

CRİPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Grupo 81

JUAN MIGUEL PULGAR ESQUIVEL 100451036

100451036@alumnos.uc3m.es

ALBA MARCO UGARTE 100451139

100451139@alumnos.uc3m.es

ID DEL GRUPO DE PRÁCTICAS: 19

DICIEMBRE DE 2022

**GRADO EN INGENIERÍA INFORMÁTICA
UC3M**



- **¿Cuál es el propósito de su aplicación?**

Nuestra aplicación es un casino virtual, donde los usuarios pueden jugar a la ruleta y al blackjack apostando dinero (Waton Coins).

Cuando el usuario entra en la aplicación se muestra un menú para registrarse o iniciar sesión si el usuario ya tiene cuenta.

```
¡Bienvenido a Casino Watón!  
  
Seleccione una opción:  
1:Iniciar sesión  
2:Registrarse  
3:Salir
```

Imagen 1: Menú de inicio

Al registrarse, se pedirán los datos personales del usuario, donde se incluye el DNI, la tarjeta de crédito y una contraseña.

Si el usuario ya se registró anteriormente, podrá iniciar sesión. La aplicación comprobará que la contraseña es válida y se corresponde con la del usuario registrado.

Si el usuario ya ha iniciado sesión, le llevará a un menú donde puede retirar o ingresar dinero (WatonCoins) , jugar a la ruleta o al blackjack.

```
Bienvenido, Darwin McMuffin  
¿Que quieres hacer hoy, Darwin McMuffin ?  
  
1:Ruleta  
2:BlackJack  
3:Ingresar dinero  
4:Retirar dinero  
5:Consultar datos personales  
6:Cerrar sesión
```

Imagen 2: Menú principal

Antes de empezar a jugar a la ruleta o al blackjack la aplicación preguntará al usuario que cantidad de dinero quiere apostar. Cuando se ha introducido la apuesta, comienza el juego. (La ruleta y el blackjack están simplificados).

En la ruleta tienes que apostar por un número del 0 al 36. Tu apuesta se duplicará si sale un número par y has apostado por uno par (o impar-impar) y tu apuesta se multiplicará por 14 si sale el 0 (y has apostado por el número 0).

```
¿Cuanto dinero quiere apostar?  
100  
¿A que número desea apostar? (Número entre 0 y 36)  
5  
¡Ha salido el número: 24 !  
  
¡Mala suerte, has perdido!  
Se han retirado: 100 de tu cuenta.  
Tu saldo restante es: 9900 Watón Coins
```

Imagen 3: Ejemplo de ruleta

El objetivo del blackjack es quedarse lo más cerca posible del número 21 pero sin pasarse. Si algún participante se pasa del 21, habrá perdido. Gana el juego quién tenga un valor de cartas más cercano al 21 (sin pasarse) .

En el blackjack se comienza barajando. Después se entrega una carta al mesero y dos al participante, todas las cartas son visibles para los demás usuarios.

Ahora comienza el turno del participante, éste decidirá si quiere otra carta o no dependiendo del valor de sus cartas. Si supera los 21 puntos perderá y si no, será el turno del mesero.

El mesero pedirá cartas hasta que superé el valor del otro participante o se pase de 21 puntos. A continuación se muestra una simulación de una partida de blackjack.

<pre>Barajando... Tus cartas son: [[4, 'PICAS'], [2, 'CORAZONES']] El valor de tus cartas son: 6 Las cartas de la casa son: [['A', 'TREBOLES']] El valor de las cartas de la casa son: 1 ¿Pides otra carta? S/NS Tus cartas son: [[4, 'PICAS'], [2, 'CORAZONES'], [9, 'CORAZONES']] El valor de tus cartas son: 15 Las cartas de la casa son: [['A', 'TREBOLES']] El valor de las cartas de la casa son: 1</pre>	<pre>¿Pides otra carta? S/NN Tus cartas son: [[4, 'PICAS'], [2, 'CORAZONES'], [9, 'CORAZONES']] El valor de tus cartas son: 15 Las cartas de la casa son: [['A', 'TREBOLES'], [10, 'PICAS']] El valor de las cartas de la casa son: 11 Tus cartas son: [[4, 'PICAS'], [2, 'CORAZONES'], [9, 'CORAZONES']] El valor de tus cartas son: 15 Las cartas de la casa son: [['A', 'TREBOLES'], [10, 'PICAS'], ['J', 'PICAS']] El valor de las cartas de la casa son: 21 !Perdiste Watón! Otra vez será. Se han retirado: 100 de tu cuenta. Tu saldo restante es: 9800 Watón Coins</pre>
---	--

