Sistema de Encriptación AES-256

Manual de Usuario

Instituto Tecnológico de Estudios Superiores de Monterrey

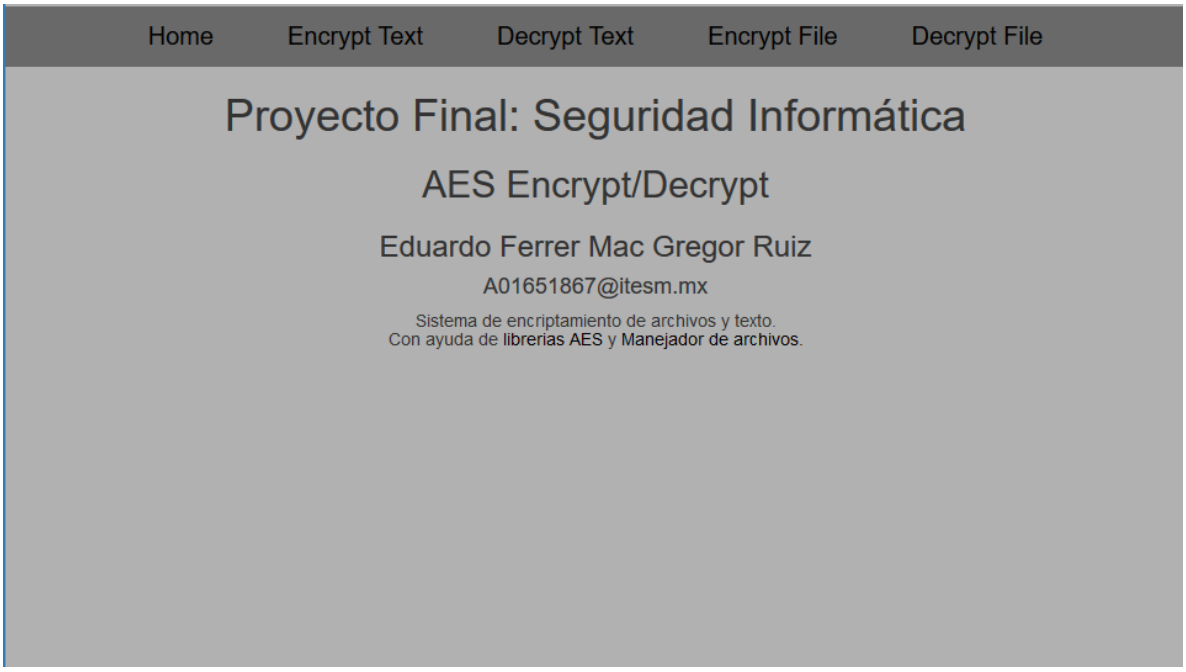
Seguridad Informática

Eduardo Ferrer Mac Gregor Ruiz A01651867

Sistema de Encriptación AES-256

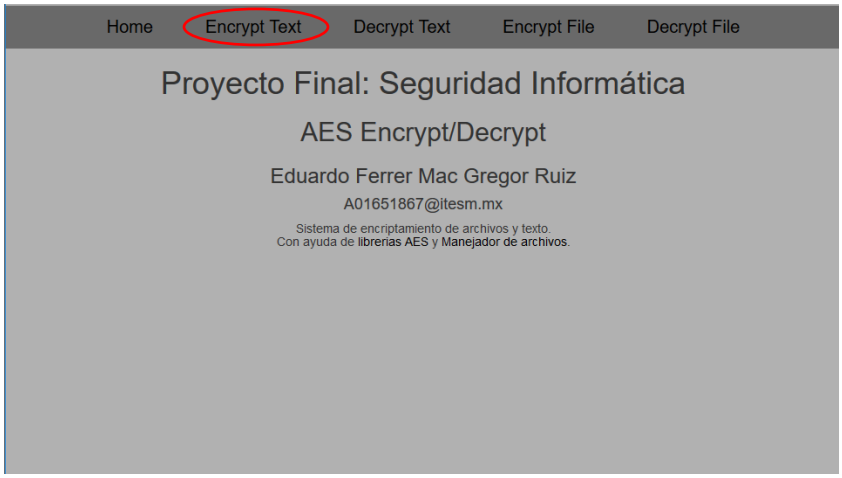
Ejecución del programa

1. Abrir la carpeta donde se ubica el software
2. Hacer click en el archivo llamado “AES-Software”, se abrirá su explorador de internet predeterminado
3. Se desplegará la pantalla inicial con una breve descripción del software



