

Hashing

Es un Proceso Criptográfico que toma una entrada (como un archivo, un mensaje o datos) y la transforma en una cadena de caracteres de longitud fija llamada **Hash** o "valor hash". Este hash es único para cada entrada y se calcula utilizando una función hash específica. El objetivo principal del hashing es garantizar la integridad y la verificación de datos. Incluso una pequeña modificación en la entrada resultaría en un hash diferente.

Además es prácticamente imposible reconstruir la entrada original a partir del hash, lo que lo hace útil para:

1 - Almacenar contraseñas de forma segura

2. Verificar la integridad de archivos

Realizar búsquedas eficientes en grandes conjuntos de datos.

Algoritmos de cifrado Hash

MD5

- Produce un valor hash de 128 bits
- Es rápido y ampliamente compatible
- Es considerado criptográficamente débil y vulnerable

Algoritmos de cifrado hash



MD5

- Produce un valor hash de 128 bits
- Es rápido y ampliamente compatible
- Es considerado criptográficamente débil y vulnerable a colisiones

RIPEMD

- Produce hash de 128 a 320 bits
- Es de código libre

SHA

- Distintas versiones pueden manejar hash de 128 hasta 512 bits
- El de 256 se considera seguro y es bastante estándar

HMAC

- Combina una función de hash como SHA-256, con una clave secreta para proporcionar autenticación y verificación de integridad de datos

