Grado en Ingeniería del Software

Metodología de la Programación

Práctica obligatoria

SOFTWARE REQUIREMENTS SPECIFICATION

Enrique Garrido González

Raúl Hernández del Amo

Daniel Alexander Juan Moreno

Daniel Lahera Esteban

Víctor López Rodríguez

Guillermo Martín García

Daniel Moreno Godoy

Víctor Alfonso Pajuelo Aguirre

Carlos Palomares Becerra

Índice

1.Introducción

1.1. Propósito

Internet cada vez está más extendido, pero eso no solo tiene buenas consecuencias, el número de hackers maliciosos está en aumento, y uno de los problemas que causa es la filtración de información personal o el espionaje en conversaciones.

El propósito de esta aplicación es asegurar la privacidad de los usuarios evitando que se filtre información importante o sensible.

1.2. Alcance

Encriptex es una aplicación que ayuda a sus usuarios usando distintos tipos de cifrados y una clave para encriptar los mensajes y conseguir que incluso si los hackers maliciosos obtienen esa información no sean capaces de comprenderla, más tarde el usuario destinatario usaría esa misma clave para desencriptar el mensaje y poder comprender la información.

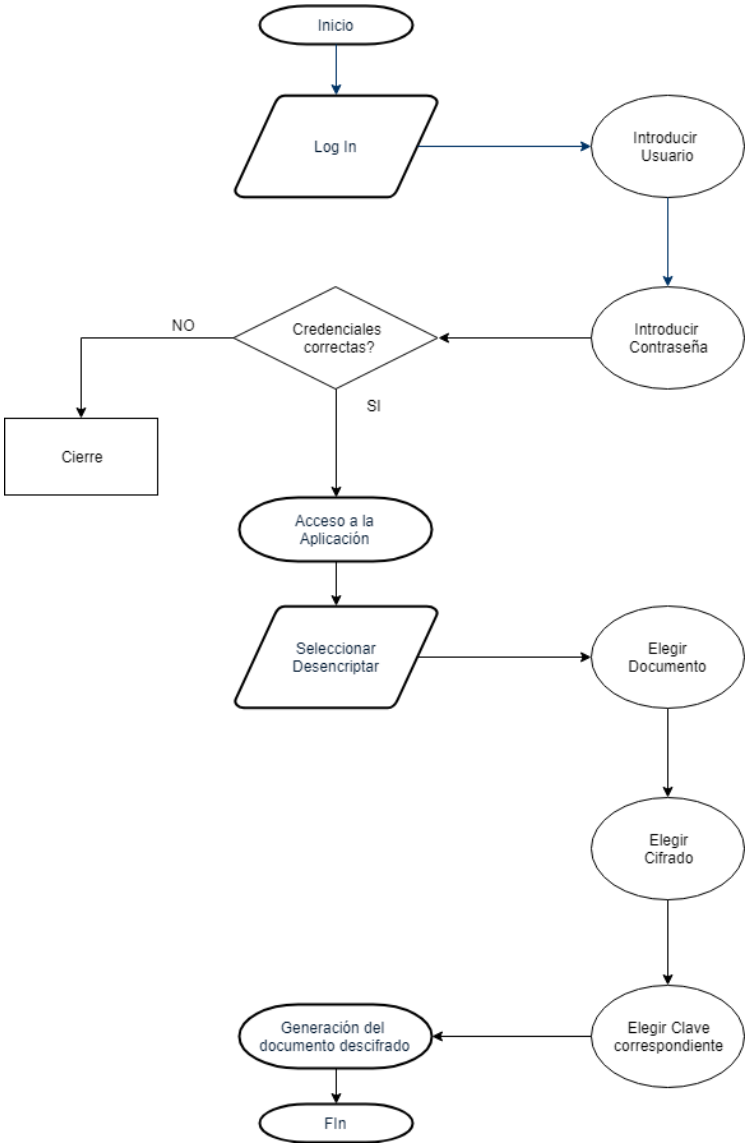
Debido a que no disponemos de un cliente que nos haya proporcionado requisitos, nosotros hemos decidido generar como base unos requisitos a los que les hemos ido aplicando cambios adecuados para mejorar el programa.

Como resultado se han creado tres apartados:

1. Requisitos diagramas que decidimos al principio del proyecto.
2. Documentación de los cambios realizados y las causas de esos cambios.
3. Instrucciones para ejecutar el programa.

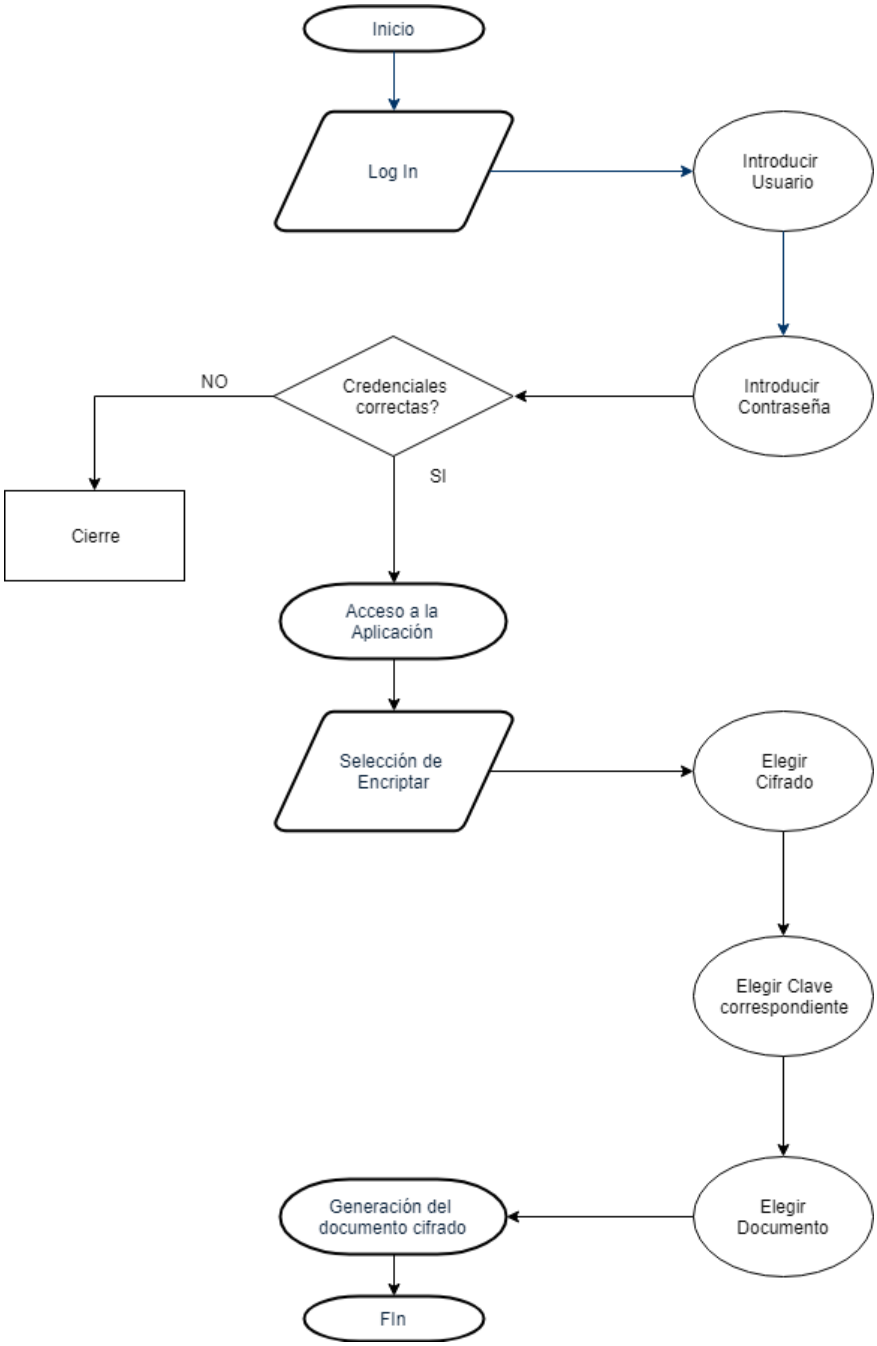
2. Descripción general

Diagrama Actividad Desencriptar



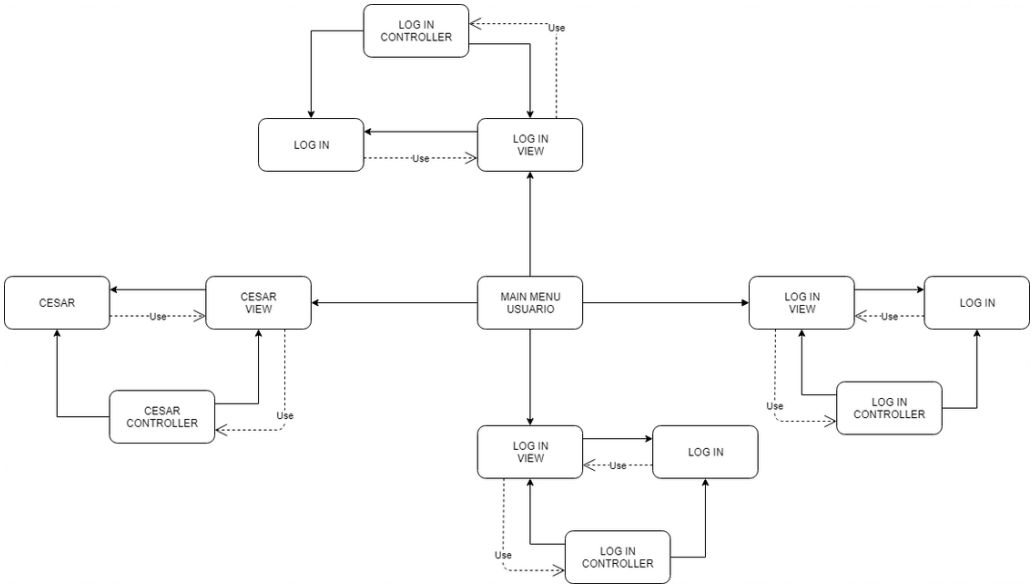
En este diagrama se muestra es flujo del proceso que realiza el usuario para desencriptar, tras realizar el log in con sus credenciales, este accederá a la aplicación desde la cual podrá seleccionar la opción de desencriptar, y al realizar la secuencia de acciones mostrada obtendrá su archivo descifrado.

