

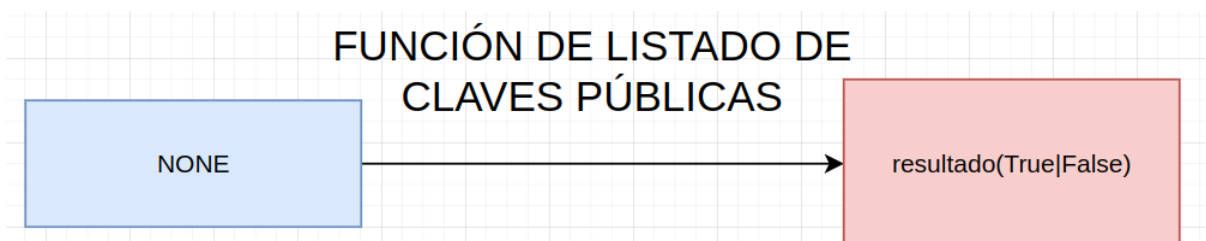
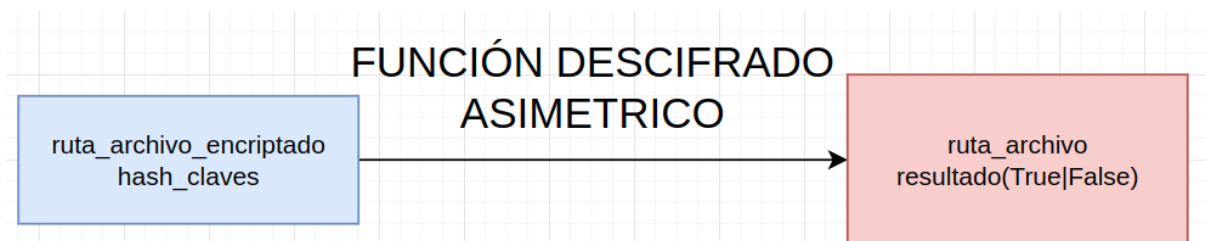
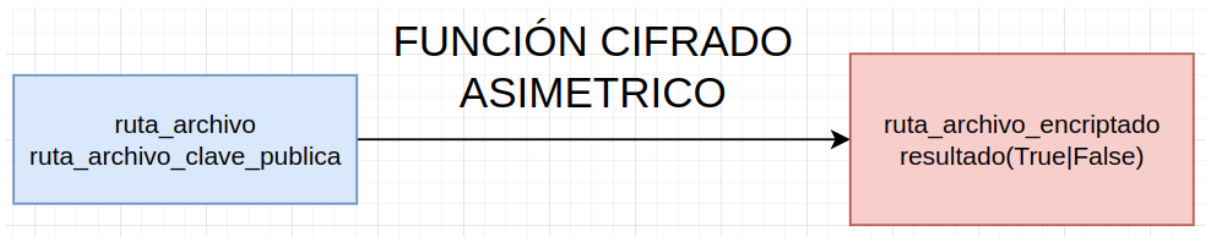
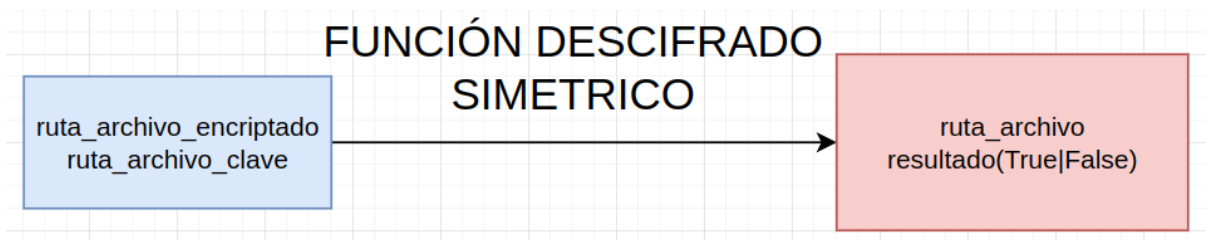
PROYECTO CIFRADOS: EXPERIENCIA DE USO

Participantes:

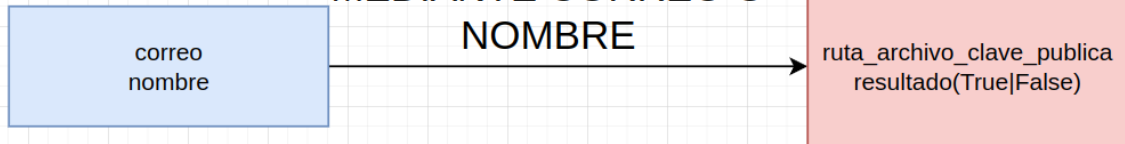
- Luis Fernando Valverde Cárdenas
- Simón Diego Ávila Garrido
- Salvador Flores Guevara

Esquema de Funciones.

