**FUNSIONES HASH**

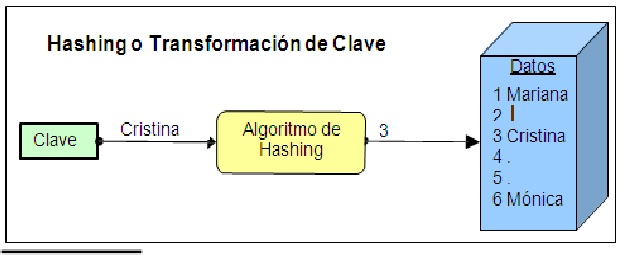
Una función criptográfica hash- usualmente conocida como “hash”- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

EJEMPLOS:

Método de dispersión (hashing)

Definición

Es un método que permite encontrar, con el mínimo esfuerzo, una clave dada dentro de un conjunto de elementos. También se denomina método de "transformación de claves", "direccionamiento calculado","direccionamiento asociativo" o de "dispersión".En la técnica de hashing se aplican cálculos o transformaciones aritméticas sobre la clave para producir directamente una dirección en una tabla o archivo de acceso directo. Por ejemplo:

[](http://2.bp.blogspot.com/-4dEmi3t6vGI/UTQlynkUUBI/AAAAAAAAAoU/ESdDxYgOgso/s1600/algoritmo+de+hashing.jpg)

**Conceptos de hashing**

***a) Clave:*** La clave contiene el valor que permite ubicar, mediante la función Hash, la posicionó registro que contiene el resto de información asociada. Normalmente la clave es el campo que identifica en forma única la información. Por ejemplo:

* Cédula de Identidad
* Registro de Información Fiscal
* Placa o Matrícula de Vehículo

***b) Función Hash:***Es un algoritmo o transformación que, aplicado a la clave, devuelve la posición del destino en donde podemos ubicar o recuperar el elemento que contiene dicha clave. Normalmente consta de tres partes:

1. **Transformación:** Si la clave no es numérica se convierte en un número. Con frecuencia se utiliza el valor ASCII de cada carácter y luego se aplican operaciones matemáticas para obtener un número entero.
2. **Generación:** El número generado se procesa con un algoritmo que trata de uniformizar la distribución de las claves en el rango de direcciones.
3. **Compresión:**Se comprime el número obtenido multiplicándolo por un factor para adecuarlo a la capacidad de almacenamiento disponible. La función Hash debe definirse al momento de diseñar el sistema y su selección tiene gran incidencia en rendimiento del sistema. Una buena función Hash debe tener las siguientes características:

En este método se requiere que los elementos estén ordenados.

El método consiste en asignar el índice a cada elemento mediante una transformación del elemento, esto se hace mediante una función de conversión llamada función hash. Hay diferentes funciones para transformar el elemento y el número obtenido es el índice del elemento.

La principal forma de transformar el elemento es asignarlo directamente, es decir al 0 le corresponde el índice 0, al 1 el 1, y así sucesivamente pero cuando los elementos son muy grandes se desperdicia mucho espacio ya que necesitamos arreglo grande para almacenarlos y estos quedan con muchos espacios libres, para utilizar mejor el espacio se utilizan funciones más complejas.

La función de hash ideal debería ser biyectiva, esto es, que a cada elemento le corresponda un índice, y que a cada índice le corresponda un elemento, pero no siempre es fácil encontrar esa función, e incluso a veces es inútil, ya que puedes no saber el número de elementos a almacenar. La función de hash depende de cada problema y de cada finalidad, y se pueden utilizar con números o cadenas, pero las más utilizadas son:

1.- Restas sucesivas:

Esta función se emplea con claves numéricas entre las que existen huecos de tamaño conocido, obteniéndose direcciones consecutivas. Un ejemplo serían los alumnos de ingeniería en sistemas que entraron en el año 2005 sus números de control son consecutivos y está definido el número de alumnos.

05210800 -05210800»» 0

05210801 -05210800»» 1

05210802 -05210800»» 2

…

05210899 -05210800»» 99

2.- Aritmética modular:

El índice de un número es resto de la división de ese número entre un número N prefijado, preferentemente primo. Los números se guardarán en las direcciones de memoria de 0 a N-1. Este método tiene el problema de que dos o más elementos pueden producir el mismo residuo y un índice puede ser señalado por varios elementos. A este fenómeno se le llama colisión. Si el número N es el 7, los números siguientes quedan transformados en:

1679 »> 6

4567 »> 3

8471 »> 1

0435 »> 1

5033 »> 0

Mientras más grande sea número de elementos es mejor escoger un número primo mayor para seccionar el arreglo en más partes. El número elegido da el número de partes en que se secciona el arreglo, y la cada sección está compuesta por todos los elementos que arrojen el mismo residuo, y mientras más pequeñas sean las secciones la búsqueda se agilizara mas que es lo que nos interesa.

3.- Mitad del cuadrado:

Consiste en elevar al cuadrado la clave y coger las cifras centrales. Este método también presenta problemas de colisión.

709^2=502681 –> 26

456^2=207936 –> 79

105^2=11025 –> 10

879^2=772641 –> 26

619^2=383161 –> 31

Nota: en caso de que la cifra resultante sea impar se toma el valor número y el anterior.

4.- Truncamiento:

Consiste en ignorar parte del número y utilizar los elementos restantes como índice. También se produce colisión. Por ejemplo, si un número de 7 cifras se debe ordenar en un arreglo de elementos, se pueden tomar el segundo, el cuarto y el sexto para formar un nuevo número:

5700931 »> 703

3498610 »> 481

0056241 »> 064

9134720 »> 142

5174829 »> 142

5.- Plegamiento:

Consiste en dividir el número en diferentes partes, y operar con ellas (normalmente con suma o multiplicación). También se produce colisión. Por ejemplo, si dividimos el número de 7 cifras en 2, 2 y 3 cifras y se suman, dará otro número de tres cifras (y si no, se toman las tres últimas cifras): 5700931 »> 57 + 00 + 931 = 988

3498610 »> 34 + 98 + 610 = 742

0056241 »> 00 + 56 + 241 = 297

9134720 »> 91 + 34 + 720 = 845

5174929 »> 51 + 74 + 929 = 105