Encriptar Texto

1. Hacer click en la opción “Encrypt Text”

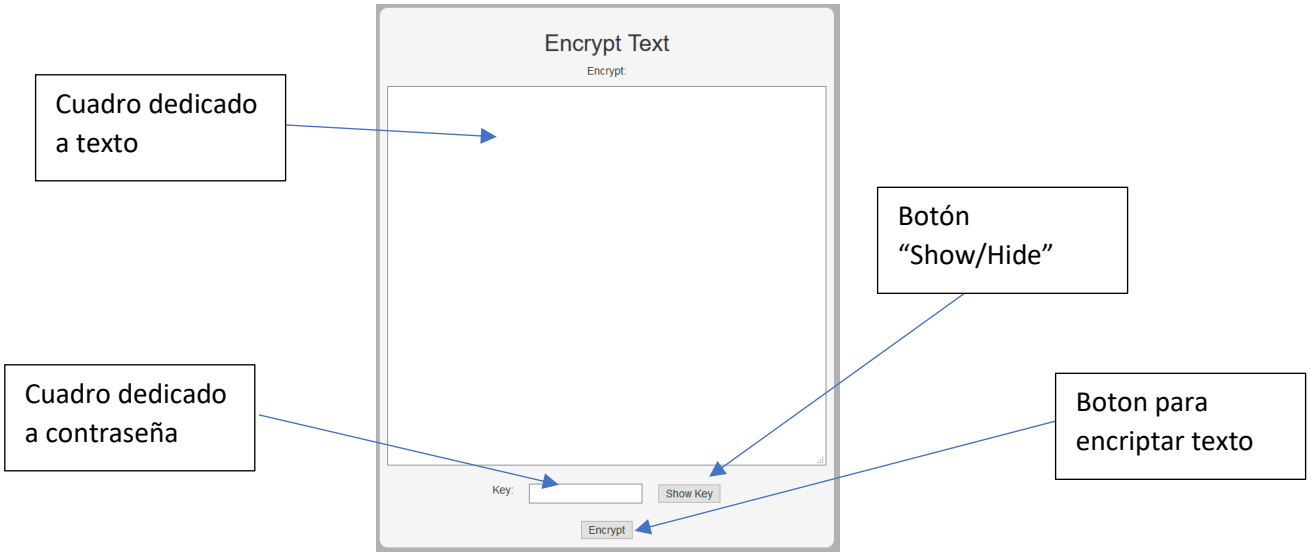


2. Ingresar el texto que se desea encriptar en el recuadro de texto dedicado
3. Ingresar la contraseña con la que se encriptara el texto en el recuadro dedicado

a. Si se desea ver la contraseña ingresada, dar click en el botón que dice “Show Key”
b. Si se desea esconder la contraseña ingresada dar click en el botón que dice “Hide Key”

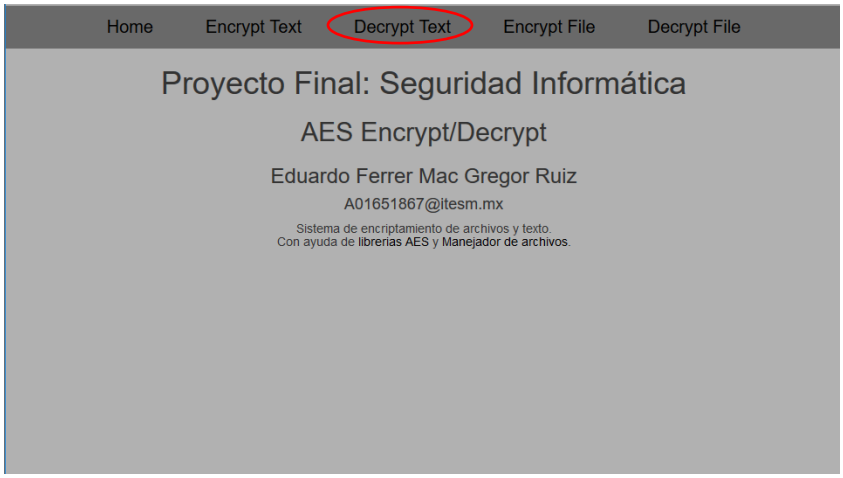
4. Dar click en el botón que dice “Encrypt”, el texto ingresado cambiará al texto encriptado