Imágenes 4 y 5: Ejemplo de blackjack

En nuestra aplicación hay dos tipos de usuarios, los clientes del casino y los “admins” que son cuentas especiales que pueden organizar y enviar certificados sobre el casino. Los administradores solo pueden ser creado desde la base de datos, así evitamos que un cliente tenga una cuenta de administrador.

```
{
  "nombre": "gAAAAABjf4UHNgEPOXtERw7fct3M2vu2H0_YCD1z9w5GDtwBeqKoc1c2ZYp_sX5Gu1AytKpR4h7V09fz3lquJe5WcLC588nudA==",
  "apellido": "gAAAAABjf4UHsYXr1RCctHDFvX9dz3zTk1-tl494rs7sxYZ7nMUcOuKPMUC9Wyr_3to6ZRFBvpE0XNgKeJVbDE2252W-0JzTMA==",
  "fecha": "gAAAAABjf4UH7MhzEQmL5ot-dxZ7Kvp2IMZ94fJA7Kc8DaukloaOC1YENAQEPNGcFRvLfmcP_yC_kr-fZmcNLYP1rQITC5WdKQ==",
  "DNI": "gAAAAABjf4UHRggn6oZN899xUlaXd4Sqicf9vVrLoU-p9_BAAd2Es7t1cI6M08iUL-Ptx5p1NAFby34aM00dNw8oHAHhHopZzw==",
  "Rol": "Admin",
  "usuario": "Admin"
}
```

Imagen 6: Ejemplo de usuario administrador

El menú para los administradores añade una función llamada “Enviar comunicado”, desde esta función el administrador que normalmente será el director del casino podrá enviar mensualmente sus informes de ganancias y/o pérdidas a “Hacienda”.

Imagen 7: Menú principal para Administrador

```
Preparando su comunicado mensual...

El comunicado es:
Hola Hacienda,
los gastos de este mes han sido : 10000000000000000 watonCoins
Firmando...
Validando firma...
La firma es válida
```

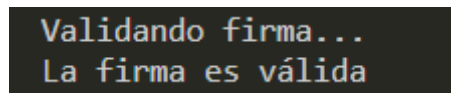
• ¿Para qué utiliza la firma digital? ¿Qué algoritmos ha utilizado y por qué? ¿Cómo gestiona las claves? ¿Cuál es la PKI que ha desarrollado?

```
{
  "mensaje": "Hola Hacienda, \nlos gastos de este mes han sido : 1000000000000000 watonCoins."
}
```

Para implementar la firma, hemos generado una clave pública y una clave privada para el director de la aplicación, que están ubicadas en los archivos Acert.pem y Akey.pem, respectivamente. Una vez hemos generado las dos claves, se utiliza una función resumen sobre el comunicado utilizando SHA256 y utilizamos la clave privada del director para firmar el resumen.

