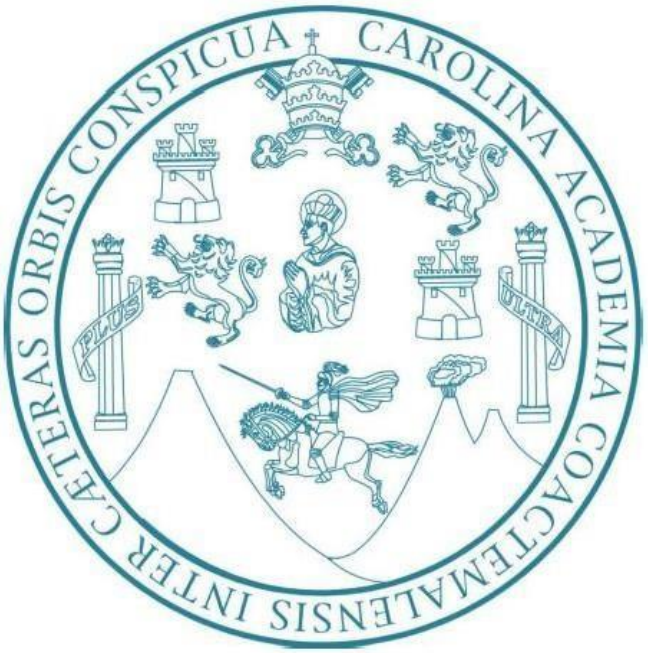
Facultad de Ingeniería

Escuela de Ciencias y Sistemas

Introducción a la Programación y Computación 1 - Sección D

Catedrático: Ing. Herman Veliz

Tutores académicos: Carlos Jimenez y Abner Cardona



PRÁCTICA 1

TABLA DE CONTENIDO

Contenido

PRÁCTICA 1 - IPC1

Objetivos

GENERALES

- ✔ Familiarizar al estudiante con el lenguaje de programación JAVA.
- ✔ Que el estudiante aplique los conocimientos adquiridos en el curso de Introducción a la Programación y computación 1.
- ✔ Elaborar la lógica para presentar una solución a la propuesta planteada.

ESPECÍFICOS

- ✔ Utilizar el lenguaje de programación Java como herramienta de desarrollo de software.
- ✔ Construcción de aplicaciones simples en consola.
- ✔ Implementación de sentencias de control, ciclos y vectores.
- ✔ Aplicación de conceptos de diagramas de flujo.
- ✔ Aplicación de conceptos de algebra matricial
- ✔ Aplicación de sistema de ecuaciones lineales: eliminación Gauss-Jordán

PRÁCTICA 1 - IPC1

DESCRIPCION GENERAL

La criptografía es una técnica que involucra diseño de métodos que protegen documentos y datos, actualmente es muy popular el uso de algoritmos matemáticos que permiten una alta confidencialidad en los mensajes.

Los sistemas informáticos cuentan con una gran importancia en la actualidad, por lo que como consecuencia se ha tenido un incremento en los problemas relacionados con seguridad. Por esta razón se le solicita a usted que aplique los conceptos matemáticos adquiridos durante la carrera de Ingeniería en Sistemas para poder desarrollar un programa que sea capaz de encriptar mensajes ingresados por el usuario haciendo uso de la teoría de matrices.

Sin embargo, no todos los cifrados son seguros. Utilizando métodos de álgebra lineal es posible romper el cifrado y encontrar la matriz clave, por lo que se le solicita emular este proceso llamado "ataque con texto claro conocido" con el fin de conocer las vulnerabilidades de un sistema y dar una posible solución.

APLICACIÓN:

MENU

El menú de la aplicación contará con las siguientes funcionalidades.

```
4   ============= MENU ===============
5   | 1. Encriptar                     |
6   | 2. Desencriptar                  |
7   | 3. Ataque con texto claro        |
8   | 4. Generar Reportes              |
9   ====================================
```

- **Proceso de encriptación (Opción 1):** En esta opción del menú se le solicita al usuario ingresar el texto a encriptar. Se deberá codificar el mensaje de acuerdo con la siguiente tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
14	15	16	17	18	19	20	21	22	23	24	25	26	27

Figura 1: Tabla codificación

Verificaciones:

- El texto ingresado puede incluir mayúsculas o minúsculas por lo que deben trabajar con CaseInsentive todo el proceso
- Verificar que los caracteres del texto estén contenidos en la tabla de codificación, en caso de ser un carácter inválido reemplazarlo por espacio (No 27).

Ejemplo:

Si mi texto de entrada es: "mensaje prueba", vemos que la longitud es 14 caracteres (13 letras + 1 espacio). Ya que la clave para el cifrado será una matriz de 3x3 tenemos que separar el mensaje en tres letras, completando el mensaje a un múltiplo de 3 con blancos.

