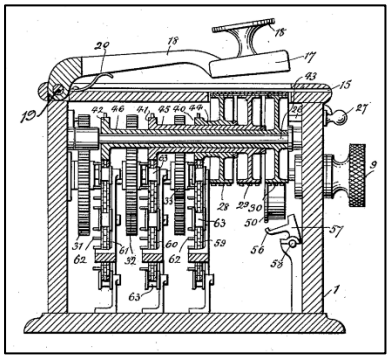
7.5.Bibliografía

[1] L. S. Hill, Cryptography in an Algebraic Alphabet, (n.d.).
[2] R. Ibáñez, *Criptografía con matrices, el cifrado de Hill*, https://culturacientifica.com/2017/01/11/criptografia-matrices-cifrado-hill/.
[3] D. Penazzi, CRIPTOGRAFIA DE CLAVE SIM´ETRICA: AES, (n.d.).
[4] C. C. Castro, Criptografia RSA, (n.d.).
[5] M. G. Larragan, *¿Qué Significa El Emblema de La Profesión Informática? (I), Criptografía (XXIII): Cifrado de Hill (I)*, https://mikelgarcialarragan.blogspot.com/2015/03/criptografia-i.html.
[6] J. P. Bonfim, O DETERMINANTE DE UMA MATRIZ, (n.d.).
[7] *Seguridad Informática I - Cifrado de Hill* (n.d.).
[8] secarcam, *Cifrado de Hill - Web sobre Informática de Secarcam*, https://secarcam.webcindario.com/?p=1432&lang=es.
[9] Juan Felipe Osorio Z, *Matrices Criptográficas: Desentrañando El Misterio Oculto Del Cifrado y Descifrado de Hill*, https://medium.com/@juanfelipeoz.rar/matrices-criptogr%C3%A1ficas-desentra%C3%B1ando-el-misterio-oculto-del-cifrado-y-descifrado-de-hill-de34a924f298.
[10] *Cifrado Hill*, in *Wikipedia, la enciclopedia libre* (2023).

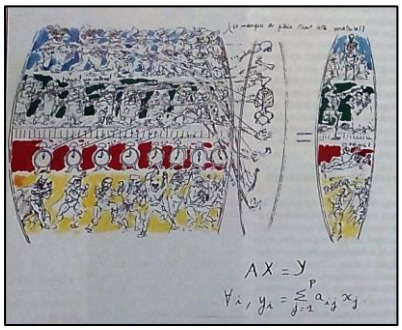
[11] C. Tomé, *Criptografía con matrices, el cifrado de Hill*, https://culturacientifica.com/2017/01/11/criptografia-matrices-cifrado-hill/.

8. Anexos

Máquina del cifrado de Hill, figura 4 de la patente. [10]



La matriz rusa, multiplicación de una matriz por una matriz columna, del artista franco-ruso Paul Kichilov. [11]



Imágenes de la patente US 1.845.947 presentada por Lester S. Hill y Louis Weisner, quienes diseñaron una máquina que implementaba el cifrado de Hill de orden 6. [11]