

Universidad de San Carlos de Guatemala

Facultad de Ingeniería

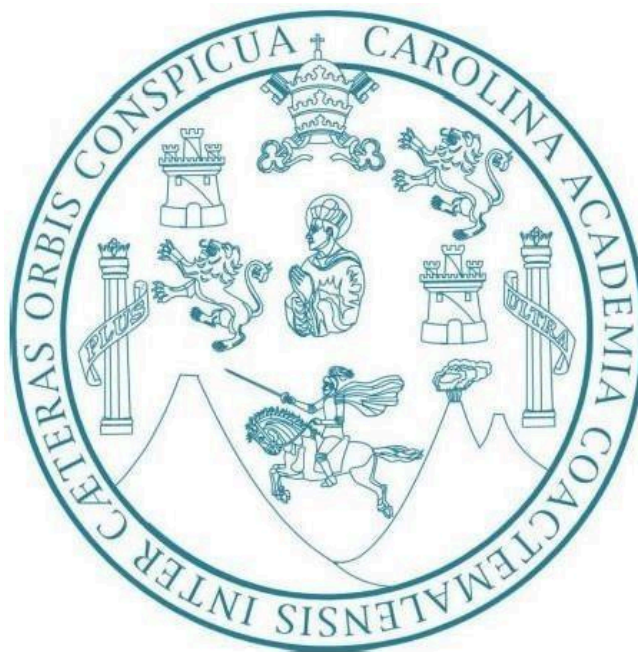
Escuela de Ciencias y Sistemas

Introducción a la Programación y Computación 1

Sección: A

Cat. Ing. Nefthali de Jesus Calderon Mendez

Tutor académico: Josué Rodolfo Morales Castillo



PRÁCTICA 1

CipherChat

ÍNDICE

ÍNDICE.....	1
OBJETIVOS.....	2
❖ GENERALES.....	2
❖ ESPECÍFICOS.....	2
DESCRIPCIÓN GENERAL.....	3
DEFINICIÓN:.....	3
APLICACIÓN.....	4
MÓDULO DE AUTENTICACIÓN.....	4
Login:.....	4
Registro de usuarios:.....	4
MÓDULO USUARIO.....	6
Lista de Contactos:.....	6
Chat:.....	6
Proceso de encriptación:.....	8
Proceso para desencriptar:.....	9
Editar perfil:.....	9
Notificaciones:.....	10
MÓDULO MODERADOR.....	12
Lista de reportes.....	12
Analizar caso.....	12
MÓDULO ADMINISTRADOR.....	15
Usuarios.....	15
Panel de moderación.....	15
Reportes.....	16
REQUERIMIENTOS PARA EL DESARROLLO DEL PROYECTO.....	16
❖ LIBRERÍAS PERMITIDAS:.....	16
❖ DOCUMENTACIÓN:.....	16
❖ RESTRICCIONES:.....	17
❖ HABILIDADES POR EVALUAR:.....	17
❖ ENTREGA:.....	18

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 usando interfaces gráficas en Java, sin el uso de drag and drop.
- Desarrollar una aplicación de mensajería con funcionalidades de encriptación y desencriptación de mensajes.
- Implementar el sistema utilizando POO, asegurando una estructura modular y escalable.
- Gestionar múltiples roles de usuario con permisos específicos.

DESCRIPCIÓN GENERAL

DEFINICIÓN:

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.

"CipherChat" es una aplicación desarrollada en Java que permite a los usuarios enviar y recibir mensajes de manera segura utilizando técnicas de encriptación y desencriptación. La aplicación estará diseñada siguiendo los principios de Programación Orientada a Objetos (POO) y contará con una interfaz gráfica amigable. Además, el sistema manejará diferentes roles de usuario, cada uno con distintos niveles de acceso y funcionalidades.