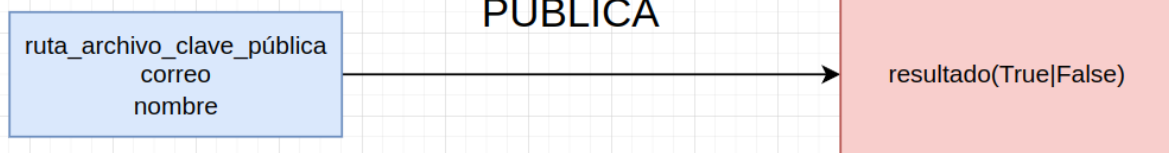
Funciones específicas



FUNCIÓN DE LOCALIZACIÓN DE LA CLAVE PÚBLICA MEDIANTE CORREO O NOMBRE

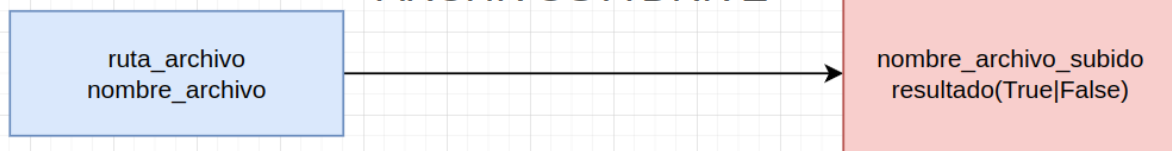


FUNCIÓN DE EXPORTACIÓN DE CLAVE PÚBLICA

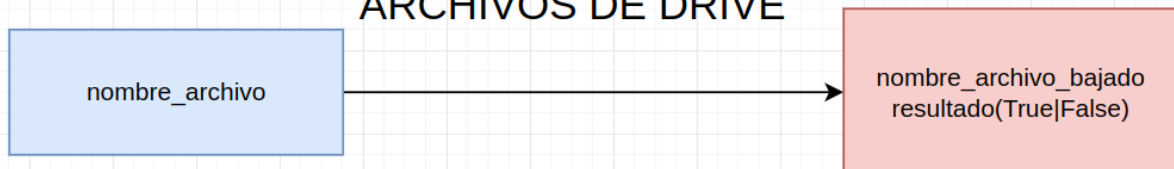


Funciones Compartidas

FUNCIÓN DE SUBIDA DE ARCHIVOS A DRIVE



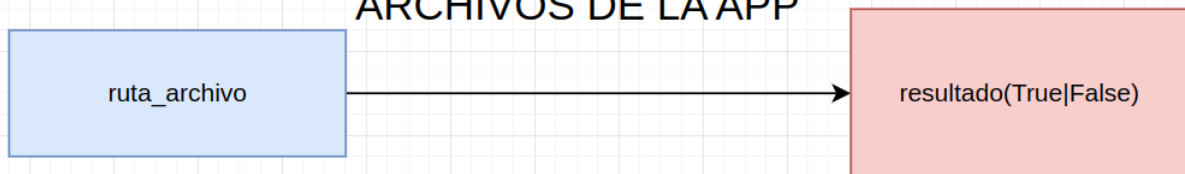
FUNCIÓN DE BAJADA DE ARCHIVOS DE DRIVE



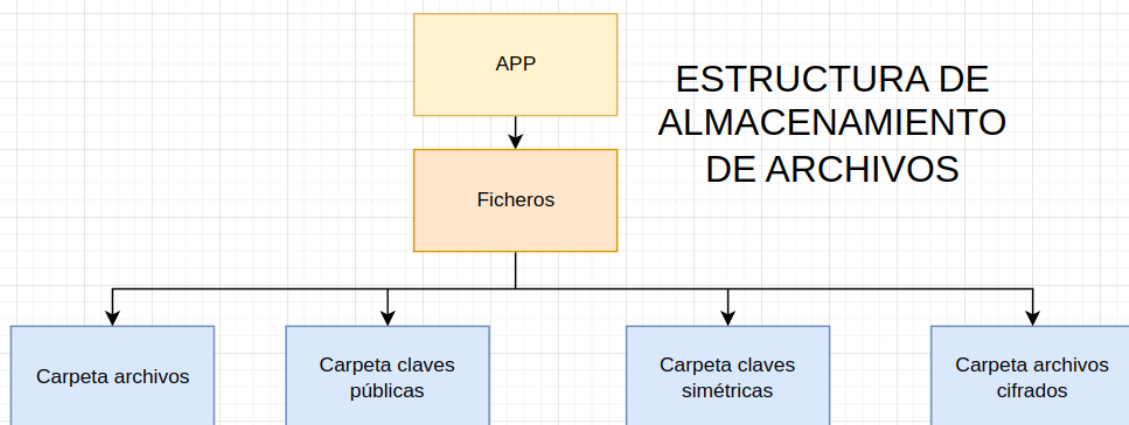
FUNCIÓN DE SUBIDA DE ARCHIVOS A LA APP



FUNCIÓN DE BAJADA DE ARCHIVOS DE LA APP



Estructura de almacenamiento de archivos.



Experiencia de uso.

CIFRADO SIMÉTRICO

Responsable: Simón Diego Ávila Garrido

- La página se compondrá de los siguientes elementos:
 - Una sección dedicada para el mensaje que desee encriptar
 - Un apartado en el que el propio usuario escribirá la clave para desencriptar dicho mensaje
 - Un apartado en el usuario dará el nombre con el que quiere que se llamen tanto el mensaje con la clave
 - Y finalmente el botón de “Encriptar”

EXPLICACIÓN DE USO:

Cuando el usuario haya elegido que es lo que quiere encriptar (un mensaje de texto, imagen, etc..) , haya generado la clave, les ponga nombre y pulse el botón sucederá lo siguiente:

1º

Automáticamente empezará la descarga de dos archivos el mensaje encriptado y la clave para desencriptarlo, adicionalmente el usuario podrá elegir si quiere que los archivos una vez descargados se guarden en su equipo o en su google drive.

2º

Después de esta operación el usuario deberá entregar el mensaje y la clave a la persona deseada.

3º

Finalmente el remitente deberá introducir la clave proporcionada para ver su contenido.

(CONSEJO): una vez usada, la clave no sirve para nada y el remitente puede borrarla, en caso de querer cifrar el mensaje de nuevo se tendrá que repetir todo el proceso anteriormente descrito.

