¿Qué es el hasheo de contraseña?

El **hasheo de contraseña** es un proceso criptográfico que convierte una contraseña en una cadena de caracteres única e irreversible. A diferencia de la **encriptación**, que es reversible (se puede descifrar con la clave correcta), el **hashing** es unidireccional, lo que significa que una vez que una contraseña es convertida en un hash, no se puede recuperar su valor original.

¿Qué es bcrypt?

`bcrypt` es una librería diseñada para aplicar un **algoritmo de hash** que protege las contraseñas de manera segura. A diferencia de la encriptación reversible, el hashing es un proceso unidireccional, lo que significa que una vez que una contraseña se convierte en un hash, no se puede "desencriptar", solo verificar.

⚙ ¿Cómo funciona bcrypt?

1. **Generación de un "salt"** 🧂
    - Se genera un **salt** aleatorio, que es un conjunto de bytes extra añadidos a la contraseña antes de aplicar el hash.
    - Esto previene ataques basados en tablas precomputadas (rainbow tables).
2. **Aplicación del algoritmo de hashing** 🔄
    - bcrypt usa una versión mejorada de **Blowfish** para generar un hash seguro.
    - Se repite un número de veces (cost factor o "rounds"), lo que hace que el proceso sea más lento y dificulte ataques de fuerza bruta.
3. **Almacenamiento del hash** 📄
    - El resultado es una cadena que incluye el hash y el salt, almacenados en la base de datos.
4. **Verificación de contraseña** 🔑
    - Cuando un usuario intenta iniciar sesión, su contraseña se vuelve a hashear con el mismo salt y se compara con el hash almacenado.

Ventajas de usar bcrypt

✔ **Resistente a ataques de fuerza bruta** 🛡️
✔ **Usa salting para evitar ataques de diccionario**
✔ **Incrementa la seguridad con más iteraciones**

En resumen, bcrypt **no encripta** sino que **hashea** la contraseña, asegurando que incluso si los datos son filtrados, los atacantes no puedan obtener fácilmente las contraseñas originales.