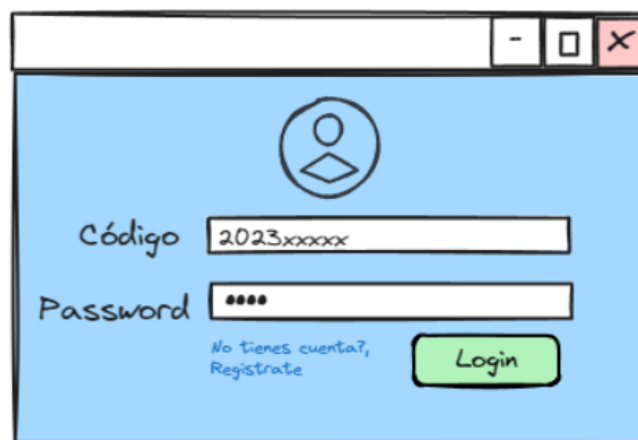
APLICACIÓN

La aplicación está dividida en los siguientes módulos:

MÓDULO DE AUTENTICACIÓN

Login:

La función de este módulo es darle el acceso al sistema a los usuarios por medio de un código y contraseña. Si se da el caso que un usuario no cuente con una cuenta previamente creada, tiene la opción de registrarse en el sistema.



A hand-drawn sketch of a login window. The window has a title bar with standard minimize, maximize, and close buttons. The main area has a light blue background. At the top center is a circular icon containing a person silhouette. Below this are two input fields: the first is labeled 'Código' and contains the text '2023xxxxx'; the second is labeled 'Password' and contains four asterisks '****'. Below the password field is a link that says 'No tienes cuenta?, Regístrate'. To the right of this link is a green button labeled 'Login'.

Si el inicio de sesión es exitoso, entonces debe mostrar un mensaje el cual diga: “Bienvenido Nombres y Apellidos del usuario”, de lo contrario, si alguna credencial no es correcta, se deberá informar al usuario y no entrar en el sistema.

Registro de usuarios:

La función de este módulo es que el usuario pueda crear su cuenta y pueda acceder al sistema de CipherChat. Los datos que se le deben de solicitar a un nuevo usuario son:

- Nombres (Obligatorio, hacer validaciones que sea llenado este campo)
- Apellidos (Obligatorio, hacer validaciones que sea llenado este campo)
- Edad (Obligatorio, hacer validaciones que sea llenado este campo)
- Sexo: M/F (Obligatorio, hacer validaciones que sea llenado este campo)
- Contraseña (Obligatorio, hacer validaciones que sea llenado este campo)
- Teléfono (Opcional)

PRÁCTICA 1 - IPC1

A hand-drawn registration form with a light blue background and a black border. At the top right, there are three small boxes: a minus sign, a square, and a red 'X'. The form contains the following fields:

- Nombres**: A text box containing "Lionel Ronaldo".
- Apellidos**: A text box containing "Ponce Pérez".
- Password**: A text box containing four asterisks "****".
- Género**: A dropdown menu with the text "Seleccione la opción" and a downward arrow icon.
- Edad**: A text box containing "32".
- Teléfono**: A text box containing "12345678".

At the bottom right of the form is a green button with the text "Sign Up".

Al darle al botón de registrar tiene que mostrar un mensaje donde muestre el nuevo código con el cuál puede iniciar sesión el usuario (El código debe de ser único y generado por el programa, se recomienda que este sea iterativo, por ejemplo si empieza desde el 202300000, el siguiente usuario tendrá el código 202300001).

A hand-drawn confirmation message box with a light blue background and a black border. On the left side, there is a green circle containing a white exclamation mark. To the right of the circle, the text reads:

Su código de
Inicio de Sesión
es:

00000000

At the bottom center is a green button with the text "Aceptar".