M	E	N	S	A	J	E		P	R	U	E	B	A
12	4	13	19	0	9	4	27	16	18	21	4	1	0

Armando la matriz M del mensaje quedaría de la siguiente forma:

12	19	4	18	1
4	0	27	21	0
13	9	16	4	27

Luego se ingresa la ruta de dos archivos que contendrá dos matrices clave de 3x3, (A) y (B) ingresadas de forma separada.

Ejemplo de archivo:

2,1,2

-1,5,-1

3,1,6

```
10
11   ========= Menu Encriptar ========
12   | 1. Ingreso Mensaje             |
13   | 2. Ingreso Matriz Clave A      |
14   | 2. Ingreso Matriz Clave B      |
15   | 3. Encriptar                   |
16   ================================
```

Proceso de encriptación: Se debe multiplicar la matriz M del mensaje ingresado con la matriz clave A, y a ese resultado sumarle la matriz B (A*M +B = C). Se muestra en consola el resultado de dicha operación, mostrando el mensaje encriptado (Matriz C).

Ejemplo:

```
17   ========= Menu Encriptar ============
18   | Mensaje Cifrado es:                |
19   | 14 4 13 19 0 9 4 27 16 18 21 4 1 0 |
20   ======================================
```

(Ejemplo de resultado)

- **Desencriptar**: El usuario deberá realizar las operaciones necesarias para obtener el texto cifrado. La fórmula es la siguiente: producto $A^{-1} * C$ -B = M, de la cual se obtiene como resultado la matriz M. Deberá de mostrar el mensaje descifrado en consola obteniendo cada carácter correspondiente de la matriz M encontrada.

  Resultado a mostrar:

```
24   ========= Menu Desencriptar ============
25   | Mensaje descifrado  es:                |
26   | mensaje prueba                         |
27   ==========================================
28
```

- **Ataque con texto plano:** Esta opción del programa emulará el caso en que un analista consigue interceptar el mensaje original y el correspondiente mensaje cifrado con el objetivo de obtener la matriz clave y poder descifrar todos los mensajes que se envíen en el sistema a posterior.

  Para esta funcionalidad el mensaje estará cifrado con solo una matriz clave(A) de 3x3.

```
41   ========= Ataque con texto plano  ============
42   | 1. Ingresar Matriz mensaje original        |
43   | 2. Ingresar Matriz mensaje cifrado         |
44   | 3. Obtener Clave                           |
45   ============================================
46
```

  El proceso consta de lo siguiente:

  Ingresar Matriz mensaje original:

  Se ingresará la ruta del archivo de texto que contiene la matriz del mensaje original.

  Ejemplo: El mensaje es "Cuaderno de cultura científica", el archivo de texto contendrá la matriz del mensaje.

```
2,21,0
3,4,18
13,15,3
4,2,21
11,20,21
18,0,2
8,4,13
20,8,5
8,2,0
```

Ingresar Matriz mensaje cifrado:

Se ingresará la ruta del archivo de texto de la matriz del mensaje cifrado.

```
17,3,2
11,25,3
25,21,4
17,5,22
6,23,2
24,10,3
1,0,5
24,3,23
12,8,8
```

Obtener Clave:

Para lograr romper el código se utiliza el método Gauss Jordán sobre la matriz formada por la matriz del mensaje original y la matriz del mensaje cifrado.

$$\left(\begin{array}{ccc:ccc} 2 & 21 & 0 & 17 & 3 & 2 \\ 3 & 4 & 18 & 11 & 25 & 3 \\ 13 & 15 & 3 & 25 & 21 & 4 \\ 4 & 2 & 21 & 17 & 5 & 22 \\ 11 & 20 & 21 & 6 & 23 & 2 \\ 18 & 0 & 2 & 24 & 10 & 3 \\ 8 & 4 & 13 & 1 & 0 & 5 \\ 20 & 8 & 5 & 24 & 3 & 23 \\ 8 & 2 & 0 & 12 & 8 & 8 \end{array}\right)$$

Matriz madre

PRÁCTICA 1 - IPC1

El procedimiento consiste en realizar una serie de operaciones sobre la matriz madre que está dividida en dos partes (matriz mensaje original y matriz mensaje cifrado), el objetivo es conseguir que en la parte izquierda quede la matriz identidad (1 0 0 / 0 1 0 / 0 0 1) **en tres de las filas** para entonces considerar la parte derecha como resultado.

Las operaciones por realizar son los algoritmos que utiliza el método Gauss-jordan para su solución: sustitución de filas procedente del resultado de sumar, restar o dividir a esa fila una combinación lineal de otras filas.