Imagen 9: Ejemplo de archivos

Una vez firmado, Hacienda (en este caso se simula) validará que el comunicado haya sido firmado por el director. Para ello usará la misma función resumen sobre el comunicado y validará la firma utilizando la clave pública del director. Si todo es correcto, se imprimirá por pantalla que la firma ha sido validada.



```
Validando firma...
La firma es válida
```

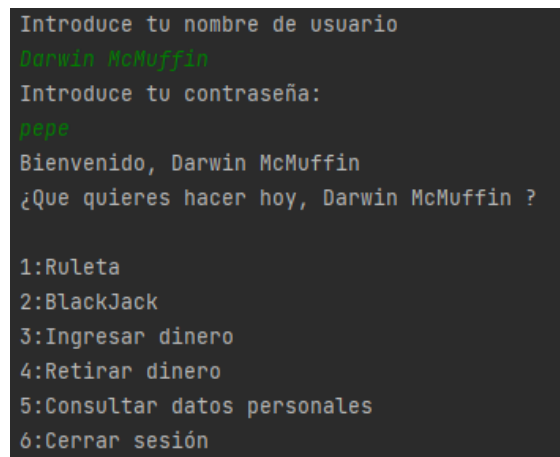
Imagen 10: Ejemplo de firma válida.

De esta forma aseguramos que los mensajes que se envían son enviados por el director de la aplicación, ya que su firma es única y ningún otro usuario puede replicarla.

En nuestra infraestructura de clave pública el director del casino sería un usuario Final (A), que recibe las claves por parte de una autoridad subordinada a una autoridad superior (AC2 y AC1). AC1 genera unas claves y AC2 recibe sus claves de AC1. A su vez, nuestro usuario final recibe sus claves de AC2, por lo que podemos decir que se generan las claves de forma jerárquica.

• **¿Qué tipo de autenticación ha implementado? ¿Por qué ha escogido este tipo y no otro?**
¿Cómo lo ha implementado?

En nuestra aplicación, hemos decidido utilizar nombre de usuario y contraseña para autenticar a los usuarios. Cada usuario tiene un nombre y una contraseña que se asigna él mismo cuando se registra. De esta forma, al iniciar sesión con ese nombre y esa contraseña se comprobará que dichos datos existan en la base de datos y en caso de existir se iniciará sesión.



```
Introduce tu nombre de usuario
Darwin McMuffin
Introduce tu contraseña:
pepe
Bienvenido, Darwin McMuffin
¿Que quieres hacer hoy, Darwin McMuffin ?

1:Ruleta
2:BlackJack
3:Ingresar dinero
4:Retirar dinero
5:Consultar datos personales
6:Cerrar sesión
```

Imagen 11: Inicio sesión del usuario

Hemos decidido escoger nombre de usuario y contraseña debido a que creemos que es la forma más común de autenticación y con la que los usuarios están más familiarizados. De este modo, nos aseguramos de que todos los usuarios entienden como registrarse e iniciar sesión correctamente y entrar en nuestra aplicación resulta sencillo y ameno. Además, este método es lo suficientemente seguro como para que no sea necesario utilizar otro aunque sea más seguro.

Como ya se ha indicado anteriormente, hemos implementado este sistema utilizando un formulario de registro y otro de inicio de sesión. En el formulario de registro se rellenan ciertos datos necesarios para iniciar sesión y otros que sirven tanto para validar al usuario y comprobar que es una persona real

como para asegurarnos de que no hay cuentas duplicadas. Una vez rellenado el formulario de registro, se añaden todos los datos del registro excepto la contraseña en el archivo `json_users.json` y el usuario y la contraseña al archivo `json_contraseñas.json`. Una vez creados estos archivos, se utiliza el algoritmo Hashlib SHA256 para generar un hash de la contraseña y eliminar la contraseña con el texto en claro. De esta forma nos aseguramos de que sea imposible que las contraseñas salgan a la luz desde nuestra base de datos ya que no se puede descifrar el hash.

```
{  
  "usuario": "Darwin McMuffin",  
  "contrasena": "7c9e7c1494b2684ab7c19d6aff737e460fa9e98d5a234da1310c97ddf5691834"  
}
```

Imagen 12: Hash de la contraseña del usuario

Cuando el usuario inicia sesión, se utiliza este mismo algoritmo para transformar a un hash la contraseña introducida por el usuario y se compara con el hash de la contraseña introducida en el registro. Si coinciden, significa que la contraseña introducida es correcta y se iniciará sesión.