**Gestión Financiera Personal**

**Grado en Ingería Informática de Gestión y Sistemas de Información**

**TRABAJO FIN DE GRADO**

**Anexo 1 – Teoria**



**Alumno:** Cuesta Alario, David

**Director: López Cuadrado, Javier**

**Curso: 2020 – 2021**

**Fecha: 2020-10-19**

**Índice de contenido**

[Sistemas de seguridad 1](#_Toc99796294)

[Métodos de Encriptación 1](#_Toc99796295)

[Validación de usuarios 1](#_Toc99796296)

[Bibliografía 2](#_Toc99796297)

[Tutoriales 2](#_Toc99796298)

[Referencias 2](#_Toc99796299)

[Titulo 1 4](#_Toc99796300)

[Titulo 2 4](#_Toc99796301)

[(Análisis) 4](#_Toc99796302)

[Titulo 3 4](#_Toc99796303)

**Índice de Ilustraciones**

Ejemplo de utilización de Charts.js 9

División de tareas – Parte 1 16

División de tareas – Parte 2 17

Estructura de Requisitos 20

Estimación de duraciones 21

Jerarquía de Actores 23

# Sistemas de seguridad

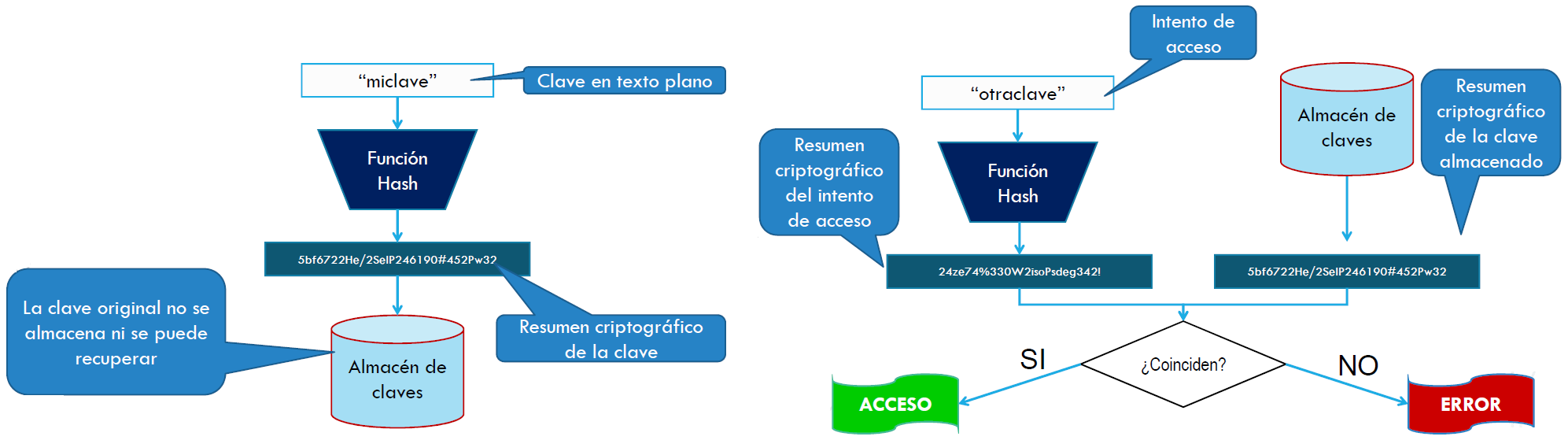
## Métodos de Encriptación

### Validación de usuarios

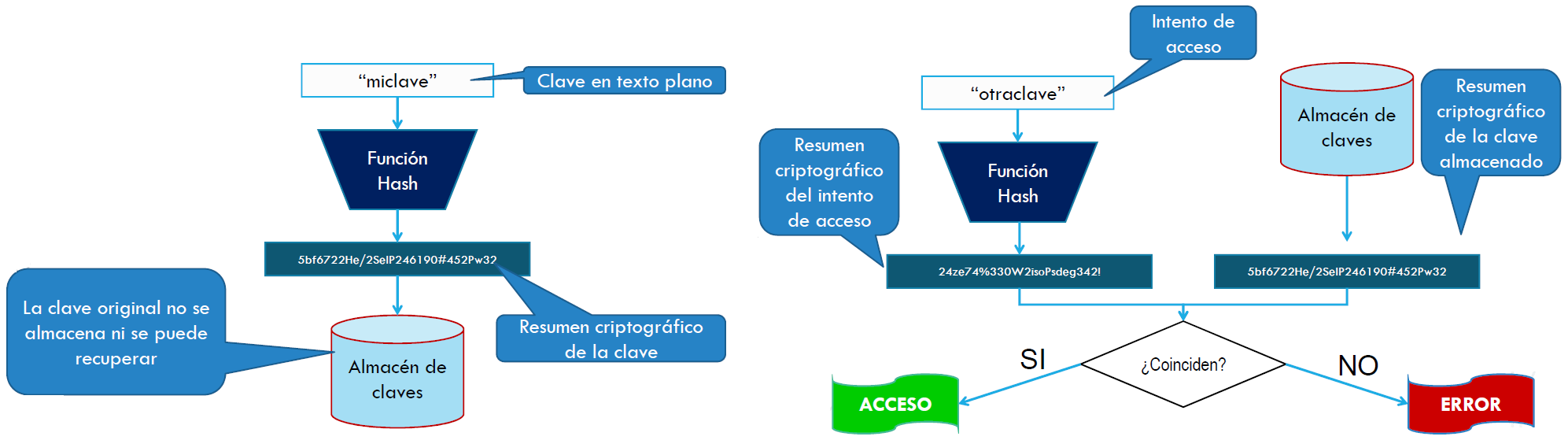
Uno de los principales problemas de la

Se pueden utilizar funciones hash para proporcionar una identificación de objetos o situaciones

