Instrucciones del proyecto

Este proyecto tiene como objetivo aplicar los conceptos de álgebra lineal al proceso de cifrado y descifrado de mensajes mediante matrices. Cada alumno recibe una matriz llave K y una cadena de números cifrados. Su tarea consiste en:

- 1. Calcular la matriz inversa K^{-1} utilizando el **método de Gauss-Jordan**.
- 2. Multiplicar la matriz inversa K^{-1} por los vectores de la cadena cifrada (en bloques de 3 en 3 números).
- 3. Obtener la secuencia numérica original y convertirla a texto según la tabla de equivalencias proporcionada.

El mensaje resultante corresponderá a una frase corta que deberá descifrarse correctamente. Presente todos los cálculos y procedimientos paso a paso en el espacio indicado.

Ejemplo de descifrado

Suponga que se le da la siguiente matriz y cadena cifrada:

$$K = \begin{pmatrix} 2 & 5 & 7 \\ 1 & 6 & 3 \\ 4 & 0 & 8 \end{pmatrix}$$
, Cadena cifrada: [7, 18, 3, 4, 9, 2, 15, 21, 5]

1. Calcular la matriz inversa K^{-1} utilizando el método de Gauss-Jordan. Para ello, se forma la matriz aumentada:

$$[K \mid I] = \begin{pmatrix} 2 & 5 & 7 & 1 & 0 & 0 \\ 1 & 6 & 3 & 0 & 1 & 0 \\ 4 & 0 & 8 & 0 & 0 & 1 \end{pmatrix}$$

Luego, aplicando operaciones elementales de fila (intercambio, multiplicación y suma), se transforma la parte izquierda en la identidad. El resultado final es:

$$[I \mid K^{-1}] = \begin{pmatrix} 1 & 0 & 0 & 0.50 & -0.39 & -0.22 \\ 0 & 1 & 0 & -0.10 & 0.26 & -0.09 \\ 0 & 0 & 1 & -0.25 & 0.24 & 0.18 \end{pmatrix} \quad \Rightarrow \quad K^{-1} = \begin{pmatrix} 0.50 & -0.39 & -0.22 \\ -0.10 & 0.26 & -0.09 \\ -0.25 & 0.24 & 0.18 \end{pmatrix}$$

2. Agrupar la cadena cifrada en vectores de tamaño 3:

3. Multiplicar K^{-1} por cada vector para recuperar los números originales del mensaje. Por ejemplo, para el primer bloque:

$$\begin{pmatrix} 0.50 & -0.39 & -0.22 \\ -0.10 & 0.26 & -0.09 \\ -0.25 & 0.24 & 0.18 \end{pmatrix} \begin{pmatrix} 7 \\ 18 \\ 3 \end{pmatrix} = \begin{pmatrix} 0.50(7) - 0.39(18) - 0.22(3) \\ -0.10(7) + 0.26(18) - 0.09(3) \\ -0.25(7) + 0.24(18) + 0.18(3) \end{pmatrix} = \begin{pmatrix} 0.83 \\ 3.03 \\ 1.45 \end{pmatrix} \approx \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix}$$

Repitiendo este proceso para los demás bloques, se obtienen los números descifrados.

4. Convertir los números a letras utilizando la siguiente tabla de equivalencias:

5. Interpretar el mensaje obtenido.

Supongamos que el resultado final es:

$$[3, 15, 4, 9, 7, 15, 27, 19, 5, 3, 18, 5, 20, 15]$$

Usando la tabla anterior:

Por lo tanto, el mensaje descifrado es:

CODIGO SECRETO

Nota: el propósito de este ejemplo es ilustrar el procedimiento paso a paso del método de Gauss-Jordan. Cada alumno deberá aplicar el mismo proceso con su propia matriz y cadena cifrada.

| Prov | vecto | 075 | ó |
|------|-------|-----|---|
| | | | |

Nombre del alumno: ______ Grupo: _____ Fecha de entrega: _____

Matriz llave:

$$K = \begin{pmatrix} 5.0 & 9.0 & 6.0 \\ 7.0 & 3.0 & 7.0 \\ 1.0 & 4.0 & 9.0 \end{pmatrix} \pmod{29}$$

Cadena cifrada:

| 338.0 | 349.0 | 298.0 | 198.0 | 155.0 | 105.0 | 158.0 | 185.0 | 182.0 | 307.0 | 344.0 | 283.0 |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| 163.0 | 192.0 | 183.0 | 271.0 | 332.0 | 267.0 | 284.0 | 205.0 | 258.0 | 438.0 | 319.0 | 342.0 |
| 278.0 | 123.0 | 154.0 | 249.0 | 274.0 | 209.0 | 285.0 | 244.0 | 100.0 | 300.0 | 221.0 | 143.0 |
| 201.0 | 236.0 | 88.0 | 414.0 | 387.0 | 284.0 | 174.0 | 176.0 | 155.0 | 358.0 | 281.0 | 324.0 |
| 191.0 | 174.0 | 97.0 | 247.0 | 162.0 | 99.0 | 331.0 | 200.0 | 149.0 | 363.0 | 336.0 | 314.0 |
| 213.0 | 202.0 | 117.0 | 399.0 | 348.0 | 330.0 | 386.0 | 277.0 | 160.0 | 315.0 | 280.0 | 242.0 |
| 193.0 | 241.0 | 150.0 | 102.0 | 55.0 | 48.0 | 216.0 | 261.0 | 120.0 | 169.0 | 98.0 | 88.0 |
| 168.0 | 199.0 | 184.0 | 261.0 | 306.0 | 178.0 | 144.0 | 134.0 | 149.0 | 307.0 | 344.0 | 283.0 |
| 195.0 | 167.0 | 168.0 | 444.0 | 437.0 | 348.0 | | | | | | |

Espacio para cálculos y observaciones: