México D.F. a 6 noviembre 2017

Instituto Tecnológico y de Estudios Superiores de Monterrey
Campus Ciudad de México
Escuela Diseño, Ingeniería y Arquitectura
Departamento de Computación
SEGURIDAD INFORMATICA

El proyecto final consiste en la implementación de un programa de cifrado/descifrado de texto y de archivos. El proyecto debe utilizar el algoritmo de cifrado de AES-252.

El sistema debe presentar un GUI que permita seleccionar entre las operaciones siguientes:

- Cifrado de un texto
- Cifrado de un archivo
- Descifrado de un texto
- Descifrado de un archivo

En el caso de que un usuario requiera cifrar un archivo el sistema debe desplegar una interfaz gráfica parecida a la de la figura 1. A través de esta interfaz el usuario debe ser capaz de:

- Ingresar el texto a cifrar, es posible que el usuario pueda llevar a cabo una operación de copiar/pegar.
- Una vez ingresado el texto a cifrar, el usuario debe ingresar la contraseña, que será la base de la generación de la llave de cifrado del texto. Es posible realizar una operación de copiar/pegar si así lo requiere.
- Por default, el sistema debe de enmascarar los caracteres de las contraseñas con los caracteres que usted decida. Si el usuario lo desea puede deshabilitar esta opción presionando el botón de “Desplegar caracteres”.
- Una vez cifrado el texto, el resultado del cifrado se desplegara en la misma pantalla donde se introdujo, en base 64. El usuario podrá llevar a cabo una operación de copiar/pegar del resultado del cifrado.

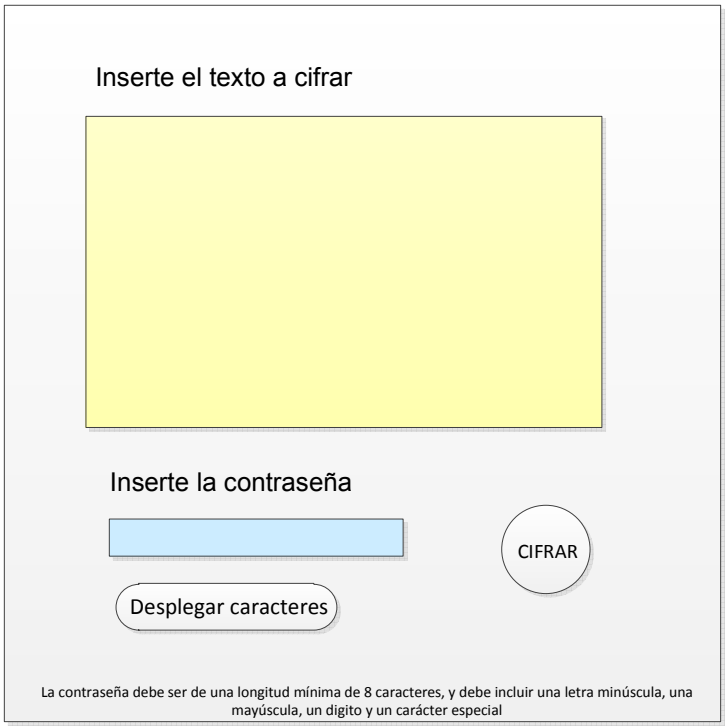

Figura 1. Interfaz gráfica para cifrado de texto

En el caso de que un usuario decida cifrar un archivo, el sistema debe desplegar una interfaz gráfica parecida a la que se encuentra en la figura 2. A través de esta interfaz el usuario debe poder llevar a cabo las siguientes operaciones:

Introducir la ruta completa donde se encuentra el archivo a cifrar, o a través del botón "Seleccionar Archivo" el sistema lo debe guiar para que pueda seleccionar dicho archivo.

Una vez seleccionado el usuario ingresará la contraseña, tomando en cuenta las mismas características del cifrado de texto.

El usuario presionará el botón de cifrar y el sistema renombrará el archivo añadiendo al final del nombre del archivo y antes de la extensión, los caracteres "**.cfr**". Si el archivo a cifrar tiene como nombre **info.doc**, el nombre del archivo cifrado será **info.cfr.doc**.

Una vez definido el nombre del archivo cifrado, el sistema debe preguntar al usuario si desea borrar el archivo original. Si el usuario responde que SI, el sistema debe borrar el archivo original y escribir el archivo cifrado en el lugar que ocupaba este. Si el sistema responde que NO, el sistema debe guiar al usuario para que seleccione el lugar donde se almacenará el archivo cifrado.