MÓDULO USUARIO

Luego de iniciar sesión como usuario se le mostrará las siguientes opciones:

Lista de Contactos:

- Mostrar todos los contactos del usuario, se debe mostrar el código del usuario, nombres, apellidos, una opción para poder dirigirse a la ventana donde se establece una conversación con el otro usuario y otra opción para eliminar a un usuario de la lista de contactos.
- Opción para buscar contactos por medio de el código, si no existe mostrar un mensaje que diga que no existe el usuario buscado y si este existe en el sistema, preguntar si se desea agregar, si es así entonces este nuevo usuario aparecerá en la lista de contactos del usuario actual, de lo contrario no se agregará (si se presiona cancelar).

Código	Nombre	Chat	Eliminar
20230001	Fernanda Alvarez	Abrir	X

Buscar contactos: 202300002

Buscar

Chat:

Se debe abrir una nueva ventana en donde se muestre el chat con el contacto seleccionado, en esta ventana se le permite al usuario escribir y enviar mensajes los cuales serán encriptados antes de enviarse. En esta ventana se debe mostrar el código del usuario con el que se está chateando, además si existen conversaciones mostrarlas todas, como si fuera messenger, osea los últimos chats se deben mostrar hasta abajo, además debe existir un apartado en donde se pueda colocar el mensaje que se desea enviar y un botón para enviar el mensaje.

Para que el botón de enviar mensaje se habilite, primero se deberán haber cargado las matrices con las cuales se encriptará el mensaje y posteriormente con estas mismas se

PRÁCTICA 1 - IPC1

desencriptará el mensaje, tanto para el administrador, como para los moderadores y el usuario destino.

Solamente se deberán de escribir las rutas en donde se encuentran las matrices y cargarlas por medio de botones. Cabe resaltar que la matriz clave A se ingresará una sola vez en el chat que se tenga con una persona en específico, esta matriz será ingresada por el usuario que envíe el primer mensaje en el chat con otro usuario, esta matriz se guardará para futuros chats con este mismo usuario. La matriz que siempre se deberá ingresar es la matriz clave B la cual se detallará más adelante.

Cada conversación que se muestre en el chat, debe mostrar la fecha y hora (03/06/2024 - 13:05) en la cual se envió el mensaje, el mensaje desencriptado y deberá existir un botón para reportar, este botón únicamente aparecerá en las conversaciones mandadas por la otra persona, no debe aparecer en las conversaciones que el usuario actual hace. Si se reporta una conversación esta será notificada a los moderadores los cuales validarán si es motivo de penalización o no, esto se detalla más adelante en el módulo de moderadores, al reportar un mensaje debe aparecer un mensaje de confirmación que se reportó con éxito el mensaje.

The screenshot displays a chat application window with a title bar containing standard minimize, maximize, and close buttons. The main interface is divided into two primary sections. On the left, a chat conversation is shown with a red header box containing the ID '202300001'. The chat area features two messages: the first is 'Hola qué tal?' with a timestamp of '03/06/2024 - 13:05'; the second is 'Qué tal mucho gusto!' with a timestamp of '03/06/2024 - 13:06' and a red 'Reportar' button below it. At the bottom of the chat area is a text input field labeled 'Texto que se enviará' and a green 'Enviar' button. On the right side of the window, there is a blue panel for loading matrices. It contains two sections: 'Ruta de la matriz clave A:' with a text input field containing '..\Matrices\MatrizA.txt' and a yellow 'Cargar' button; and 'Ruta de la matriz clave B:' with a text input field containing 'C:\Matrices\MatrizB.txt' and another yellow 'Cargar' button.

Se recomienda usar una lista dinámica global la cual guarde todas las conversaciones de todos los usuarios y a la hora de mostrar los chats, filtrar por medio de los códigos de los usuarios.

PRÁCTICA 1 - IPC1

Proceso de encriptación:

1. Con el texto que se desea enviar, primero se deberá de 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 Case Insensitive todo el proceso.
- Si alguna vocal tiene tilde, entonces deberá colocar el valor de esa letra sin la tilde, por ejemplo si viene ágil, entonces la “á” será tomada como si viniera “A”, por lo tanto se le asignaría un valor de 0.
- 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 filas, completando el mensaje a un múltiplo de 3 con espacios en blanco.

