



Índice

[**• ¿Cuál es el propósito de su aplicación?**](#_gjdgxs) **3**

[**• ¿Para qué utiliza el cifrado asimétrico?**](#_g3sm5kfiortr) **3**

[• ¿Qué algoritmos ha utilizado y por qué?](#_1fob9te) 3

[• ¿Cómo gestiona las claves?](#_3znysh7) 3

[CAPTURAS](#_uukcuui80oib) 4

[**• ¿Para qué utiliza la firma digital?**](#_1gxrzkb71r1m) **4**

[• ¿Qué algoritmos ha utilizado y por qué?](#_3dy6vkm) 4

[• ¿Cómo gestiona las claves?](#_ab9ap8bjm7zy) 4

[• ¿Cuál es la PKI que ha desarrollado?](#_573ikfh7y0ig) 4

[CAPTURAS CÓDIGO](#_3tsax388ypye) 5

[• ¿Qué tipo de autenticación ha implementado?](#_37i5smq3vi4o) 7

[• ¿Por qué ha escogido este tipo y no otro?](#_afbu9pvqznsj) 7

[• ¿Cómo lo ha implementado?](#_gvycnsym8obp) 8

[CAPTURAS CÓDIGO](#_sb1p77ukbewj) 8

[**Mejoras**](#_ropxwttwgz6t) **9**

Grupo: 12

ID de grupo de prácticas: 12

Nombre de todos los alumnos:

* José David Rico Días (100441800)
* Samuel Fernández Fernández (100432070)

------------------------------------------------------------------------------------------------------------------------------

**Credenciales para acceso a nuestra aplicación criptográfica:**

[Enlace a la aplicación](https://losladrones.josedaviddavi41.repl.co) (Si el enlace está roto enviar correo a 100441800@alumnos.uc3m.es)

**DNI / NIE:** 24769653X

**Clave:** 12345678

------------------------------------------------------------------------------------------------------------------------------

# • ¿Cuál es el propósito de su aplicación?

Nuestra aplicación es un sistema de gestión bancaria llamado "LOSLAdrones", donde tendremos diferentes funcionalidades como el registro de usuarios, el inicio de sesión, la transferencia de dinero, consulta de saldo, ver movimientos o borrar la cuenta. En esta primera entrega hemos implementado el inicio de sesión, la consulta de movimientos y el cierre de la sesión.Logotipo, nombre de la empresa

Descripción generada automáticamente

Mediante esta aplicación pretendemos crear un sistema seguro y encriptado (como expondremos a continuación) de gestión personal de cuentas.

# **•** ¿Para qué utiliza el cifrado asimétrico?

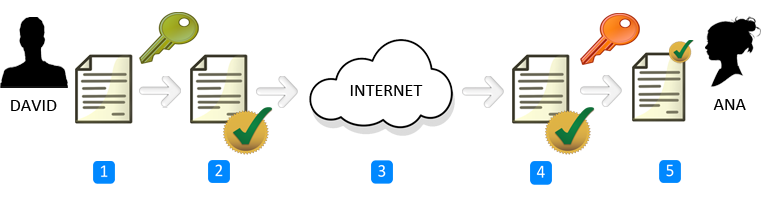
En nuestra aplicación utilizamos el cifrado asimétrico para cifrar la petición al servidor de certificación raíz.

## • ¿Qué algoritmos ha utilizado y por qué?

Hemos utilizado el algoritmo RSA ya que es el algoritmo de cifrado asimétrico más cómodo de usar ya que viene implementado en el propio navegador.

## **•** ¿Cómo gestiona las claves?

En este caso las claves son generadas automáticamente y almacenadas en el navegador al realizar la petición.



### 

### CAPTURAS

# 

# 

# 

# 

# 

# 

# 

# 

# 

# • ¿Para qué utiliza la firma digital?

En nuestra aplicación firmamos un pdf emitido por nuestro sistema donde veremos el número de cuenta y el saldo actual. Además, al abrir el pdf podemos ver cómo está firmado y comprobarlo desde este mismo como se muestra en las capturas posteriores.

## **•** ¿Qué algoritmos ha utilizado y por qué?

Hemos utilizado el algoritmo RSA ya que es un sistema criptográfico de clave pública que utiliza la factorización de números enteros y está ampliamente extendido.

