Trabajo Práctico Grupal
Mensajes secretos - Parte 2

Objetivo General

Sumar funcionalidad a la aplicación desarrollada en la Parte 1 del TP Grupal, que permite cifrar mensajes para ser enviados sin poder ser interceptados.

En este caso agregaremos funcionalidad para que:

- ➔ quienes hagan uso de la aplicación deban estar previamente registrados como usuarios
- ➔ podremos asignar a nuestro mensaje un destinatario específico
- ➔ preservaremos los datos en un archivo csv.

Planificación para el desarrollo de la aplicación

Para que puedan alcanzar el objetivo general exitosamente, los vamos a guiar en el proceso de modificación del código logrado para la Parte 1. Es importante que sigan las indicaciones aquí descritas y las dadas por los docentes a cargo.

- ➔ Deberán ir cumpliendo los objetivos en orden y a medida que los cumplan, subir lo producido al campus.

- ➔ Deberán preservar una versión del programa de la Parte 1, y generar una nueva versión por cada uno de los objetivos a cumplir.

Objetivo 1: Registración e ingreso de usuarios

Previo al uso de la aplicación será necesario que los usuarios de la misma se identifiquen mediante el ingreso de un usuario y su clave. Por ello, nuestro botón de "Continuar" de la primera ventana, será reemplazado por 2 botones, uno de "Crear Usuario", y otro de "Ingreso Usuario".

1. Creación de Usuario

El **"Crear Usuario"**, deberá desplegar una nueva ventana para poder registrar un usuario, su clave y una pregunta de seguridad para recuperación de la clave.

El identificador del usuario debe ser validado, sólo puede estar formado por letras, números, y los caracteres "_" "-" "."; y tener como mínimo 5 caracteres y como máximo 15. Escribir una función de validación del identificador del usuario, e incluir al menos 10 casos de prueba significativos.

A su vez, la clave del usuario, deberá tener una longitud de entre 4 y 8 caracteres, formada por al menos una letra mayúscula, una letra minúscula, un número, y al menos uno de los siguientes caracteres: "_" "-" "#" "*". Además, no puede haber caracteres repetidos adyacentes. Escribir una función de validación de la clave del usuario, e incluir al menos 10 casos de prueba significativos.

La pregunta para recuperación de clave debe poder ser elegida entre las siguientes opciones, que deberán estar en el archivo preguntas.csv:

1,Apellido de su abuela materna
2,Nombre de tu mascota
3,Nombre de tu mejor amigo/amiga
4,Cantante preferido
5,Ciudad preferida

Deben agregar 5 preguntas más a las existentes al archivo, cada una de las cuales debe estar identificada por los números del 6 al 10 respectivamente.

Los datos de los usuarios creados deben ser guardados en un archivo csv, cuyo formato debe ser:

Id_usuario,clave_usuario,id_pregunta,respuesta_recuperacion,intentos_recuperacion

En la creación del usuario se debe controlar que el identificador del usuario no exista previamente en el archivo, en caso de existir, se debe informar "Identificador en uso".

2. Ingreso de Usuarios

Si el botón presionado es **"Ingreso Usuario"**, en este caso se desplegará una ventana con título "Identificación para acceso", que solicitará el usuario y la clave. Se deberá validar que el identificador exista y que la clave sea la correcta. Caso contrario, se deberá informar "Identificador inexistente o clave errónea", y debajo "Si no se encuentra registrado debe registrarse previamente o si olvidaste la clave presiona el botón recuperar clave".

3. Recuperación de Clave

El botón de recuperación de clave debe estar ubicado en la ventana de “Identificación para acceso”.

En caso de solicitar la recuperación de la clave, se deberá desplegar una ventana de título: “Recuperación Clave”, que le muestre al usuario la pregunta que corresponda y que le solicite el ingreso de la respuesta. Ingresada la respuesta se deberá corroborar que coincida con la registrada oportunamente por el usuario, y si esto fuera así, se le mostrará cuál es la clave de acceso que fue registrada. Si la respuesta no es la correcta, se deberá mostrar: “Respuesta incorrecta”, y además registrar en el archivo recuperacion.csv que hubo 1 intento de recuperación de clave para ese usuario. Un usuario puede tener hasta 3 intentos fallidos de recuperación de clave consecutivos. Si la recuperación fue exitosa, el valor vuelve a cero. Si el usuario tiene más de 3 intentos fallidos, su usuario debe ser bloqueado de forma que no pueda ser utilizado. Si intenta acceder al sistema y su usuario está bloqueado, se le debe advertir la situación con el mensaje de advertencia “Usuario bloqueado”.