CIFRADO SIMÉTRICO

El usuario elige lo que quiere cifrar y pulsara un boton para generar una clave, adicionalmente podra dar nombre tanto al archivo del mensaje cifrado como del archivo de la clave

Mensaje:

Clave:



Alberto



El usuario le da al botón de "Encriptar y descargar" y comenzará la descarga de los dos archivos

Ordenador de ALBERTO



Mensaje encriptado

Clave

Una vez con estos documentos, se los envía a la persona deseada



Ordenador de JUAN



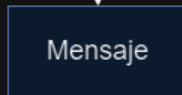
Juan

Mensaje encriptado

Clave

El receptor usa la clave para descryptar el mensaje encriptado

Mensaje



INICIO

C. SIMETRICO

C. ASIMETRICO

C. HIBRÍDO

DOCUMENTACIÓN

AREA DE CIFRADO SIMÉTRCIO

PULSE AQUI PARA ELEGIR EL ARCHIVO QUE QUIERAS ENCRYPTAR

"Nombre puesto por el usuario"

A CONTINUACIÓN PULSE AQUI PARA GENERAR LA CLAVE PARA ENCRYPTAR EL ARCHIVO

"Nombre de la clave"

REVISELO TODO ANTES DE PULSAR EL BOTON DE "ENCRYPTAR Y DESCARGAR"

ENCRYPTAR Y DESCARGAR

CIFRADO ASIMÉTRICO

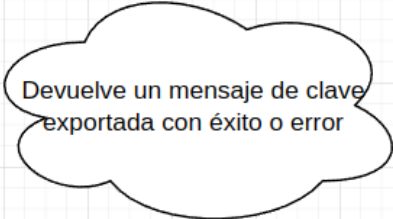
Responsable: Luis Fernando Valverde Cárdenas

Todo empezará con una página dedicada al cifrado asimétrico con diferentes apartados donde se identifican:

- Listado de claves públicas
- Exportación de clave pública

Página Cifrado Asimétrico

Exportación de claves públicas

Correo:	<input type="text" value="Introduce tu correo electrónico"/>	
Nombre:	<input type="text" value="Introduce tu nombre"/>	
	<input type="button" value="Examinar... (subir archivo)"/>	

En el apartado de “exportación de claves públicas” se le pedirá al usuario lo siguiente:

- Correo electrónico
- Nombre
- Archivo que contiene la clave pública en formato pem