Observaciones: Cualquier texto ingresado puede ser copiado, pegado y/o cortado



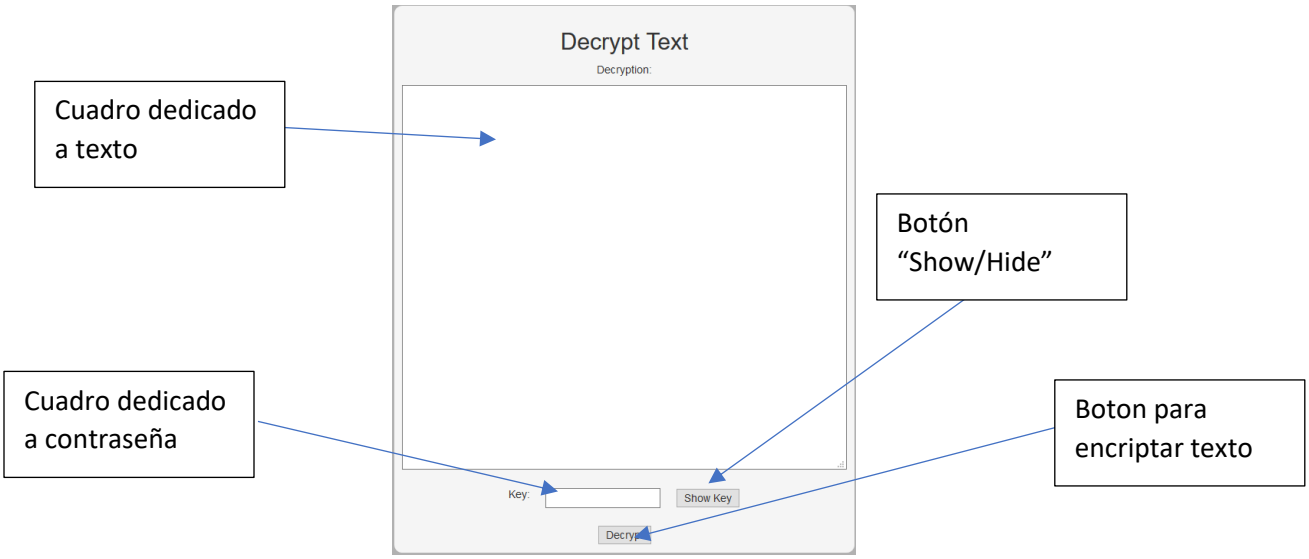
Desencriptar Texto

1. Hacer click en la opción “Decrypt Text”



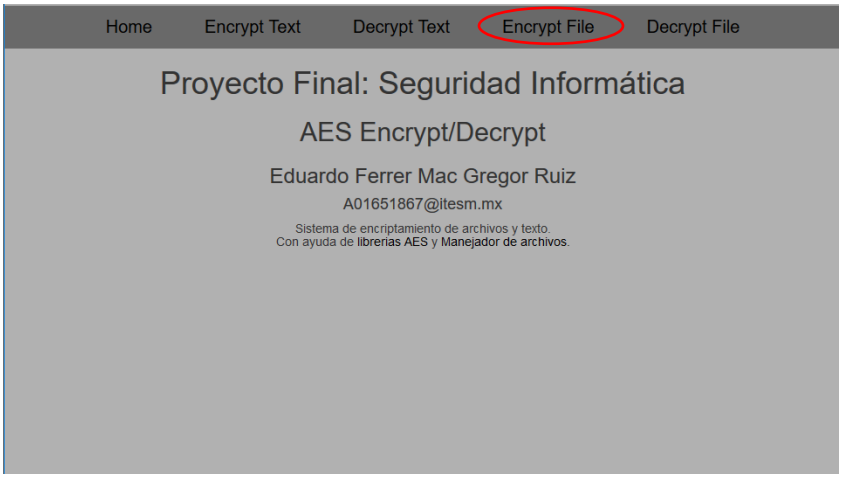
2. Ingresar el texto que se desea desencriptar en el recuadro de texto dedicado
3. Ingresar la contraseña con la que se encriptara el texto en el recuadro dedicado
    a. Si se desea ver la contraseña ingresada, dar click en el botón que dice “Show Key”
    b. Si se desea esconder la contraseña ingresada dar click en el botón que dice “Hide Key”
4. Dar click en el botón que dice “Decrypt”, el texto ingresado cambiará al texto original

