

INSTITUTO TECNOLÓGICO

SUPERIOR DE JEREZ

JEREZ, ZACATECAS

NOMBRE:

ADRIANA DE JESUS MARQUEZ MENDOZA

NÚMERO DE CONTROL:

S17070161

CORREO ELECTRONICO:

[marquez98709@gmail.com](mailto:marquez98709@gmail.com)

CARRERA:

INGENIERIA EN SISTEMAS COMPUTACIONALES

SEMESTRE:

Quinto Semestre

ACTIVIDAD:

Actividad 1 - Mapa Conceptual funciones hash

DOCENTE:

M.T.I, I.S.C. SALVADOR ACEVEDO SANDOVAL

MATERIA:

Estructura de Datos

Fecha:

29/11/2019

**1.- ¿Qué es una función HASH y para qué sirve?**

Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Es una estructura de datos que asocia llaves o claves con valores.

**2.- ¿Cuáles son las funciones HASH más utilizadas?**

* **Message-Digest algorithm** (MD; o en español, Algoritmo de resumen del mensaje).
* **MD5: de 128 bits. Muy** utilizado. Desaconsejado por cuestiones de seguridad. Se sigue utilizando para comprobar ficheros.
* **MD6: de 256 bit,** se procesa mediante multitarea. Nuevo algoritmo, recomendado para la seguridad.
* **Secure Hash Algorithm** (SHA; o en español, Algoritmo de Hash Seguro).
* **SHA-1: 160 bits**. Desaconsejado por cuestiones de seguridad. Se sigue utilizando para comprobar ficheros.
* **SHA-2:** de 256 bits (SHA-256) y 512 bits (SHA-512), existen otros. Muy utilizado, aunque desaconsejado por cuestiones de seguridad.
* **SHA-3:** de 256 bits (SHA3-256) y 512 bits (SHA3-512), existen otros. Nuevo algoritmo, recomendado para la seguridad.

**3.- ¿Qué aplicaciones reales tienen dichas funciones?**

El software que realiza los cálculos y las comprobaciones para estos, se denomina con el "nombre del algoritmo" terminado con prefijo "sum". Hay muchas aplicaciones que se pueden utilizar a nivel de usuario.

**4.- ¿Qué problemas se presentan al utilizarlas?**

Computacionalmente cara de ejecución, se han invertido muchos esfuerzos en el desarrollo de estrategias para la resolución de colisiones que mitiguen el mal rendimiento del hasheo. Sin embargo, ninguna de estas estrategias es tan efectiva como el desarrollo de una buena función hash de principio.

**5.- ¿Qué es una TABLA HASH y para qué sirve?**

Es una estructura de datos no lineal cuyo propósito final se centra en llevar a cabo las acciones básicas (inserción, eliminación y búsqueda de elementos) en el menor tiempo posible, mejorando las cotas de rendimiento respecto a un gran número de estructuras.

Pues sirve para clasificar los datos y poder acceder a ellos, buscar, ordenar o modificar de una forma mucho más óptima que haciéndolo de otro modo.

**6.- ¿Qué aplicaciones reales tienen dichas tablas?**

Confección de diccionarios, pues la facilidad de búsqueda hace que las palabras puedan ser encontradas en lapsos muy cortos.

# Referencias

*EcuRed*. (s.f.). Obtenido de EcuRed: https://www.ecured.cu/Tabla\_hash

*Google sites*. (s.f.). Obtenido de Google sites: https://sites.google.com/a/espe.edu.ec/programacion-ii/home/tablas-hash

*jarroba.com*. (3 de septiembre de 2016). Obtenido de jarroba.com: https://jarroba.com/tablas-hash-o-tabla-de-dispersion/

*jarroba.com*. (2 de marzo de 2016). Obtenido de jarroba.com: https://jarroba.com/codigo-hash/

*latam*. (9 de abril de 2014). Obtenido de latam: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/