Diagrama Actividad Encriptar



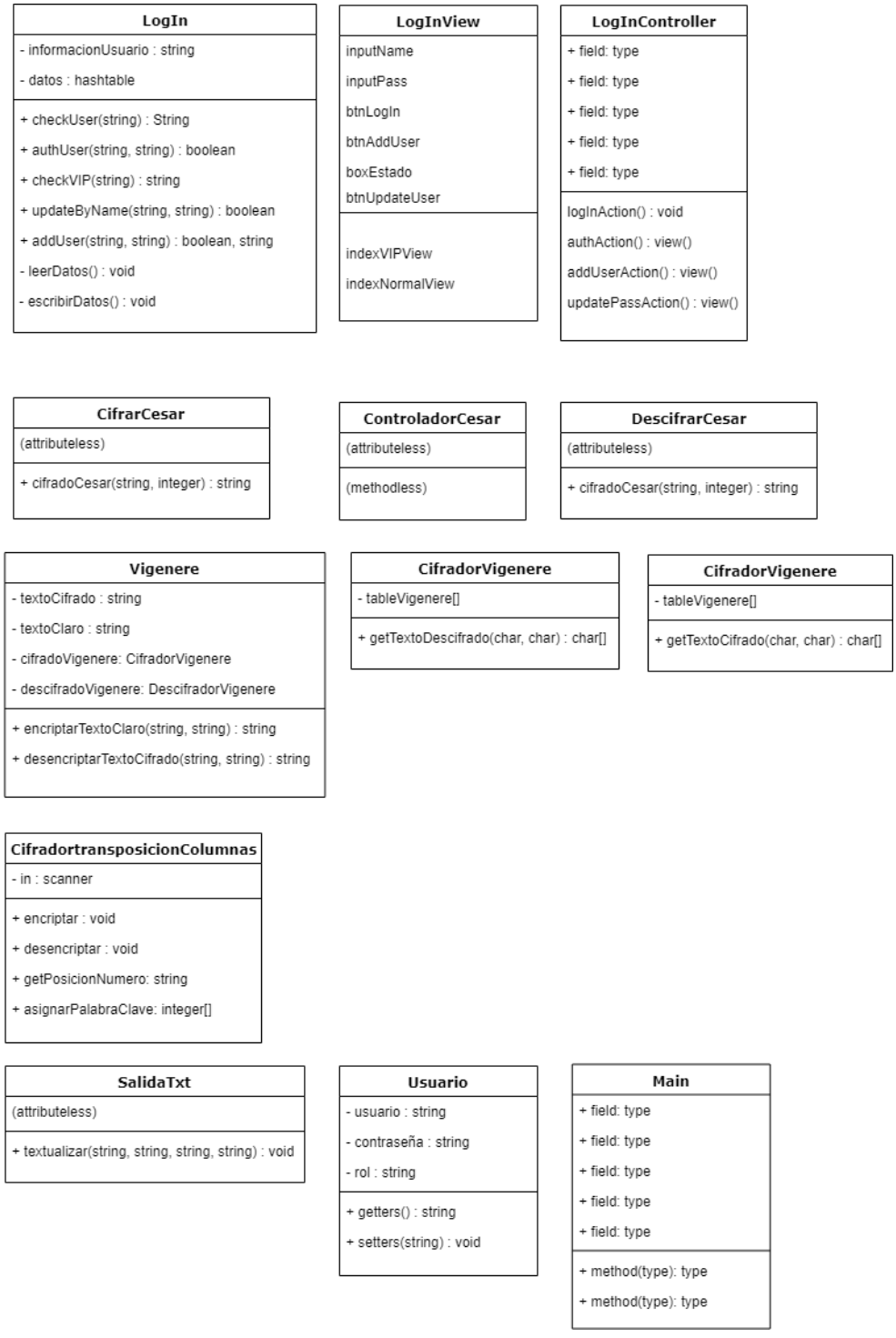
Similar al diagrama de actividad de desencriptar, tras realizar el log in con sus credenciales, el usuario accederá a la aplicación desde la cual podrá seleccionar la opción de encriptar, y al realizar la secuencia de acciones mostrada obtendrá su archivo cifrado.

Diagrama Clases



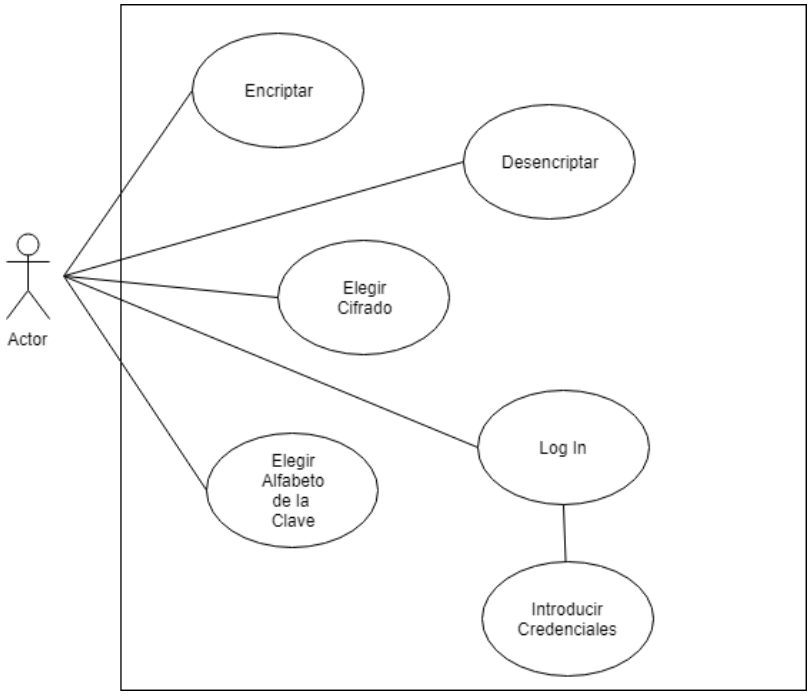
A continuación se muestra la estructura estática de la aplicación, en principio los módulos serán independientes entre sí, todos invocados por el usuario a través del menú principal. Por temas de espacio se han omitido atributos y métodos.