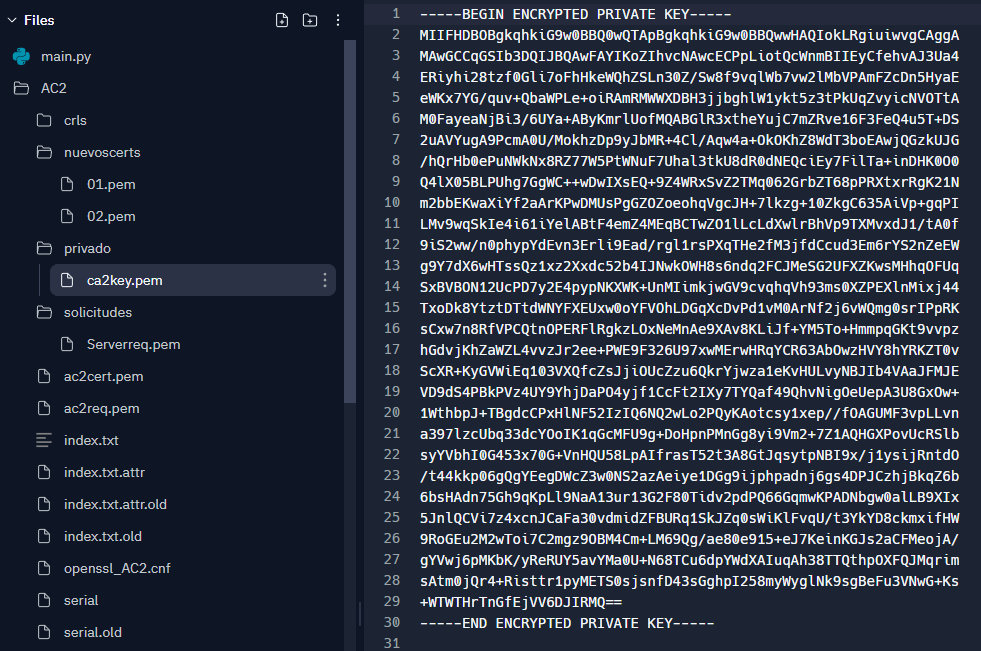
## **•** ¿Cómo gestiona las claves?

Las claves son almacenadas en el propio servidor y para el sistema de firma el servidor obtiene un hash del mensaje a firmar y lo procesa con su clave privada obteniendo así la firma; se envía el mensaje y la firma; entonces el usuario recalcula el hash y descifra el hash original con la clave pública del emisor, validando así la firma del mensaje. Además el algoritmo es seguro mientras no exista una forma rápida de descomponer un número grande en producto de primos.

## **•** ¿Cuál es la PKI que ha desarrollado?

Hemos creado una infraestructura de clave pública donde tenemos a una autoridad AC1 (Autoridad de certificación raíz), la cual es un código y servidor aparte que hemos creado para extender un certificado a una autoridad AC2 (Autoridad subordinada) que se encargará de expedir certificados para todos los servidores del banco (A).

### CAPTURAS CÓDIGO



## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

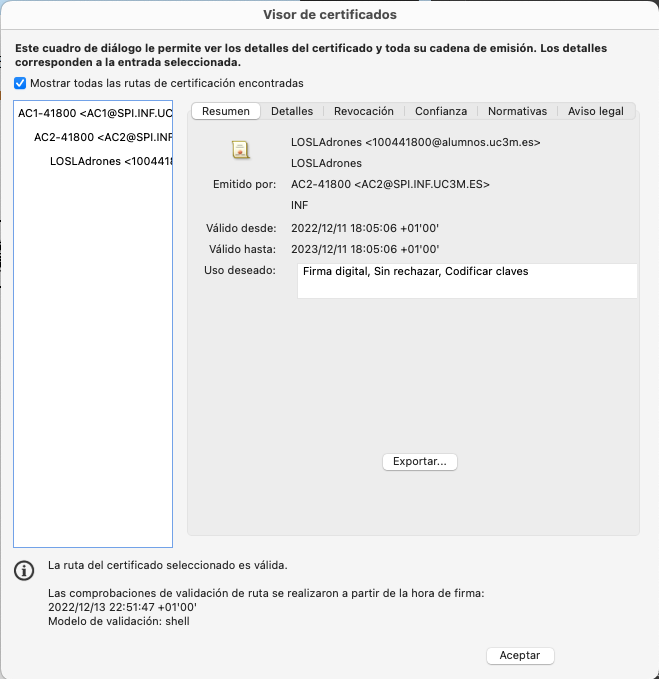
## 

## 

## 

## 

## 



## **•** ¿Qué tipo de autenticación ha implementado?

En nuestra aplicación hemos implementado la autenticación mediante secretos donde los usuarios conocen su DNI y su contraseña y para acceder a su cuenta del banco deben introducirlos, además estos datos son gestionados en nuestra base de datos la cual se cifra simétricamente.

