Instituto Tecnológico Superior de Jerez

Actividad 1 - Mapa conceptual

Jerez de García Salinas

Fecha

26/11/2019

Alumno:

Mario Alberto Loya Rodríguez

Carrera:

Ingeniería en Sistemas Computacionales

Semestre 5

Materia:

Estructura de Datos

Tema:

6.- Métodos de búsqueda

No. de control:

16070135

Profesor:

ISC Salvador Acevedo Sandoval

Cuestionario

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

Las funciones Hash (también conocidas como funciones resumen) son funciones que, utilizando un algoritmo matemático para transformar un conjunto de datos en un código alfanumérico con una longitud fija. Da igual la cantidad de datos que se utilice (muchos o pocos), el código resultante tendrá siempre el mismo número de caracteres.

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

- DES(Unix)
  Ejemplo: IvS7aeT4NzQPM
  Utilizados en Linux y otras similares OS.
  Longitud: 13 caracteres.
  Descripción: Los dos primeros caracteres son la azar (caracteres aleatorios, en nuestro Ejemplos el azar es la cadena “IV”), luego sigue el hash actual.
- De dominio en caché de credenciales
  Ejemplo: Admin:b474d48cdfc4974d86ef4d24904cdd91
  Se utiliza para almacenar en caché las contraseñas de dominio de Windows.
  Longitud: 16 bytes.
  Algoritmo: MD4(MD4(Unicode($pass)).Unicode(strtolower($username)))
- MD5(Unix)
  Ejemplo: $1$12345678$XM4P3PrKBgKNnTaqG9P0T/
  Utilizados en Linux y otras similares OS.
  Longitud: 34 Caracteres
  Descripción: El hash comienza con la firma $ 1 $, entonces ahí va el azar (hasta 8 caracteres al azar, en nuestro Ejemplos En la sal es la cadena “12345678”), entonces ahí va uno más el carácter $, seguido por el hash actual.

Algoritmo: La verdad es que es un circuito llamado el algoritmo MD5 2000 veces.

- MD5(APR)
  Ejemplo: $apr1$12345678$auQSX8Mvzt.tdBi4y6Xgj.
  Utilizados en Linux y otras similares OS.
  Longitud: 37 caracteres
  Descripción: El hash comienza con la firma $ apr1 $, entonces ahí va la sal (hasta 8 caracteres al azar, en nuestro Ejemplos En la sal es la cadena “12345678”), entonces ahí va uno más el carácter $, seguido por el hash actual.
  Algoritmo: La verdad es que es un circuito llamado el algoritmo MD5 2000 veces.
- MD5(phpBB3)
  Ejemplo: H9123456785DAERgALpsri.D9z3ht120
  Usado en phpBB 3.x.x.(Foros)
  Longitud: 34 characters.
  Descripción: El hash comienza con la firma H $ $, entonces ahí va uno de los personajes (por lo general el número ‘9 ’), entonces ahí va la sal (8 caracteres al azar, en nuestro Ejemplos En la sal es la cadena “12345678”), seguido por el hash actual.
  Algoritmo: La verdad es que es un circuito llamado el algoritmo MD5 2048 veces.
- MD5(WordPress)
  Ejemplo: PB123456780BhGFYSlUqGyE6ErKErL01
  Usado en WordPress.
  Longitud: 34 characters.
  Descripción: El hash comienza con la firma $ P $, entonces ahí va uno de los personajes (más a menudo “B” el número), entonces ahí va la sal (8 caracteres al azar, en nuestro Ejemplos En la sal es la cadena “12345678”), seguido por el hash actual.

Algoritmo: La verdad es que es un circuito llamado el algoritmo MD5 8192 veces.

- MySQL
  Ejemplo: 606717496665bcba
  Usado en las versiones antiguas de MySQL
  Longitud: 8 bytes.
  Descripción: El hash se compone de dos DWORD, cada uno no exceda el valor de 0x7fffffff.
- MySQL5
  Ejemplo: *E6CC90B878B948C35E92B003C792C46C58C4AF40
  Usado en la versiones nuevas de MySQL5
  Longitud: 20 bytes.
  Algoritmo: SHA-1(SHA-1($pass))
  Nota: Los hashes se van a cargar en el programa sin el asterisco que se encuentra en el comienzo de cada hash.
- RAdmin v2.x
  Ejemplo: 5e32cceaafed5cc80866737dfb212d7f
  Used in the application Remote Administrator v2.x.
  Longitud: 16 bytes.
  Nota: La contraseña se rellena con ceros a la Longitud de 100 bytes, que se aloja toda la cadena con el algoritmo MD5.
- MD5
  Ejemplo: c4ca4238a0b923820dcc509a6f75849b
  Utilizados en v2.x phpBB, versión Joomla 1.0.13 a continuación y muchos otros foros y CMS.
  Longitud: 16 bytes.
  Algoritmo: Igual que la función md5 () en PHP.
- md5($pass.$salt)
  Ejemplo: 6f04f0d75f6870858bae14ac0b6d9f73:1234
  Utilizados en WB News, Joomla versión 1.0.13 y superiores.
  Longitud: 16 bytes.