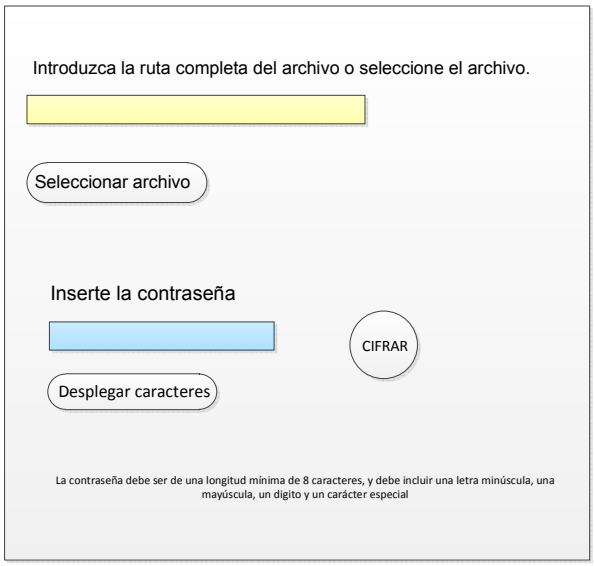

Figura 2. Interfaz gráfica de cifrado de archivos.

Para el caso de descifrar un texto, el sistema debe desplegar una interfaz parecida a la mostrada en la figura tres. A través de esta interfaz el usuario debe contar con las facultades necesarias para:

- Ingresar el texto cifrado
- Introducir la contraseña
- Presionar el botón DESCIFRAR y el texto descifrado debe ser desplegado en la misma ventana donde se introdujo el texto cifrado. Si el texto no está en formato de base 64, el sistema debe desplegar un mensaje de error.

Todos los puntos anteriores deben cumplir con lo estipulado en los dos casos anteriores.

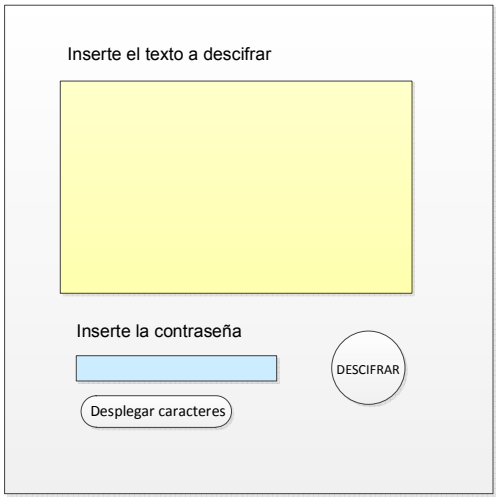

Figura 3. Interfaz gráfica de descifrado de texto.

Por último para el descifrado de archivos el sistema debe mostrar un GUI parecido al de la figura 4. El usuario seleccionara el archivo a descifrar, introducir la contraseña y presionar la opción de descifrar. Una vez descifrado el archivo, el sistema guiara al usuario para que indique donde escribirá el archivo descifrado.

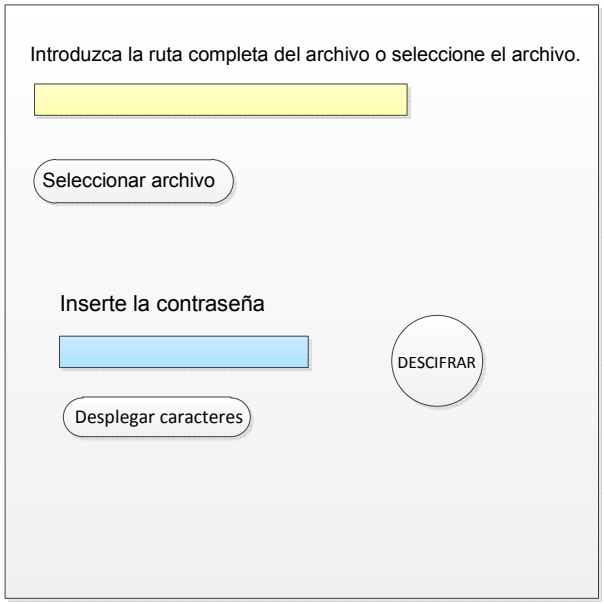

Figura 4. Interfaz gráfica de descifrado de archivos.

Consideraciones no técnicas.

- El proyecto es opcional.
- El proyecto es individual.
- Debe incluir un sistema de instalación que se encargue de instalar el programa en la computadora del usuario. No asuma que el usuario conoce de computación. Debe especificar que requiere en la computadora y como instalar lo que se requiere. El usuario lo único que debe hacer es dar doble click en un icono y el programa debe empezar su ejecución. El programa no debe ser llamado desde ningún framework de desarrollo.
- El proyecto se probará sobre un sistema Windows 7 de 64 bits.
- Es necesario incluir el código fuente impreso y en un archivo.
- Deben entregar manual del usuario, dentro del cual se debe incluir una explicación de cómo implementó el proyecto, en particular la forma en que cifraron.
- Se tomará en cuenta la facilidad de uso y la calidad de las interfaces gráficas implementadas.

- La fecha límite para entregarlo es día del examen final. Al inicio de este debe entregar los documentos impresos y ya se deberá de contar con los archivos necesarios para probar el proyecto.