Objetivo 2: Envío de Mensajes con y sin destinatario

Una vez que un usuario se haya identificado correctamente, accederá a la ventana de título: “cifrado y envío de mensajes”. Vamos a modificar la ventana que nos permitía presionar uno de los posibles 4 botones (Cifrar mensaje César, Cifrar mensaje Atbash, Descifrar mensaje César, Descifrar mensaje Atbash), y le sumaremos un botón de “Enviar mensaje cifrado César” y otro de “Enviar mensaje cifrado Atbash”.

En estos 2 casos, la aplicación deberá abrir una nueva ventana con un título acorde, y solicitar el ingreso de un destinatario válido. Para el caso que el mensaje quiera ser destinado a todos los usuario, se deberá indicar con el ingreso de un asterisco “*”; de lo contrario el usuario deberá ingresar como destinatario el identificador de un usuario existente.

Si el usuario ingresa un destinatario inexistente, se le debe advertir mediante un mensaje de “Destinatario Inexistente”.

Si el destinatario ingresado es válido, se debe proceder a solicitar el mensaje a cifrar de igual modo que se hacía anteriormente.

Una vez que el usuario haya ingresado: el destinatario del mensaje, el mensaje y elegido el cifrado; se deben preservar los datos en el archivo mensajes.csv.

El archivo csv, debe tener el siguiente formato:

destinatario,remitente,cifrado,mensaje-cifrado

- ➔ ***destinatario***: identificador válido ingresado por el usuario tal como lo ingresó, sin cifrar
- ➔ ***remitente***: identificador del usuario que envía el mensaje, sin cifrar

- ➔ ***cifrado***: si se utilizó cifrado Atbash, entonces, será una “A”; si en cambio el cifrado utilizado es el Cesar, será una “C”, y a continuación el valor de la clave utilizada, por ejemplo: “C9”, indicará que se utilizó Cesar con clave 9.

- ➔ ***mensaje-cifrado***: el mensaje ingresado por el usuario pero cifrado

Una vez grabados los datos en el archivo csv, se debe mostrar el mensaje:

Mensaje Enviado

El archivo mensajes.csv es acumulativo, todos los mensajes deben ser agregados a este archivo y preservarse tras las ejecuciones del programa.

Objetivo 3: Consultar mensajes cifrados

Dado que ahora los mensajes tienen un destinatario y además se preservan, el destinatario debe poder consultar los mensajes que les fueron enviados. Vamos a agregar un nuevo botón que permita “Consultar mensajes recibidos”.

Esta opción debe darle la posibilidad al usuario de leer los mensajes que hay para él en el archivo mensajes.csv y mostrárselos pero descifrados. También se le deben mostrar los mensajes que hayan sido dirigidos a todos.

Una posible forma de visualización podría ser primero los mensajes dirigidos a todos, y luego los mensajes dirigidos al usuario en particular, apareciendo desde los últimos guardados en el archivo hacia los primeros. Mostrar los mensajes de forma tal que sean claramente visualizados, por ejemplo separar de algún modo los mensajes uno de otros, y los mensajes dirigidos a todos deben ser diferenciados del algún modo, por ejemplo anteponiendo un “#” al identificador del remitente.

Ejemplo de los mensajes que podría visualizar un usuario:

```
Lista de Mensajes:
——————————————————————————————————
#RRHH: El próximo mes recibirán un aumento del 100%
——————————————————————————————————
#Gte_Vtas: La competencia lanzará un nuevo producto similar al nuestro
——————————————————————————————————
Rosa-María: Tenemos que acordar un nuevo presupuesto
——————————————————————————————————
El_Jefe: No informes en la reunión los errores cometidos en la campaña
——————————————————————————————————
Total de Mensajes: 4
```