Diagrama Objetos



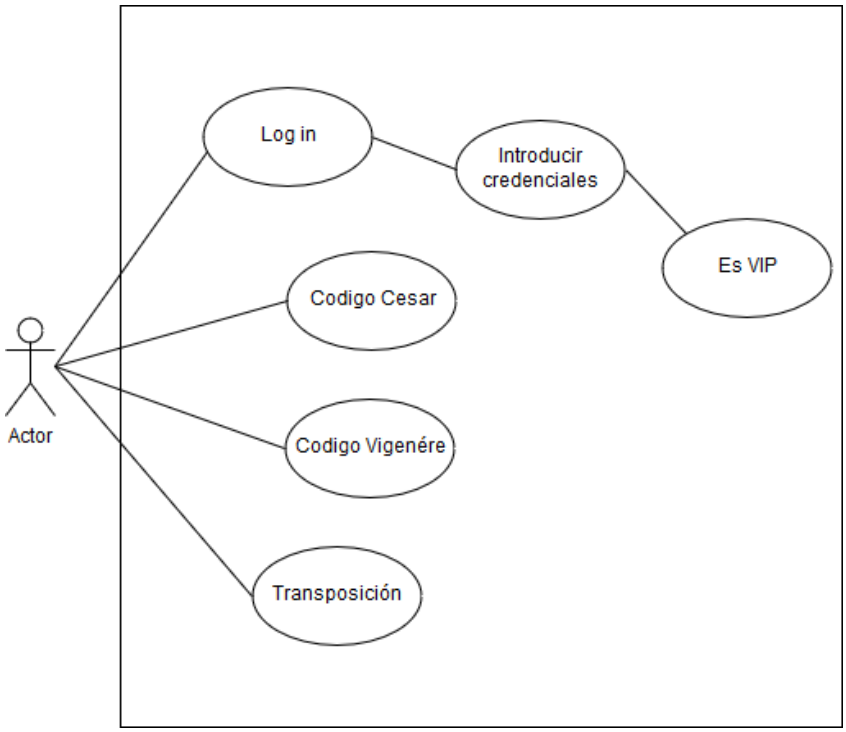
Aquí tenemos los métodos y atributos omitidos en el diagrama de clases, a priori son los mostrados, puede estar sujeto a cambios y no corresponderse al producto final.

Diagrama Caso de Uso: Aplicación General



Dada la aparente simplicidad de la aplicación, se ha realizado el caso se uso general de la aplicación para que el cliente pueda, de un solo vistazo, observar su funcionalidad. Dejar claro que para acceder a estas opciones siempre hay que pasar por el log in, como se muestra en los diagramas de actividades.

Diagrama Caso de Uso: Usuario VIP



El usuario introduce sus credenciales, el sistema lo reconoce como usuario VIP y le da acceso a los privilegios y funciones correspondientes, aparte de los que ya disfrutan los usuarios de “rol normal”. Este usuario es capaz de utilizar el método de encriptado de Vigenère.

2.1. Requisitos Iniciales

- **Funcionales:**
  - Log-in:
    - Iniciar sesión.
    - Añadir usuario.
  - Actualizar usuario:
    - Cambiar nombre de usuario.
    - Cambiar contraseña.
  - Encriptar:
    - Por teclado.
    - Por txt.
  - Desencriptar:
    - Desde teclado.
    - Desde txt.
  - Guardar a txt.
  - Sistema de rol:
    - Privilegios VIP.