En la tabla de contenido solamente aparecen 27 números, hay que trabajar con los números enteros "módulo 27". Es decir, se consideran los números enteros 0, 1, 2…, 26 y el resto se identifica con estos de forma cíclica. Así, el 27 es igual a 0, el 28 a 1, el 29 a 2, etc, y lo mismo con los números negativos, de forma que – 1 es igual 26, – 2 es igual 25, etc. Esto se resume a una pequeña instrucción: (n)mod (27) donde únicamente se debe verificar resultados negativos (aplicar forma cíclica). Ejemplos

13+5 = 18, convirtiéndolo; 18mod27 = 18
2-5 = -3 convirtiéndolo; (2-5) mod27 = -3 (aplicar ciclo debido a negativo) 27-3 = 24
6*13 = 78 convirtiéndolo; 78mod27 = 24
** división es caso especial, se explica más adelante**

Ejemplo Operaciones para realizar:

La posición 0,0 tiene que ser un 1, para poder obtener la matriz identidad, el número es un 2, debemos dividir por 2 (módulo 27) la primera fila. Ya que al trabajar con modulo 27 no se puede dividir, se haya el inverso multiplicativo modular de 2(Modulo 27) que es 14, luego la equivalencia a dividir por 2 es igual a multiplicar por 14 de la siguiente forma (2) *(14) mod (27).

Al multiplicar la primera fila (2, 21, 0: 17, 3, 2,) por 14 (módulo 27) se transforma en (1, 24, 0: ,22, 15, 1,). (n)*14Mod27

Ahora, para conseguir un 0 en la primera posición de cada fila se realiza las siguientes sustituciones (método de Gauss Jordan).

"2nda fila" = "2nda fila" – 3 * "1era fila" (módulo 27)
"3era fila" = "3ª fila" – 13 * "1era fila" (módulo 27)
"4ta fila" = "4ta fila" – 4 * "1era fila" (módulo 27)
"5ta fila" = "5ta fila" – 11 * "1era fila" (módulo 27)
"6ta fila" = "6ta fila" – 18 * "1era fila" (módulo 27)

Se así podría seguirse con el resto, aunque no es necesario fijarnos en el resultado de las tres últimas filas para conseguir el objetivo. después de las sustituciones anteriores, la matriz se ha transformado en la siguiente matriz

$$\left(\begin{array}{ccc:ccc} 1 & 24 & 0 & 22 & 15 & 1 \\ 0 & 13 & 18 & 26 & 7 & 0 \\ 0 & 0 & 3 & 9 & 15 & 18 \\ 0 & 14 & 21 & 10 & 26 & 18 \\ 0 & 26 & 21 & 7 & 20 & 18 \\ 0 & 0 & 2 & 6 & 10 & 12 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{array}\right)$$

Siguiendo con el proceso, se debe obtener un 1 en la segunda fila siguiendo la diagonal. Como en esa posición está el 13, debemos buscar su inverso multiplicativo modular, que resulta que es 25 (13 x 25 = 325, que tomando módulo 27, es igual a 1). Es decir, hay que multiplicar la segunda fila por 25, de manera que esta segunda fila (0, 13, 18: 26, 7, 0), quedaría al multiplicarla por 25 (módulo 27) en (0, 1, 18: 2, 13, 0), (n)*25Mod (27). Siguiendo el método de Gauss Jordan se deben obtener los ceros.

"1era fila" = "1ta fila" – 24 * "2ª fila" (módulo 27)
"4ta fila" = "4ta fila" – 14 * "2ª fila" (módulo 27)
"5ta fila" = "5ta fila" – 26 * "2ª fila" (módulo 27)

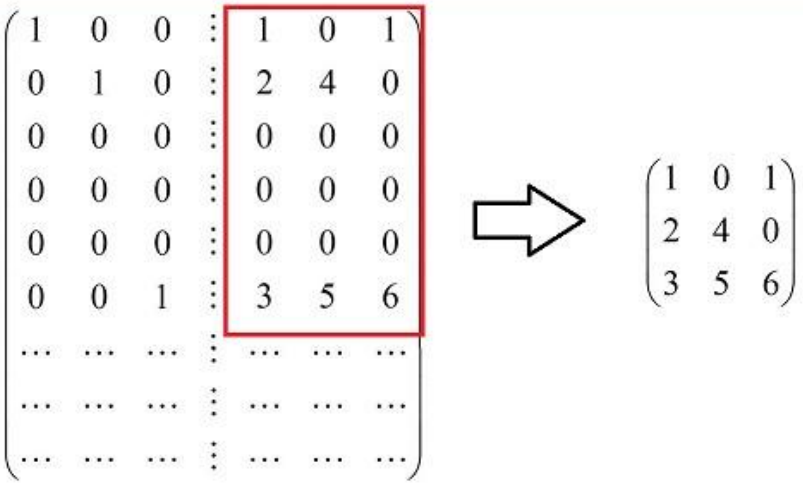
quedando la matriz de la siguiente forma:

$$\left(\begin{array}{ccc:ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 18 & 2 & 13 & 0 \\ 0 & 0 & 3 & 9 & 15 & 18 \\ 0 & 0 & 12 & 9 & 6 & 18 \\ 0 & 0 & 12 & 9 & 6 & 18 \\ 0 & 0 & 2 & 6 & 10 & 12 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{array}\right)$$