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

PRÁCTICA 1 - IPC1

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

2. Luego como ya se tiene en memoria la matriz clave A y B; aclaración: la matriz A es siempre de 3x3 y la matriz B será del mismo tamaño que la matriz M.

Ejemplo de archivo:

2,1,2

-1,5,-1

3,1,6

3. Se debe multiplicar la matriz M del mensaje ingresado con la matriz clave A, y a ese resultado sumarle la matriz B ($A * M + B = C$). Ejemplo del mensaje encriptado (Matriz C), este no se debe mostrar solo almacenar, ya que se usará después para el proceso de descryptar:

Mensaje Cifrado es:

14 4 13 19 0 9 4 27 16 18 21 4 1 0

Proceso para descryptar:

Cuando un mensaje llega al usuario destino, el sistema deberá realizar las operaciones necesarias para obtener el texto descifrado.

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 el chat de los usuarios que están teniendo una conversación.

Editar perfil:

Se debe crear una nueva ventana donde se pueden actualizar los siguientes campos del usuario, tomar en cuenta que esta ventana debe mostrar en campos de texto los datos actuales del usuario, en caso ningún campo sea actualizado, la información actual del usuario persistirá y en caso se cambie algún campo, pues su información será actualizada, se debe poder ver el código y género de igual manera, pero estos no se pueden cambiar, los campos que se pueden actualizar son:

PRÁCTICA 1 - IPC1

- Nombres
- Apellidos
- Contraseña
- Edad
- Teléfono

Luego de modificar el/los campos se le debe dar actualizar y luego se mostrará un mensaje de confirmación.

The mockup shows a web browser window with a dark-themed interface. At the top, there are three tabs: 'Lista de contactos', 'Notificaciones', and 'Editar perfil' (which is highlighted in orange). Below the tabs is a form for editing a user profile. The form is organized into three columns. The first column contains fields for 'Código:' (202300001), 'Nombres:' (Lionel Ronaldo), and 'Apellidos:' (Ponce Pérez). The second column contains fields for 'Género:' (Masculino), 'Edad:' (24), and 'Teléfono:'. The third column contains a 'Contraseña:' field (12345678). A green 'Actualizar' button is located at the bottom right of the form.

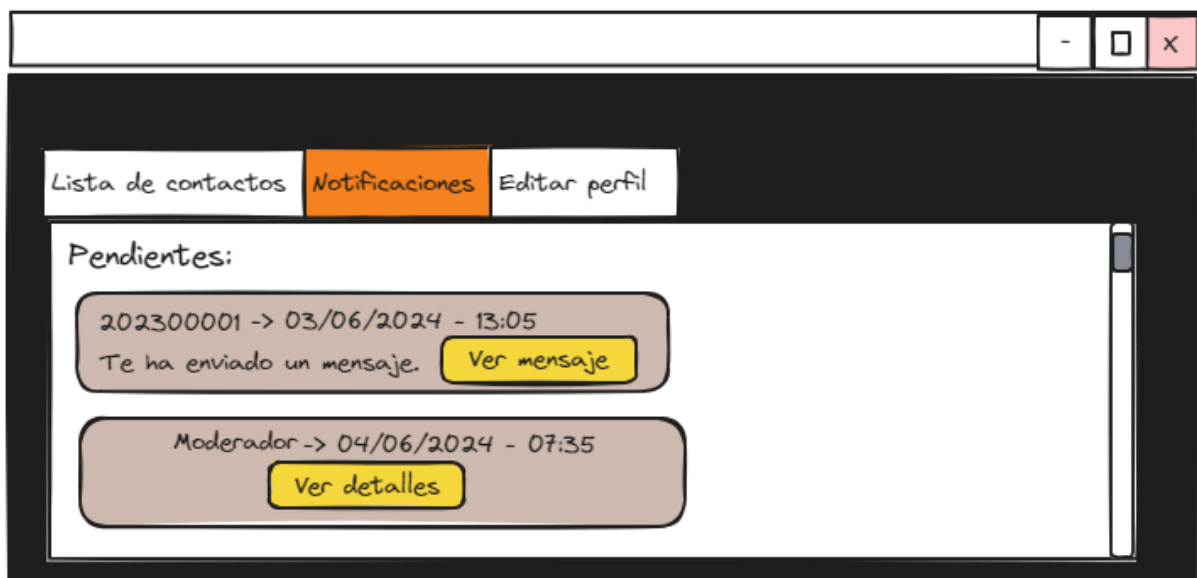
Notificaciones:

El usuario debe ser capaz de ver el listado de sus notificaciones, estas notificaciones le llegarán al usuario en los siguientes casos:

- Otro usuario le envía un mensaje. Para este tipo de notificación se deberá mostrar el código del usuario que envió el mensaje, la fecha y hora (03/06/2024 - 13:05) en la cual se mandó el mensaje y mostrar un texto que diga “Te ha enviado un mensaje.”. También deberá haber una opción para poder ver el mensaje, por ejemplo un botón y este abrirá directamente la ventana para chatear con el usuario que envió el mensaje, este tipo de notificación se quitará de la lista solo si se abre el chat con el otro usuario, ya sea desde el botón de la notificación o si en la lista de contactos se abre el chat con este usuario (no es necesario que el usuario responda). De lo contrario la notificación permanecerá allí.

PRÁCTICA 1 - IPC1

- Advertencia por parte de los moderadores. Si un usuario reporta un mensaje que otro usuario envió, entonces el moderador se encargará de validar el reporte y si en dado caso es motivo de advertencia, al usuario reportado le aparecerá una notificación la cual deberá mostrar:
 - Moderador (Ya que es el nombre del usuario que envió el mensaje)
 - Fecha y hora (03/06/2024 - 13:05) en la cual el moderador envió el mensaje.
 - Un botón que diga “Ver detalles” y al presionar este mismo, se abra una ventanita en la cual diga “Advertencia # X, un usuario ha reportado un mensaje que has enviado, se realizó la validación y este mensaje es penalizable, si se te realizan dos advertencias, entonces se te eliminará del sistema.”, donde X es el número de penalizaciones que tiene el usuario en general, no importa si otro usuario distinto lo reportó anteriormente, estas penalizaciones son acumulables. Luego se detallará que pasa si el usuario tiene dos penalizaciones.



El módulo debe contar con una opción para poder realizar Logout.

MÓDULO MODERADOR

Para ingresar al módulo del moderador se usarán las siguientes credenciales en el Login:

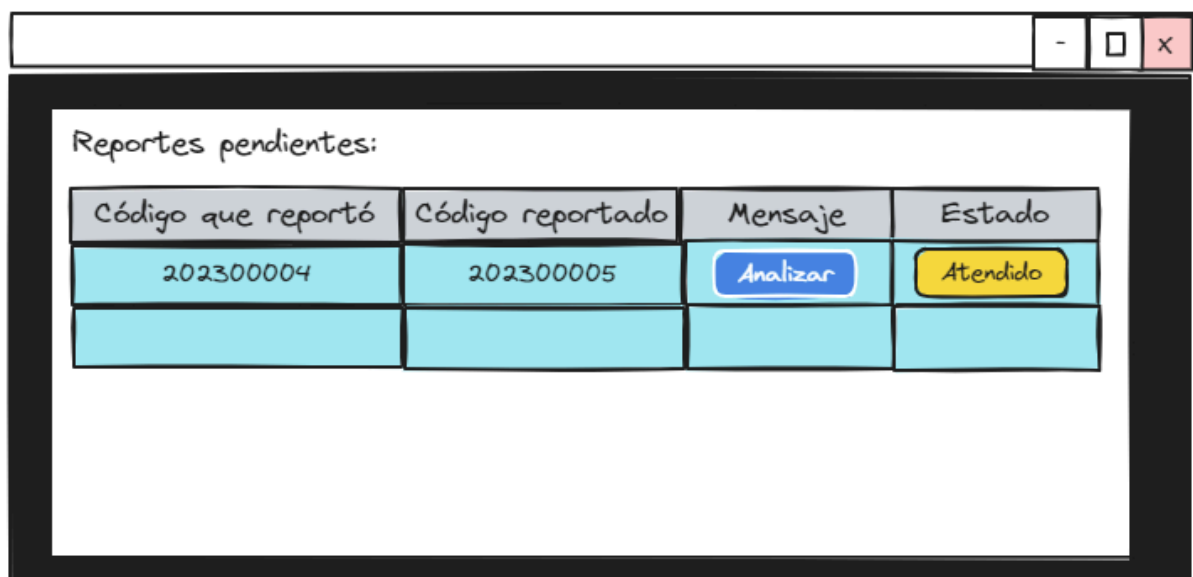
Código: 202010033

Password: p1IPC1

El módulo debe contar con una opción para poder realizar Logout.

Lista de reportes

El moderador debe ser capaz de poder ver todos aquellos reportes pendientes, cada reporte en la lista debe mostrar el código del usuario que realizó el reporte, el código del usuario que fue reportado y un botón que diga “Analizar” el cual al presionarlo abra una nueva ventana en la cual se pueda analizar el caso, esta ventana se detallará en Analizar caso. Una vez se haya analizado y resuelto el caso, se deberá marcar el estado del reporte en “Atendido”.



Código que reportó	Código reportado	Mensaje	Estado
202300004	202300005	Analizar	Atendido

Analizar caso

En esta ventana se mostrará el mensaje encriptado de primero (Matriz C), es importante tomar en cuenta que por cada mensaje que se mande en un chat, se deben guardar las matrices: A, B, C y M. El moderador para poder visualizar el mensaje tendrá la opción de “Desencriptar el mensaje temporalmente”. Al seleccionar la opción de desencriptar un mensaje se deberá generar un reporte el cual se guarde con el siguiente formato: Código del usuario reportado_D.html. Ej: 202300005_D.html

Este reporte debe llevar lo siguiente:

PRÁCTICA 1 - IPC1

1. Matriz encriptada (Matriz C)
2. Cálculo de la matriz inversa de (A) por cofactores
 - 2.1. Mostrar matriz clave A
 - 2.2. Determinante de la Matriz clave A
 - 2.3. Matriz adjunta de la matriz clave A
 - 2.4. Matriz traspuesta de la matriz adjunta de la matriz clave A
 - 2.5. Matriz inversa de A $\rightarrow A^{-1} = \frac{(A^*)^T}{|A|}$

Donde $|A|$ es el determinante de la matriz
 A^* es la matriz adjunta
 $(A^*)^T$ es la matriz traspuesta de la adjunta
3. Matriz clave B
4. Matriz resultante de (C - B)
5. Matriz (M), resultado de $A^{-1} * C - B = M$
6. Mensaje Descifrado
7. Fecha y hora en la que se generó el reporte

Una vez se haya generado el reporte deberá de mostrarse un mensaje de confirmación y luego se mostrará en pantalla el mensaje ya descifrado en lugar del encriptado.

Luego de que se haya analizado el caso se deberá seleccionar la opción de “Encriptar mensaje”, esta opción deberá generar un reporte el cual se guarde con el siguiente formato:

Código del usuario reportado_E.html. Ej: 202300005_E.html

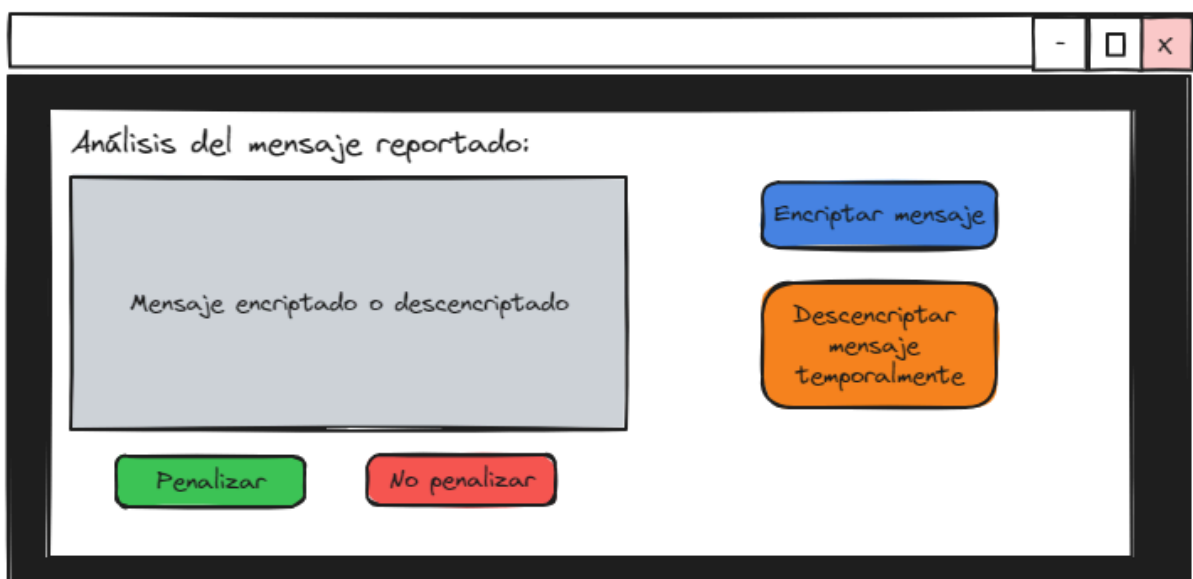
Este reporte debe llevar lo siguiente:

1. Mensaje reportado (Mostrar el mensaje desencriptado)
2. Mensaje ingresado ya codificado en la matriz M
3. Matriz clave A
4. Matriz clave B
5. Matriz resultante de (A * M)
6. Matriz C, obtenida de $[A * M + B]$
7. Mensaje cifrado
8. Fecha y hora de generación del reporte

PRÁCTICA 1 - IPC1

Una vez se haya generado el reporte deberá de mostrarse un mensaje de confirmación y luego se mostrará en pantalla el mensaje nuevamente cifrado.

Por último el moderador tendrá la opción de penalizar o no al usuario, si penaliza al usuario a este le llega la notificación anteriormente descrita y se le suma al usuario una penalización, recordar que estas penalizaciones son acumulables y si se llega a 2 de estas, el administrador deberá evaluar el caso. Si el usuario no es penalizado entonces no se manda ninguna notificación a ningún usuario ni se acumulan penalizaciones. Luego de haber hecho esto se le redirigirá al moderador a su pantalla principal.



MÓDULO ADMINISTRADOR

Para ingresar al módulo del administrador se usarán las siguientes credenciales en el Login:

Código: Carnet del estudiante

Password: p1IPC1

El módulo debe contar con una opción para poder realizar Logout.

Usuarios

El administrador debe ser capaz de poder visualizar todos los usuarios del sistema, se debe mostrar como mínimo el código y el nombre completo de cada usuario, también tiene que tener las siguientes opciones:

- Crear un nuevo usuario
- Editar un usuario en específico del listado de usuarios (Recordar que cuando se edita un usuario se debe mostrar su información actual y no se puede editar el código y el género)
- Eliminar un usuario en específico

Panel de moderación

El sistema automáticamente debe notificar al administrador cuando se detecte que un usuario tiene 2 penalizaciones acumuladas, de igual manera tendrá una opción para poder analizar los casos, solo que en esta ocasión la nueva ventana deberá mostrar los mensajes reportados ya descifrados, además ambos mensajes deberán mostrar su respectiva fecha y hora en que fueron enviados por el usuario.