- **No funcionales**
  - Tamaño máximo de 1000 caracteres.
  - Devolver mensaje en menos de 5 segundos.
  - Tamaño mínimo de la contraseña de usuario y de la clave de cifrado de 5 caracteres y máximo de 30.

2.1.1.Funcionales

Iniciar sesión

Desencadenante	El usuario selecciona log-in.
Descripción	Debido a la posibilidad de tener varios mensajes encriptados y distintas claves para cada uno se proporciona una base de datos a cada usuario donde se almacenan los mensajes con sus respectivas claves.
Precondición	El usuario introducido debe pertenecer a la base de datos.
Proceso	El usuario introduce el usuario y la contraseña y el sistema comprueba que pertenece a la base de datos.
Postcondición	Se carga toda la información del usuario.
Excepción	El usuario puede retroceder en cualquier momento.
Errores	Genera mensajes de error cuando se deja en blanco o se introduce un usuario que no existe en la base de datos y cuando deja en blanco o introduce una contraseña que no coincide con la de ese usuario.

Añadir usuario

Desencadenante	El usuario selecciona añadir usuario.
Descripción	Para poder iniciar sesión es necesario registrarse en la base de datos de usuarios.
Precondición	No existe un usuario con ese nombre en la base de datos.
Proceso	El usuario introduce usuario y contraseña y el sistema comprueba que no existe un usuario con ese nombre.
Postcondición	Se guarda el nombre de usuario y su contraseña en la base de datos.
Excepción	El usuario puede retroceder en cualquier momento.
Errores	Genera un mensaje de error cuando se deja en blanco o se introduce un usuario que existe en la base de datos.

Cambiar nombre de usuario

Desencadenante	El usuario selecciona cambiar nombre de usuario una vez ha iniciado sesión.
Descripción	Como la base de datos puede contener información privada de importancia y se pueden filtrar el nombre de usuario y la contraseña, o al usuario simplemente no le gusta el nombre que ha elegido, se le otorga la posibilidad de cambiar su nombre de usuario.
Precondición	El usuario ha iniciado sesión.
Proceso	Como ya se ha iniciado sesión, el sistema conoce el nombre del usuario, asi que solo debe introducir el nuevo nombre y el sistema comprueba que no existe ningún usuario con ese nuevo nombre en la base de datos.
Postcondición	El sistema actualiza el nombre de usuario con el nuevo nombre introducido.
Excepción	El usuario puede retroceder en cualquier momento y se queda con el nombre original.
Errores	Genera un mensaje de error cuando se deja en blanco o se introduce un usuario que existe en la base de datos.

Cambiar contraseña

Desencadenante	El usuario selecciona cambiar contraseña una vez ha iniciado sesión.
Descripción	Como la base de datos puede contener información privada de importancia y se pueden filtrar el nombre de usuario y la contraseña, o al usuario simplemente no le gusta la contraseña que ha elegido, se le otorga la posibilidad de cambiar su contraseña.
Precondición	El usuario ha iniciado sesión.
Proceso	El usuario introduce la nueva contraseña.
Postcondición	El sistema actualiza la contraseña con la nueva contraseña introducida.
Excepción	El usuario puede retroceder en cualquier momento y se queda con la contraseña original.
Errores	Se genera un mensaje de error cuando

Encriptar por teclado

Desencadenante	El usuario selecciona encriptar por teclado una vez ha iniciado sesión
Descripción	El usuario no siempre quiere encriptar textos de gran tamaño, a veces simplemente quiere encriptar una palabra o una frase, por lo que es más sencillo escribirla manualmente.
Precondición	El usuario ha iniciado sesión
Proceso	El usuario introduce el tipo de cifrado, el texto a cifrar y la clave, y el sistema cifra el texto.
Postcondición	El sistema devuelve por pantalla el mensaje cifrado con el método y la clave seleccionados y guarda el texto encriptado y la clave en la base de datos del usuario.
Excepción	El usuario puede retroceder en cualquier momento.
Errores	Se genera un mensaje de error si se deja en blanco el campo de texto, clave o tipo de cifrado y si se introduce un tipo de cifrado que no posee el sistema.

