

Memoria del Proyecto de Encriptación y Desencriptación

Índice



- [Introducción](#) 
- [Fases del proyecto](#) 
- [Manual de usuario](#) 
- [Software](#) 
- [Librerías](#) 
- [Detalles de implementación](#) 
 - [Interfaz Dinámica](#) 
 - [Encriptar](#) 
 - [Desencriptar](#) 
- [Team](#) 

Introducción

Esto es una práctica dentro de la carrera **Ing.Multimedia** en la **Universidad de Alicante**. En este proyecto se realiza un trabajo en grupo (4 alumnos) relacionado con la seguridad y donde se pretende que desarrollemos conocimientos en el ambito de seguridad.

El proyecto irá cambiando en función con las fases hasta tener un programa completo con todas las funcionalidades.

Fases del proyecto

Fase	Descripción	Requisitos	Estado
Fase 1	Implementación de un sistema que cifra y descifra archivos multimedia con AES256	<ul style="list-style-type: none">- Cifrado de al menos 6 archivos multimedia con claves diferentes- Almacenamiento de claves en un archivo o base de datos	 Completado
Fase 2	Diseño e implementación de un sistema para autenticar al administrador y encriptar claves AES con RSA	<ul style="list-style-type: none">- Autenticación del administrador- Generación de claves RSA (pública y privada)- Encriptación de claves AES con clave pública	 Pendiente

Fase	Descripción	Requisitos	Estado
Fase 3	Sistema para el acceso de usuarios a los contenidos cifrados	- Generación de claves RSA para cada usuario - Sistema de acceso a contenidos cifrados - Mejoras en el sistema de autenticación	✗ Pendiente

Manual de Usuario

Encriptar un Archivo

1. Abre la aplicación.
2. Haz clic en el botón "Seleccionar Archivo" y elije el archivo que deseas encriptar.
3. Haz clic en "Encriptar". El archivo encriptado se guardará en una carpeta específica, y se mostrará un mensaje de confirmación.

Desencriptar un Archivo

1. En la lista de archivos encriptados, haz clic en "Desencriptar" al lado del archivo que desea desencriptar.
2. El archivo desencriptado se guardará en otra carpeta, se borrará en la que se encontraba actualmente, y se mostrará un mensaje de confirmación.

Software

- **Visual Studio:** Entorno de desarrollo integrado de Microsoft utilizado para desarrollar aplicaciones, sitios web, servicios web y aplicaciones móviles.
- **.NET Framework** Tecnología que soporta la construcción y ejecución de aplicaciones y servicios web, simplifica el desarrollo y la implementación de aplicaciones.

Lenguaje: C#

Librerías

Fase 1

System: Se usa para operaciones generales y básicas

System.Collections.Generic: Almacenado y manipulación de datos, como "botonesYFilas".

System.IO: Para la lectura y escritura de archivos.

System.Windows.Forms: Construye y manipula la interfaz gráfica, como botones y paneles.

System.Security.Cryptography: Se utiliza para encriptar y desencriptar archivos.

```
System.Linq: Se usa para manipular y consultar datos a la hora del uso del "any".
```

Detalles de implementación

Fase 1

Interfaz Dinámica

El código utiliza un diseño dinámico donde los archivos encriptados se muestran en tiempo real. Cuando un archivo se encripta, se agrega automáticamente a la lista visual en la interfaz de usuario. Esto se logra a través del método [CrearNuevaFila\(\)](#) que crea una nueva fila en la interfaz para cada archivo encriptado.

Para borrar un archivo, se usa el método [EliminarFila\(\)](#) que remueve la fila de la interfaz y elimina el archivo encriptado, así como sus claves asociadas, del sistema de archivos.

La actualización de la lista visual se realiza a través del método [ActualizarLista\(\)](#), que limpia y reconstruye la lista de archivos encriptados basándose en los archivos presentes en el directorio de almacenamiento.

Para verificar y listar los archivos encriptados al iniciar la aplicación, se utiliza el método [ComprobarArchivosEncriptados\(\)](#).

Encriptar

El proceso de encriptación se inicia cuando el usuario selecciona un archivo para encriptar y hace clic en "Encriptar". El evento asociado (**encriptar_Click**) llama al método [MetodoDeEncriptado\(\)](#).

1. [MetodoDeEncriptado\(\)](#): Este método se asegura de que un archivo esté seleccionado, genera una clave y un IV aleatorios, y procede a encriptar el archivo seleccionado. Utiliza AES para la encriptación.
2. [GenerarClaveAleatoria\(\)](#) y [GenerarIVAleatorio\(\)](#): Estos métodos usan RNGCryptoServiceProvider para generar una clave y un IV aleatorios.
3. El archivo encriptado, junto con la clave y el IV, se almacenan en archivos separados dentro de un directorio específico.
4. La interfaz se actualiza automáticamente para listar el nuevo archivo encriptado mediante el [ActualizarLista\(\)](#).


Desencriptar


El proceso de desencriptación inicia cuando el usuario hace clic en "Desencriptar" al lado de un archivo encriptado listado en la interfaz. El evento asociado (**desencriptar_Click**) llama al método [Desencriptado\(\)](#).


1. [Desencriptado\(String nombre\)](#): Este método recupera la clave y el IV asociados con el archivo encriptado desde sus archivos respectivos. Luego, utiliza estos para desencriptar el archivo.
2. Utiliza AES para la desencriptación, especificando la clave y el IV, y el modo CBC.


3. El archivo descriptado se almacena en un directorio específico, y el usuario recibe una notificación de que la descriptación fue exitosa.
4. La interfaz se actualiza automáticamente para reflejar los cambios con el `ActualizarLista()`, y el archivo descriptado se puede acceder desde el directorio especificado.

Team

 Yohannes Befikadu - ybbb2@alu.ua.es

 Valentino Quiles - vqmq1@alu.ua.es

 Felix Valois - fvp10@alu.ua.es

 Jose Angel - jsg25@alu.ua.es