**HASH**

Un hash en ciberseguridad se refiere a una función matemática que toma un conjunto de datos (como un archivo, contraseña o cualquier otro tipo de información) y produce una cadena de caracteres alfanuméricos de longitud fija, que representa de manera única los datos originales.

Los valores devueltos por una función hash se denominan **resumen de mensajes o simplemente valores hash.**

**Objetivos del hash**

* Integridad de datos
* Contraseñas seguras
* Almacenamiento seguro
* Verificación de descargas
* Firma digital

Entre los algoritmos hash mas habituales se pueden mencionar algunos como: MD5, SHA-1, SHA-256 y SHA-3.

**Características de hash**

* **Tamaño fijo:** un hash tiene una longitud fija y predefinida, independientemente del tamaño de los datos de entrada. Esto significa que el resultado del hash siempre tendrá la misma longitud, lo que facilita su almacenamiento y comparación.
* La función hash convierte datos de longitud arbitraria a una longitud fija. Este proceso a menudo se denomina **hash de los datos.**
* En general, el hash es mucho mas pequeño que los datos de entrada, por lo que las funciones has a veces se denominan funciones de compresión.
* Dado que un hash es una representación mas pequeña de datos más grandes, también se le conoce como resumen.
* La función hash con salida n de bits se denomina función hash de n bits. Las funciones mas populares generan valores entre 160 y 512.
* **Unidireccionalidad:** es computacionalmente difícil o prácticamente imposible calcular el conjunto de datos de entrada original a partir del valor de hash. En otras palabras, no puedes obtener los datos originales a partir del hash, lo que proporciona cierto nivel de seguridad, especialmente en el almacenamiento de contraseñas.
* Eficiencia de operación: generalmente, para cualquier función hash h con entrada x, el calculo de h(x) es una operación rápida.
* Las funciones de hash computacional son mucho más rápidas que un cifrado simétrico.
* **Resistencia a colisiones:** un buen algoritmo de hash debe ser resistente a colisiones, lo que significa que es computacionalmente difícil encontrar dos conjuntos de datos distintos que produzcan el mismo valor de hash. Esto es fundamental para garantizar la integridad de datos.
* **Cambios mínimos en los datos de entrada:**
* **Distribución uniforme:**
* **Resistencia a ataques criptográficos:**

**Funciones hash**

**Resumen de mensajes (MD)**

la familia MD se compone de funciones hash MD2, MD4, MD5 y MD6. Fue adoptado como estándar de internet RFC 1321. Es una función hash de 128 bits.

**Función de hash seguro (SHA)**

La familia de SHA se compone de cuatro algoritmos SHA, SHA-0, SHA-1, SHA-2, SHA,3.

* SHA-224 (224 bits)
* SHA-256 (256 bits)
* SHA-384 (384 bits)
* SHA-512 (512 bits)

Cabe mencionar que, dentro de los algoritmos de hash, y debido al aumento en el procesamiento y capacidad de calculo de los equipos actuales, la familia MD (principalmente MD5) ya no son tan seguros como antes, por lo que el uso de otros algoritmos de hash es recomendable.

**La técnica de Salting**

La técnica de salting se utiliza para hacer del hash una herramienta más segura.

Un salt, es una cadena aleatoria de caracteres, es una entrada adicional a la contraseña antes del hash.

**La técnica HMAC**

Un HMAC utiliza un algoritmo que combina una función de hash criptográfica con una clave secreta.