El siguiente paso sería conseguir un 1 en la posición que se corresponde con la tercera fila y columna, Sin embargo, en este momento nos encontramos con una excepción por trabajar módulo 27, y es que los números enteros módulo 27 admiten "divisores de cero", como el 3 y el 9, ya que el producto de 3 por 9 es igual a 0 (módulo 27), y estos no tienen inverso. En consecuencia, no se puede conseguir un 1 en la tercera columna de las filas 3, 4 y 5. Y al multiplicarlas por 9 se anulan todos sus elementos, luego esas tres filas no nos interesan. Por lo tanto, vamos a intentar conseguir un 1 en la tercera columna de la fila 6, para lo cual tenemos que multiplicar por el inverso de 2, que como ya sabemos es 14. Y a la fila 6 pasa de (0, 0 ,2: 6 ,10, 12) a (0, 0, 1: 3, 5, 6), al multiplicarla por 14.

"2nda fila" = "2nda fila" – 18 * "6ta fila" (módulo 27)

Luego, tras realizar Jordan, la parte derecha de la matriz es nuestro resultado, la cual no toma en cuenta las filas que han sido eliminadas por la excepción.



El resultado es la matriz transpuesta de la matriz clave. Deberá mostrar en consola la matriz clave (No la matriz transpuesta).

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 1 & 0 & 6 \end{pmatrix}$$

(Resultado final: matriz clave utilizada en la encriptación)

- **Generar Reportes**: Parte importante de ser ingenieros en Sistemas, es tener la habilidad de poder generar reportes, para poder visualizar resultados en cualquier tipo de software. Por lo tanto, para este programa se le solicitan 3 diferentes reportes en formato HTML.

    1. Reporte Encriptar: Debe contener el texto a encriptar, la matriz M del mensaje, Las dos matrices clave y los pasos de las operaciones realizadas y el resultado.
    2. Reporte Desencriptar: Debe contener la matriz encriptada, los pasos realizados para obtener la matriz del mensaje y el mensaje correspondiente.
    3. Reporte "Ataque con texto claro": Debe contener la matriz del mensaje original, la matriz del mensaje cifrado, la matriz madre, la primera y últimas dos iteraciones de Gauss Jordan, la matriz transpuesta y la matriz clave encontrada.

    Cada reporte debe contener la fecha y hora de generación. Mínimo se deben mostrar 4 pasos para que el reporte sea tomado como valido. El diseño queda a discreción del estudiante (Se tomará en cuenta en los puntos).

    La generación de cada reporte se puede realizar en cualquier momento de la ejecución por lo cual deben validar si tiene datos a reportar o no.

PRÁCTICA 1 - IPC1

Requerimientos para el desarrollo del proyecto:

DOCUMENTACION:

- ✔ Diagrama de flujo general del programa.
- ✔ Manual Técnico (descripción de los métodos creados) en PDF.
- ✔ Manual de Usuario (Como funciona la aplicación y como el usuario interactúa con ella).

RESTRICCIONES:

- ✔ La aplicación debe ser desarrollada en el lenguaje de programación Java.
- ✔ No se permite el uso de estructuras que implemente Java (ArrayList, LinkedList, etc.).
- ✔ No se permite el uso de librerías para realizar las operaciones entre matrices.
- ✔ No se permite utilizar código copiado o bajado de Internet.
- ✔ El IDE por utilizar queda a discreción del estudiante (se recomienda el uso de Eclipse)
- ✔ Copias obtendrán una nota de 0 y reporte a la Escuela de Ciencias y Sistemas.

HABILIDADES POR EVALUAR:

- ✔ Uso de variables globales y locales.
- ✔ Uso de memoria estática
- ✔ Uso de estructuras de control y de selección
- ✔ Uso correcto de los arreglos y matrices.
- ✔ Conocimientos sobre sistemas computacionales
- ✔ Habilidad para analizar y sintetizar información
- ✔ La habilidad de comprender y realizar diagramas
- ✔ Habilidad para resolver problemas.

ENTREGA:

- ✔ **FECHA DE ENTREGA:** 13/02/2021 antes de las 23:59 PM. No se aceptarán entregas a partir de esa hora.
- ✔ Adjuntar lo solicitado en un archivo .zip con el siguiente formato: [IPC1]Practica1_carnet.rar. Ejemplo: [IPC1]Practica1_201900000.rar
- ✔ Subir el archivo .zip en la tarea asignada en Google Classroom y en UEDI.