Hashing

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

Ademas es Practicamente imposible reconstruir la entrada original a partir del hash, lo que lo hace util para:

1 - Almacenar contraseñas de forma segura

2. Verificar la integridad de archivos

Realizar busquedas eficientes en grandes conjuntos de datos.

Algoritmos de cifrado Hash

MD5

- Produce un valor hash de 128 bits
- Es rapido y ampliamente compatible
- Es considerado Criptograficamente Debil vulnerable