* La evaluación de la función hash debería ser poco costosa para facilitar la rápida comparación de elementos candidatos a ser iguales y de esta forma poder implementar algoritmos de búsqueda rápidos.
* Es labor del diseño de la función hash capturar la esencia del criterio de igualdad. Una buena función hash debe asegurarse de que dos objetos o situaciones que se considerar iguales den lugar al mismo valor hash. No obstante, dos objetos pueden ser considerados iguales sin ser idénticos.



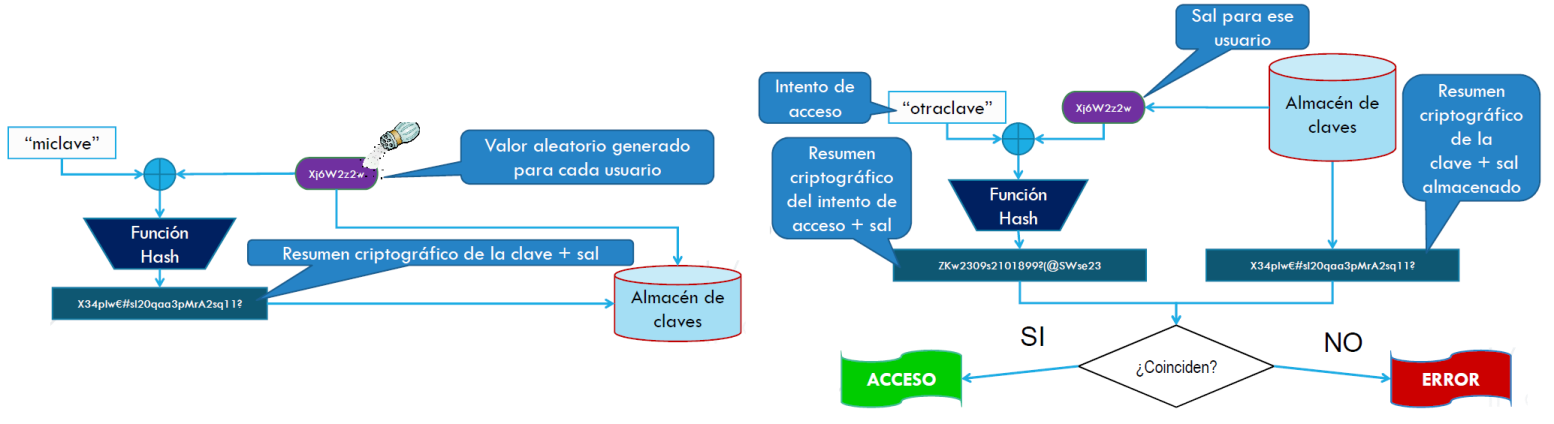
2 Almacenamiento de claves mediante Hash



2 identificación de claves mediante Hash

Problemas

* Todo el que utilice la misma clave tendrá el mismo hash
* Se pueden precalcular los hash de todo el espacio de claves si se dispone de la base de datos



Ventajas del uso de sal

* La misma clave tiene una codificación distinta cada vez
* Dificulta los ataques por fuerza bruta
* Tener disponible la base de datos las claves y la sal no aporta nada dado que no puedes saber a cual pertenece cada uno

# Bibliografía

Este apartado de la documentación está destinado a facilitar el entendimiento del resto del documento. De este modo se incluirán las definiciones de los términos clave para su correcto entendimiento, así como las referencias de las que se ha obtenido la información para su elaboración

## Tutoriales

Para alcanzar una correcta comprensión de aquellas herramientas con las que no estaba familiarizado antes de comenzar con la ejecución de este proyecto he recurrido a algunos tutoriales.

Aquellos que me han sido de mayor utilidad se recopilan a continuación:

|  |  |
| --- | --- |
| **Autor** | **Articulo** |
| [Luis Cabrera Benito](https://parzibyte.me/#contacto) | [Cifrado de MySQL con AES](https://parzibyte.me/blog/2019/06/01/cifrado-datos-mysql-aes/) |

## Referencias

Toda la información utilizada para redactar esta documentación ha sido extraída de las fuentes externas que se exponen a continuación:

|  |  |
| --- | --- |
| **Autor** | **Articulo** |
| Métodos de encriptación | Apuntes de la Asignatura Sistemas de seguridad |

# Titulo 1

## Titulo 2

Texto normal y corriente

## (Análisis)

Texto normal y corriente

### Titulo 3

Texto normal y corriente

#### Titulo 4

Texto normal y corriente

##### **Titulo 5**

Texto normal y corriente