Encriptar por txt

Desencadenante	El usuario selecciona encriptar por txt una vez ha iniciado sesión.
Descripción	El usuario puede querer encriptar textos en formato txt y para ello se da la opción de cargar el archivo en el sistema.
Precondición	El usuario ha iniciado sesión y posee el archivo.txt a encriptar en algún lugar de la máquina.
Proceso	El usuario introduce el tipo de cifrado, la ruta del txt a cifrar y la clave, y el sistema cifra el texto.
Postcondición	El sistema devuelve por pantalla el mensaje cifrado con el método y la clave seleccionados y guarda el texto encriptado y la clave en la base de datos del usuario.
Excepción	El usuario puede retroceder en cualquier momento.
Errores	Se genera un mensaje de error si se deja en blanco el campo de texto, clave o tipo de cifrado, si se introduce un tipo de cifrado que no posee el sistema y si se introduce una ruta en la que no existe ningún txt.

Desencriptar por base de datos

Desencadenante	El usuario selecciona desencriptar por teclado una vez ha iniciado sesión.
Descripción	Si lo que el usuario quiere desencriptar es uno de los mensajes de la base de datos se puede hacer rápidamente seleccionándolo directamente.
Precondición	El usuario ha iniciado sesión y tiene en su base de datos el mensaje a desencriptar.
Proceso	El usuario selecciona un mensaje e introduce el tipo de cifrado y la clave, y el sistema cifra el texto.
Postcondición	El sistema devuelve por pantalla el mensaje descifrado con el método y la clave seleccionados.
Excepción	El usuario puede retroceder en cualquier momento.
Errores	Se genera un mensaje de error si se deja en blanco el campo de texto, clave o tipo de cifrado, si se introduce un tipo de cifrado que no posee el sistema y si no hay mensajes en la base de datos.

Desencriptar por txt

Desencadenante	El usuario selecciona desencriptar por teclado una vez ha iniciado sesión.
Descripción	Se quiere garantizar al usuario que si recibe un archivo.txt que contiene un mensaje encriptado, va a poder desencriptarlo sin meterlo por pantalla o tenerlo en la base de datos
Precondición	El usuario ha iniciado sesión y tiene en su equipo el archivo.txt con el mensaje a desencriptar.
Proceso	El usuario introduce el tipo de cifrado, la ruta del txt a descifrar y la clave, y el sistema descifra el texto.
Postcondición	El sistema devuelve por pantalla el mensaje descifrado con el método y la clave seleccionados.
Excepción	El usuario puede retroceder en cualquier momento.
Errores	Se genera un mensaje de error si se deja en blanco el campo de texto, clave o tipo de cifrado, si se introduce un tipo de cifrado que no posee el sistema y si se introduce una ruta en la que no existe ningún txt.

Privilegios VIP

Desencadenante	Introducción de sistema de roles para dar privilegios a usuarios VIP.
Descripción	Se quiere dotar de provilegios a usuarios VIP, que, por distintas razones, podrán acceder a más funcionalidades que los usuarios “normales”
Precondición	El usuario es un usuario de tipo VIP.
Proceso	El usuario se logea y el sistema le reconoce como usuario VIP.
Postcondición	El usuario VIP puede acceder a la encriptación por Vigenère.
Excepción	El usuario puede retroceder en cualquier momento.
Errores	Genera mensajes de error cuando se deja en blanco o se introduce un usuario que no existe en la base de datos y cuando deja en blanco o introduce una contraseña que no coincide con la de ese usuario.

2.1.2.No Funcionales

Devolver mensaje cifrado en menos de 5 segundos

Desencadenante	El usuario ejecuta la aplicación.
Descripción	Al tener en cuenta la posible impaciencia del usuario y la consecuente pérdida de usuarios, se decide que el máximo tiempo de espera para encriptar o desencriptar un mensaje será de 5 segundos.
Precondición	
Proceso	Debido a que el sistema se ha desarrollado con la intención de que este requisito se cumple siempre, no se toman medidas en caso de incumplirse.
Postcondición	La operación continúa de forma normal.
Excepción	
Errores	Como el sistema no proporciona la opción de contactar a los creadores del sistema a través de él, si el usuario detecta que la operación dura más de 5 segundos debe ponerse en contacto con ellos de forma externa para entender por qué.