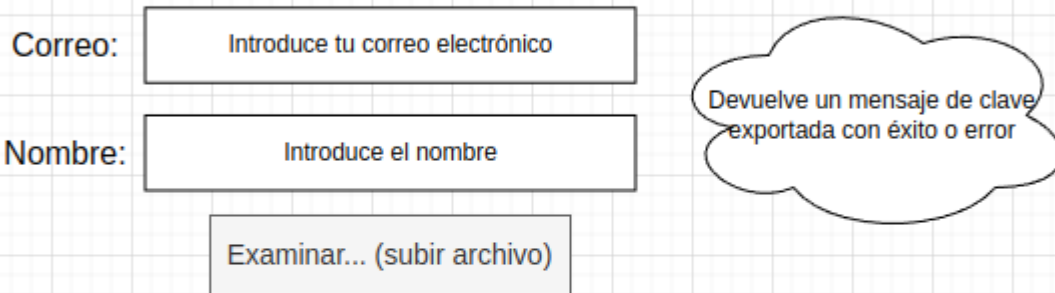
Una vez introducidos los siguientes datos, el usuario accionará el botón y la aplicación se llevará el correo y el archivo se almacenará en una carpeta (ficheros) de la aplicación.

Para que se pueda distinguir de quién es el archivo de clave pública se escribirá en un fichero índice.txt situado en la carpeta (ClavesPúblicas) donde en cada línea estará escrita el correo:nombre:rutaDelArchivo

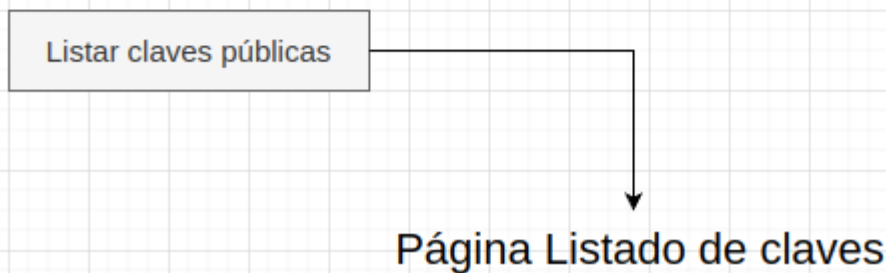
En el apartado de “listado de claves públicas” estará compuesto por un botón que al accionar el usuario será redirigido a otra página.

Página Cifrado Asimétrico

Exportación de claves públicas



Listado de claves públicas



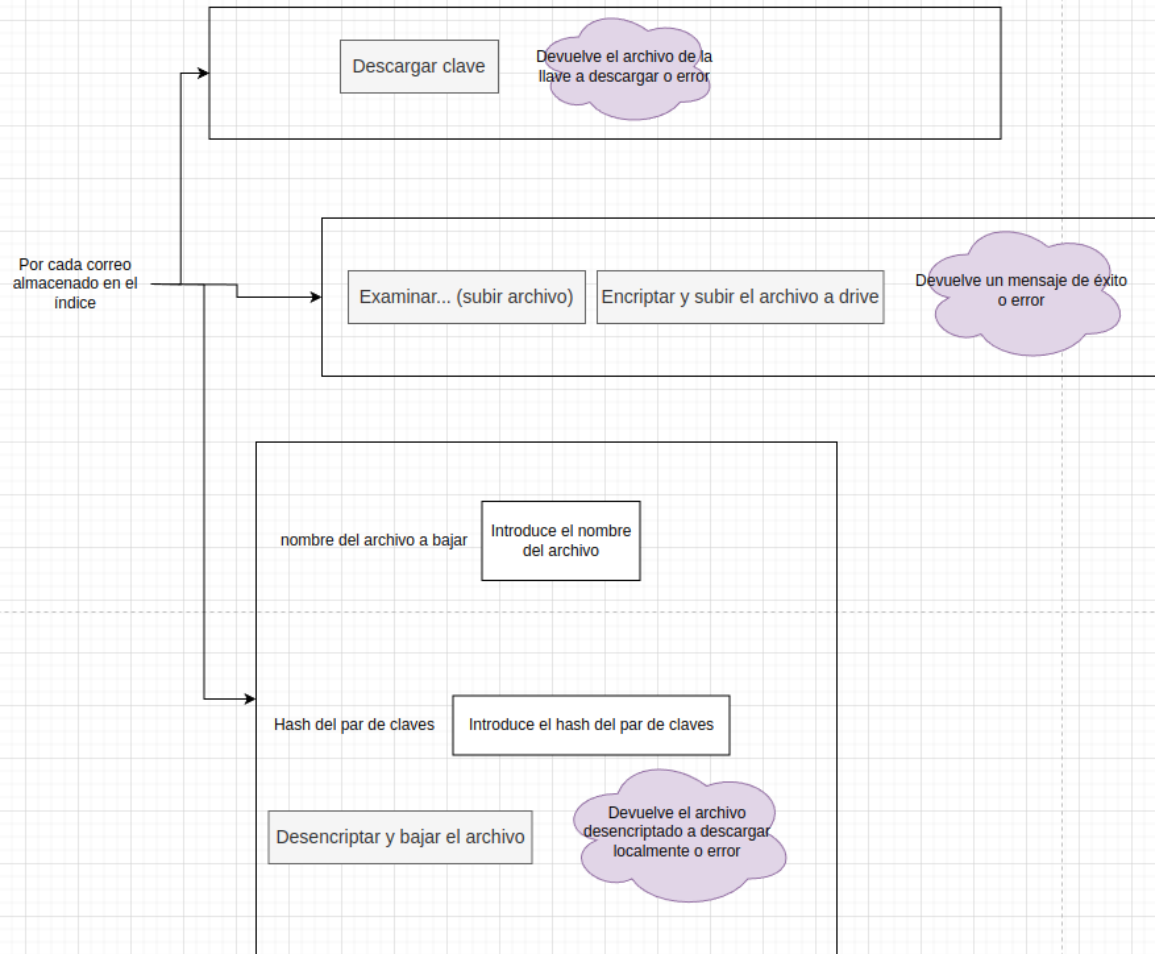
La aplicación leerá cada línea del archivo índice y separará el correo de la ruta del archivo estando separados por ':', a continuación irá generando por cada correo una serie de etiquetas html con las siguientes funcionalidades:

- Descargar clave (asociada al correo)
- Encriptar y subir archivo a drive (clave asociada al correo)
 - El usuario tendrá que especificar un archivo a encriptar y subir
- Descifrar y descargar un archivo situado en drive
 - El usuario tendrá que especificar el hash de su par de claves
 - El usuario tendrá que un menú de tipo radio en el que se le listará los archivos que ha subido a drive

En el apartado de "Descargar clave" al accionar el botón aparecerá un fichero para descargar localmente

Página Listado de claves

Correo



CIFRADO HÍBRIDO

Responsable: Salvador Flores Guevara

En primer lugar veremos una página donde aparecerá cifrado híbrido en lo que veremos 2 tipos, subir un fichero y encriptarlo y descargar un fichero de drive y desencriptarlo

Necesidades del usuario:

Aparecerá una página donde se verán los correos asociados a una clave publica, pero la página estará en el cifrado asimétrico.

Por cada correo habrá un apartado relacionado con el cifrado híbrido donde el usuario tendrá que especificar lo siguiente:

- El usuario tendrá que subir un archivo
- Contraseña

Ahora tendrá que accionar un botón para empezar el cifrado híbrido con los requisitos especificados anteriormente.

El archivo se almacenará en una carpeta de la aplicación.

Anteriormente se ha creado una función de cifrado simétrico donde como parámetros de entrada se especificará la ruta del archivo y la contraseña.

Esa función se encargará de hacer el cifrado simétrico y devolverá como resultado una clave simétrica y el archivo encriptado.

Utilizaremos la función de cifrado de asimétrico que tendrá como entrada la clave simétrica y el correo.

Y como resultado devolverá la clave simétrica encriptada

El fichero encriptado se subirá a drive y la clave simétrica encriptada también.

Aparecerá una página donde se verán los correos asociados a una clave publica, pero la página estará en el cifrado asimétrico.

Por cada correo habrá un apartado relacionado con el cifrado híbrido donde el usuario tendrá que especificar lo siguiente:

- El usuario tendrá que especificar el fingerprint de su clave privada
- Contraseña

Mediante la función de drive se descargará el archivo y la clave simétrica encriptada a una carpeta de la aplicación mediante una función creada anteriormente de cifrado asimétrico y mediante esa función tendrá como parámetros de entrada la clave simétrica encriptada y el correo y fingerprint de su clave privada, devolverá como resultado la clave simétrica desencriptada

Mediante la función de descriptado simétrico tendrá como parámetros de entrada el archivo encriptado y la contraseña y devolverá como resultado el archivo descriptado y dicho archivo se le descargará al usuario.

CIFRADO HÍBRIDO

ENCRIPtar ARCHIVO

ELIJA EL ARCHIVO

EXAMINAR
ARCHIVO

CONTRASEÑA

ESCRIBA AQUI SU
CONTRASEÑA

ENCRIPtar

DESENCRIPtar ARCHIVO

LISTA DE ARCHIVOS

ELIJA SU ARCHIVO

CONTRASEÑA

ESCRIBA AQUI LA
CONTRASEÑA

DESENCRIPtar