Observaciones: Cualquier texto ingresado puede ser copiado, pegado y/o cortado



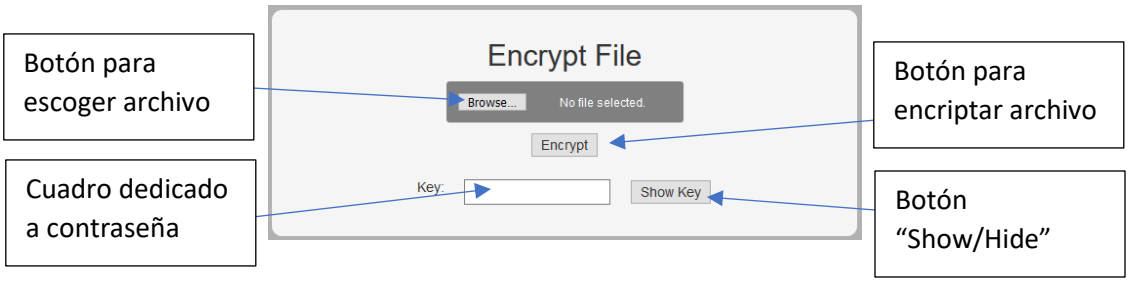
Encriptar Archivo

1. Hacer click en la opción "Encrypt File"



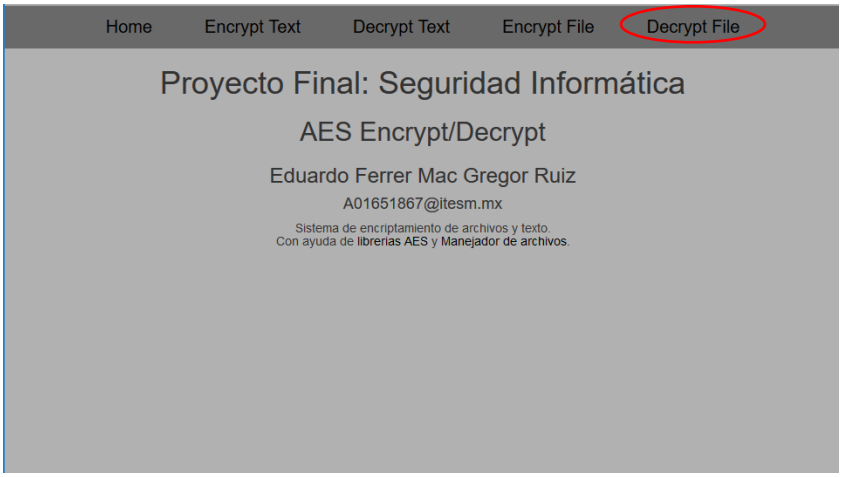
2. Dar click en el botón que dice "Browse…"
3. Se desplegará un explorador de archivos en donde debe escoger el archivo que se desea encriptar
4. Ingresar la contraseña con la que se encriptara el texto en el recuadro dedicado
    a. Si se desea ver la contraseña ingresada, dar click en el botón que dice "Show Key"
    b. Si se desea esconder la contraseña ingresada dar click en el botón que dice "Hide Key"
5. Dar click en el botón que dice "Encrypt", el explorador descargará el archivo encriptado con el mismo nombre pero sobreponiendo en la terminación de este el texto ".crt" (archivo.extension -> archivo.crt.extension)

Observaciones: Los archivos también pueden ser arrastrados al botón "Browse…" para su encripción