Tamaño máximo de texto de 100 caracteres

Desencadenante	El usuario encripta o desencripta un texto.
Descripción	Para evitar que el encriptado tarde más de 5 segundos, se ha limitado el máximo de caracteres del texto o de un txt a 100.
Precondición	Se introduce un texto o txt.
Proceso	El usuario introduce un texto o la ruta de un txt y el programa comprueba que no supera los 100 caracteres.
Postcondición	La operación continúa de forma normal (pidiendo la clave para el encriptado o desencriptado.
Excepción	Como se puede cancelar la operación en cualquier momento también se cancela esta comprobación.
Errores	Se genera un mensaje de error cuando el texto a encriptar supera los 100 caracteres.

Tamaño mínimo de la contraseña de usuario y de la clave de cifrado de 5 caracteres y máximo de 30

Desencadenante	El usuario introduce la contraseña de usuario o la clave de cifrado.
Descripción	Como el aspecto principal del sistema es la seguridad, se valora que una contraseña o clave menor a 5 caracteres no es lo suficientemente segura y a partir de 30 sería fácil olvidarla.
Precondición	Se introduce una contraseña o clave.
Proceso	El usuario introduce una contraseña o clave y el programa comprueba que no tiene entre 5 y 30 caracteres.
Postcondición	La operación continúa de forma normal.
Excepción	Como se puede cancelar la operación en cualquier momento también se cancela esta comprobación.
Errores	Se genera un mensaje de error cuando la clave o contraseña no alcance los 5 caracteres o supere los 30.

2.2. Cambios realizados

Eliminación de la base de datos de mensajes y claves

Como el objetivo del programa es encriptar y, por tanto, la seguridad, se ha eliminado la base de datos del programa de cada usuario al considerar que la opción de exportar a txt es suficiente para mantener la información que le interese sin riesgo a que se filtre a través del programa.

Eliminación del requisito ”cambio de nombre de usuario”

Al considerar posibles actualizaciones futuras hemos eliminado la opción de cambio de nombre de usuario (por ejemplo, si se añade la opción de enviar un mensaje a otro usuario, el cambio de nombre podría causar errores en el programa o confusión en el usuario que quiere mandarlo).

Eliminación de los requisitos sobre el tamaño mínimo o máximo de caracteres en los campos

Cuando se quieren encriptar textos muy grandes manteniendo el número máximo de caracteres, la única solución sería fragmentar ese texto, como consecuencia el proceso para descifrarlo también sería más tedioso, porque el usuario tendría que descifrar varios textos individualmente y después unirlos.

Además el mensaje de error se produce una vez se ha introducido el texto, por lo que si el usuario no sabe de antemano que hay un número máximo de caracteres, se daría cuenta una vez ha introducido el texto, lo que causaría frustración.

Cambio en el requisito sobre el tiempo mínimo de encriptado y desencriptado

Al eliminar el tamaño mínimo y máximo de los campos el tiempo de encriptación puede superar los 5 segundos. Así que se ha dejado de considerar un requisito necesario para todos los casos, y se ha decidido que solo debe cumplirse cuando el número de caracteres es menor a 1000.

Inclusión de interfaz gráfica (más tarde se anula esta decisión)

Para aumentar la satisfacción de los usuarios se ha integrado una interfaz gráfica al programa, haciéndolo más intuitivo.

Eliminación de los requisitos “Encriptar por txt” y “Desencriptar desde txt”

Debido a la falta de tiempo nos hemos visto obligados a decidir entre la interfaz gráfica y la encriptación/desencriptación por txt, como los dos tipos de requisitos tienen el mismo objetivo (Facilitar el uso de la aplicación), hemos eliminado el que creemos que lo cumple peor.

Cancelación de la interfaz gráfica

A pesar de haber cancelado dos requisitos debido a la inclusión de la interfaz gráfica, al final hemos tenido problemas y por falta de tiempo se ha cancelado.