## **•** ¿Por qué ha escogido este tipo y no otro?

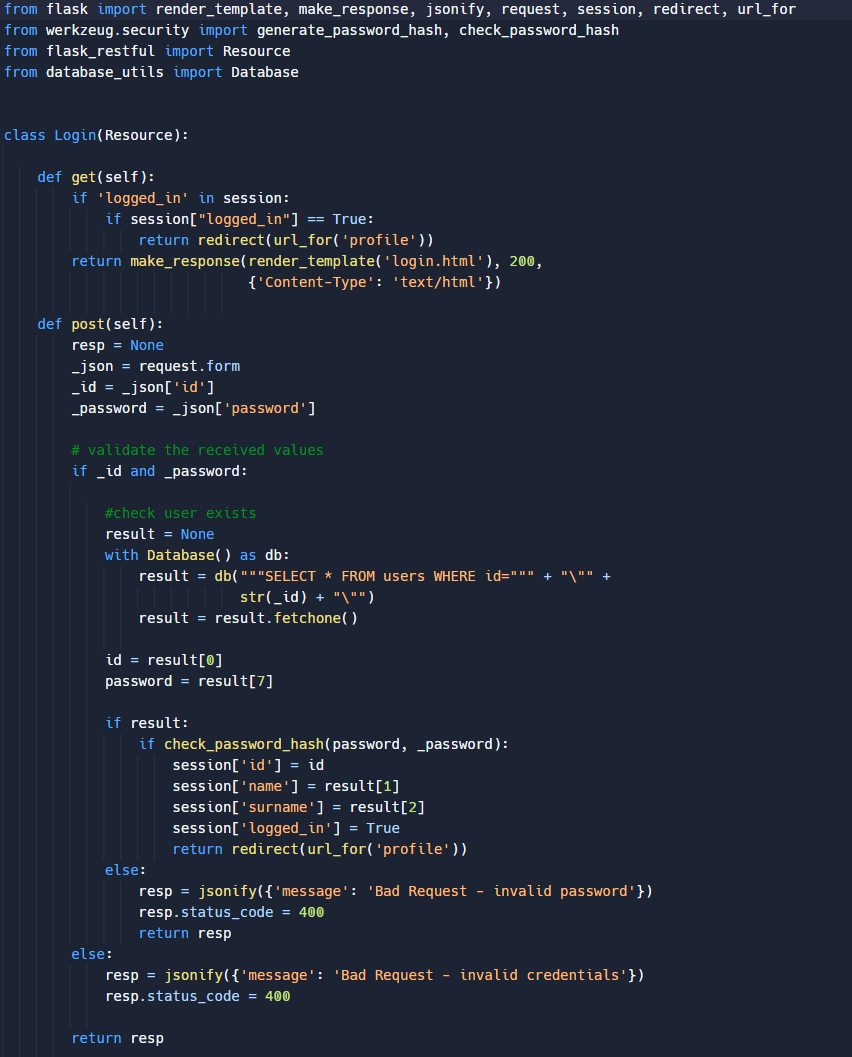
Hemos escogido la autenticación mediante secretos en gestión de contraseñas ya que es un sistema sencillo y amigable con los usuarios, además nos permite gestionar a los usuarios y sus contraseñas en nuestro sistema de una forma eficiente.

## **•** ¿Cómo lo ha implementado?

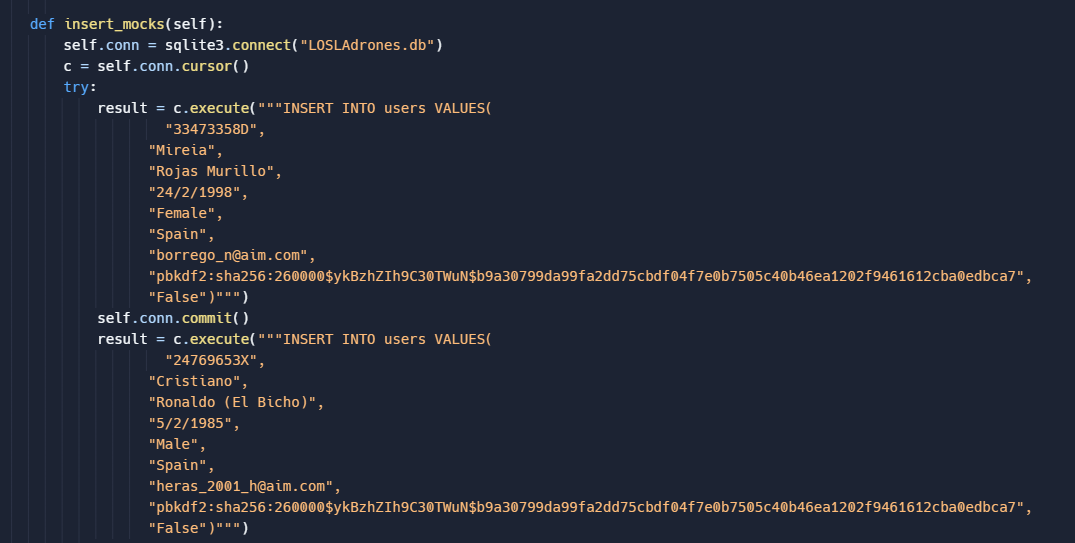
Con el servidor activo, cuando un usuario introduce un DNI y una contraseña se crea una consulta a nuestra base de datos, donde se comprueba si el DNI existe y es correcto, además, comprueba que la contraseña sea correcta comparando los hashes, ya que esta está almacenada de forma hasheada en nuestra BBDD para la máxima seguridad. Si todo está en orden el usuario es redirigido a su perfil personal.

### 

### CAPTURAS CÓDIGO



# 



# 

# Mejoras

Puedes descargar el pdf firmado donde está implementado un código QR que te redirecciona a nuestra app.