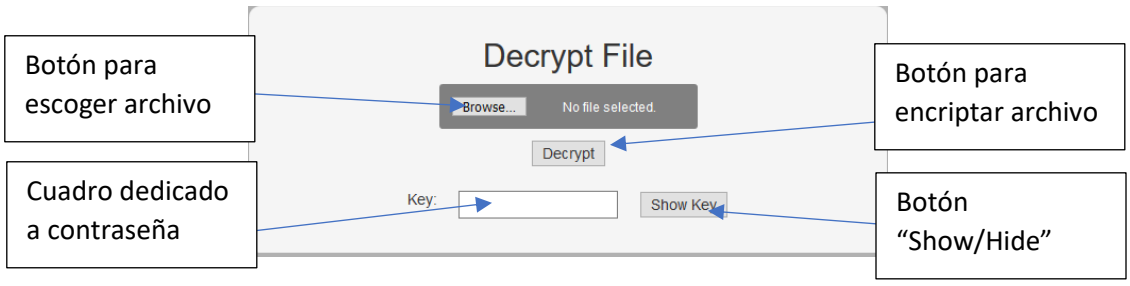
Desencriptar Archivo

1. Hacer click en la opción "Decrypt File"



2. Dar click en el botón que dice "Browse…"
3. Se desplegará un explorador de archivos en donde debe escoger el archivo que se desea desencriptar
4. Ingresar la contraseña con la que se encriptara el texto en el recuadro dedicado
    a. Si se desea ver la contraseña ingresada, dar click en el botón que dice "Show Key"
    b. Si se desea esconder la contraseña ingresada dar click en el botón que dice "Hide Key"
5. Dar click en el botón que dice "Decrypt", el explorador descargará el archivo original. Si este cuenta en su nombre con el siguiente texto ".crt", este será reemplazado por un carácter vacío. (archivo.crt.extension -> archivo.extension)

Observaciones: Los archivos también pueden ser arrastrados al botón "Browse…" para su desencripción



Algoritmo de Encriptación

Librerias utilizadas:

- AES (AES implementation in JavaScript (c) Chris Veness 2005-2014 / MIT Licence)
    - Es una librería la cual cuenta con todo el algoritmo de encriptación AES-256, además que incluye funciones para encriptar por texto plano o encriptar por archivos
- FileSaver (The MIT License Copyright © 2016 Eli Grey.)
    - Es una libreria la cual permite el manipular y generar archivos nuevos para que el explorador después pueda descargarlos

Metodología

El primer paso que tuve que realizar es la adquisición del texto deseado a encriptar y desencriptar, según la página, y verificar si está en base 64. Para esto ultimo javascript posee las funciones “atob()” y “btoa()”, las cuales convierten cualquier texto a base 64 y en caso de mostrar error es porque existe un carácter que no pertenece a ese sistema de cifrado. Luego es obtener la contraseña del usuario, la cual debió ser ingresada en la pantalla desplegada. El último paso es llamar la función que encripta texto plano de la librería previamente mencionada (encrypt(text,password,256)), esta regresa un string con el resultado del proceso de encriptación, y posteriormente desplegarlo en el recuadro de texto del sistema.

Para la encriptación y desencriptación de archivos solo se requiere obtener el archivo mediante el elemento html “input:file” e ingresar la variable en la función de la librería “encryptFile(file,password,256)”, esto claro junto con la contraseña que el usuario ingreso en la pantalla. Se tuvo que modificar la librería AES para que el archivo encriptado tuviera el nombre deseado para el proyecto. La función regresa un archivo con el nombre modificado, ya sea encriptado agregando “.crt” o desencriptado removiendo “.crt”, y este es descargado por el explorador a la ubicación que desee el usuario.

Código Desarrollado

Adjunto el código del núcleo en donde se lleva a cabo el controlador entre la interfaz y las librerías utilizadas, son 5 funciones (nombre del archivo -> js.js):

- encryptText() : Encripta texto en base64
- decryptText() : Desencripta texto en base64
- fileEncrypt() : Encripta archivos
- fileDecrypt() : Desencripta archivos
- changeInput(): Maneja el cambio entre enseñar la contraseña ingresada y ocultarla

Js.js

```
function encryptText(){
    password = document.getElementById('password').value;
    text = document.getElementById('encryptText').value;

    try{
        text = btoa(text);
        encrypt =  Aes.Ctr.encrypt(text, password, 256);

    }
    catch(err){
        alert("Not valid Base 64 text");
    }


    document.getElementById('encryptText').value = encrypt;
}
function decryptText(){
    password = document.getElementById('password').value;
    text = document.getElementById('decryptText').value;


    try{

        decrypt =  atob(Aes.Ctr.decrypt(text, password, 256));
    }
    catch(err){
        alert("Not valid Base 64 text");
    }

    document.getElementById('decryptText').value = decrypt;
}
```

```
function fileEncrypt(){
    password = document.getElementById('password').value;
    files = document.getElementById('fileEncrypt');

    encryptFile(files.files[0],password);

}

function fileDecrypt(){
    password = document.getElementById('password').value;
    files = document.getElementById('fileDecrypt');

    decryptFile(files.files[0],password);
}


var checked = false;
function changeInput(){

    if (checked) {
        checked = false;
        document.getElementById('password').type = "text";
        document.getElementById('viewPassword').value = "Hide Key";
    }
    else{
        checked = true;
        document.getElementById('password').type = "password";
        document.getElementById('viewPassword').value = "Show Key";
    }

}
```