Luego de haber analizado los casos el administrador tendrá dos opciones:

- Omitir caso: Si el administrador escoge esta opción, se le hará un reset al contador de penalizaciones del usuario, osea su contador sería igual a 0.
- Bloquear usuario: Si el administrador escoge esta opción, el usuario será bloqueado del sistema, esto quiere decir que no será eliminado, pero este tampoco podrá ingresar, por lo que la próxima vez que el usuario intente hacer Login, el sistema le dará un mensaje de error el cual indique que ha sido bloqueado del sistema por la acumulación de penalizaciones.

Una vez se haya analizado el caso del usuario se deberá retornar a la pantalla principal del administrador y ya no se deberá mostrar el caso en la lista.

Reportes

El administrador tendrá una sección donde podrá visualizar los siguientes reportes:

- Gráfica de pie: Usuarios correctos vs. Usuarios bloqueados
- Gráfica de barras: Top 3 usuarios que han enviado más mensajes en general

REQUERIMIENTOS PARA EL DESARROLLO DEL PROYECTO

❖ LIBRERÍAS PERMITIDAS:

➤ Para el desarrollo de este proyecto, tiene permitido el uso de las siguientes librerías:

- AWT
- SWING
- JFreeChart
- ArrayList, LinkedList
- Si tiene duda del uso de alguna otra librería, consultar primero al auxiliar por medio de los medios oficiales de comunicación.

❖ DOCUMENTACIÓN:

➤ Diagrama de flujo general del programa. Investigar cuáles son las figuras correctas que se deben aplicar de acuerdo al flujo de su programa, a continuación se deja un ejemplo:

<https://es-static.z-dn.net/files/d0e/fd80205a8e997e25f2958fedb199872a.jpg>

- Manual técnico
- Manual de usuario
- Para los manuales (técnico y de usuario) seguir la plantilla la cual está en Uedi en material de apoyo. Para el manual técnico deberá insertar imágenes como mínimo del número de línea y el nombre de su método, procedimiento o función, variables globales, librerías utilizadas y su respectiva descripción. Para el manual de usuario deberá obligatoriamente adjuntar imágenes y su

respectiva descripción de cómo funciona su programa, qué ventanas muestra, resultados, etc...

❖ RESTRICCIONES:

- La aplicación debe ser desarrollada en el lenguaje de programación JAVA
- No se permite utilizar código copiado o bajado de Internet, ni ayuda entre compañeros, el trabajo es **individual**.
- El IDE por utilizar queda a discreción del estudiante (se recomienda el uso de NetBeans)
- Copias obtendrán una nota de 0 y reporte a la Escuela de Ciencias y Sistemas.
- La interfaz gráfica de usuario debe ser construida sin ayuda del IDE (PROHIBIDO usar Drag and Drop), únicamente utilizar las librerías de AWT y Swing.
- Durante la calificación se le solicitará al estudiante modificar el código del proyecto con el objetivo de validar la creación de este.
- Su repositorio debe de estar **privado**.
- Cualquier librería que quiera implementar debe de consultarlo primero con el auxiliar.
- El estudiante no tendrá derecho a calificación si no presenta interfaz gráfica, no se calificará ninguna funcionalidad en consola.
- El estudiante no tendrá derecho a calificación si no manejó su código utilizando un repositorio de github.

❖ HABILIDADES POR EVALUAR:

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

- Habilidad para resolver problemas.
- Capacidad de crear interfaces gráficas de usuario.

❖ ENTREGA:

- **FECHA DE ENTREGA:** 13/06/2024 antes de las **13:00** horas (No se aceptarán entregas, ni commits a partir de esa fecha y hora)
- Adjuntar el código fuente y la documentación en el repositorio privado de GitHub con el siguiente formato: [IPC1-A]Practical_carnet, por ejemplo: [IPC1-A]Practical_202010033.
- Subir el enlace del repositorio de GitHub en la tarea asignada en UEDI.
- Agregar de colaborador al repositorio al auxiliar: RMorales202010033