- md5($salt.$pass)
  Ejemplo: f190ce9ac8445d249747cab7be43f7d5:12
  Utilizados en osCommerce, AEF, Galería y otros CMS.
  (osCommerce tenía una falla más grande..)
  Longitud: 16 bytes.
- md5(md5($pass))
  Ejemplo: 28c8edde3d61a0411511d3b1866f0636
  Utilizados en e107, DLE, AVE, Diferior, Koobi y otros CMS.
  Longitud: 16 bytes.
- md5(md5($pass).$salt)
  Ejemplo: 6011527690eddca23580955c216b1fd2:wQ6
  Utilizado en vBulletin, IceBB.
  Longitud: 16 bytes.
  Notes: [1] [3] [4]
- md5(md5($salt).md5($pass))
  Ejemplo: 81f87275dd805aa018df8befe09fe9f8:wH6_S
  Utilizados en IPB.
  Longitud: 16 bytes.
- md5(md5($salt).$pass)
  Ejemplo: 816a14db44578f516cbaef25bd8d8296:1234
  Usado en MyBB.
  Longitud: 16 bytes.
- md5($salt.$pass.$salt)
  Ejemplo: a3bc9e11fddf4fef4deea11e33668eab:1234
  Usado en TBDev.
  Longitud: 16 bytes.
- md5($salt.md5($salt.$pass))
  Ejemplo: 1d715e52285e5a6b546e442792652c8a:1234
  Usado en DLP.
  Longitud: 16 bytes.

- SHA-1
  Ejemplo: 356a192b7913b04c54574d18c28d46e6395428ab
  Se utiliza en muchos foros y CMS.
  Longitud: 20 bytes.
  Algoritmo: Igual que el sha1 () en PHP.
- sha1(strtolower($username).$pass)
  Ejemplo: Admin:6c7ca345f63f835cb353ff15bd6c5e052ec08e7a
  Utilizados en SMF.
  Longitud: 20 bytes.
- sha1($salt.sha1($salt.sha1($pass)))
  Ejemplo: cd37bfbf68d198d11d39a67158c0c9cddf34573b:1234
  Utilizados en WoltLab BB.
  Longitud: 20 bytes.
- SHA-256(Unix)
  Ejemplo:
  $5$12345678$jBWLgeYZbSvREnuBr5s3gp13vqiKSNK1rkTk9zYE1v0
  Utilizados en Linux y otras similares OS.
  Longitud: 55 characters.
  Descripción: El hash comienza con la firma de $ 5 $, entonces ahí va la sal (hasta 8 caracteres al azar, en nuestro Ejemplos En la sal es la cadena “12345678”), entonces ahí va uno más el carácter $, seguido por el hash actual.
  Algoritmo: La verdad es que es un circuito llamado el algoritmo SHA-256 5000 veces.
  Notes: [1] [2]
- SHA-512(Unix)
  Ejemplo:
  $6$12345678$U6Yv5E1lWn6mEESzKen42o6rbEmFNLlq6Ik9X3reMXY3doKEuxrcDohKUx0Oxf44aeTIxGEjssvtT1aKyZHjs
  Utilizados en Linux y otras similares OS.
  Longitud: 98 caracteres.

Descripción: El hash comienza con la firma de $ 6 $, entonces ahí va la sal (hasta 8 caracteres al azar, en nuestro Ejemplos En la sal es la cadena “12345678”), entonces ahí va uno más el carácter $, seguido por el hash actual.

Algoritmo: La verdad es que es un circuito llamado el algoritmo SHA-512 5000 veces.

3.- ¿Qué aplicaciones reales tienen dichas funciones?

- Detección de registros duplicados.
- Localización de puntos cercanos entre sí.
- Verificar la integridad de los mensajes.
- Verificación de contraseñas.
- Agilizar la recuperación de los registros de datos.
- Validación de los datos.
- Cifrado.

4.- ¿Qué problemas se presentan al utilizarlas?

- Necesidad de ampliar el espacio de la tabla si el volumen de datos almacenados crece. Se trata de una operación costosa.
- Dificultad para recorrer todos los elementos. Se suelen emplear listas para procesar la totalidad de los elementos.
- Desaprovechamiento de la memoria. Si se reserva espacio para todos los posibles elementos, se consume más memoria de la necesaria; se suele resolver reservando espacio únicamente para punteros a los elementos.

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

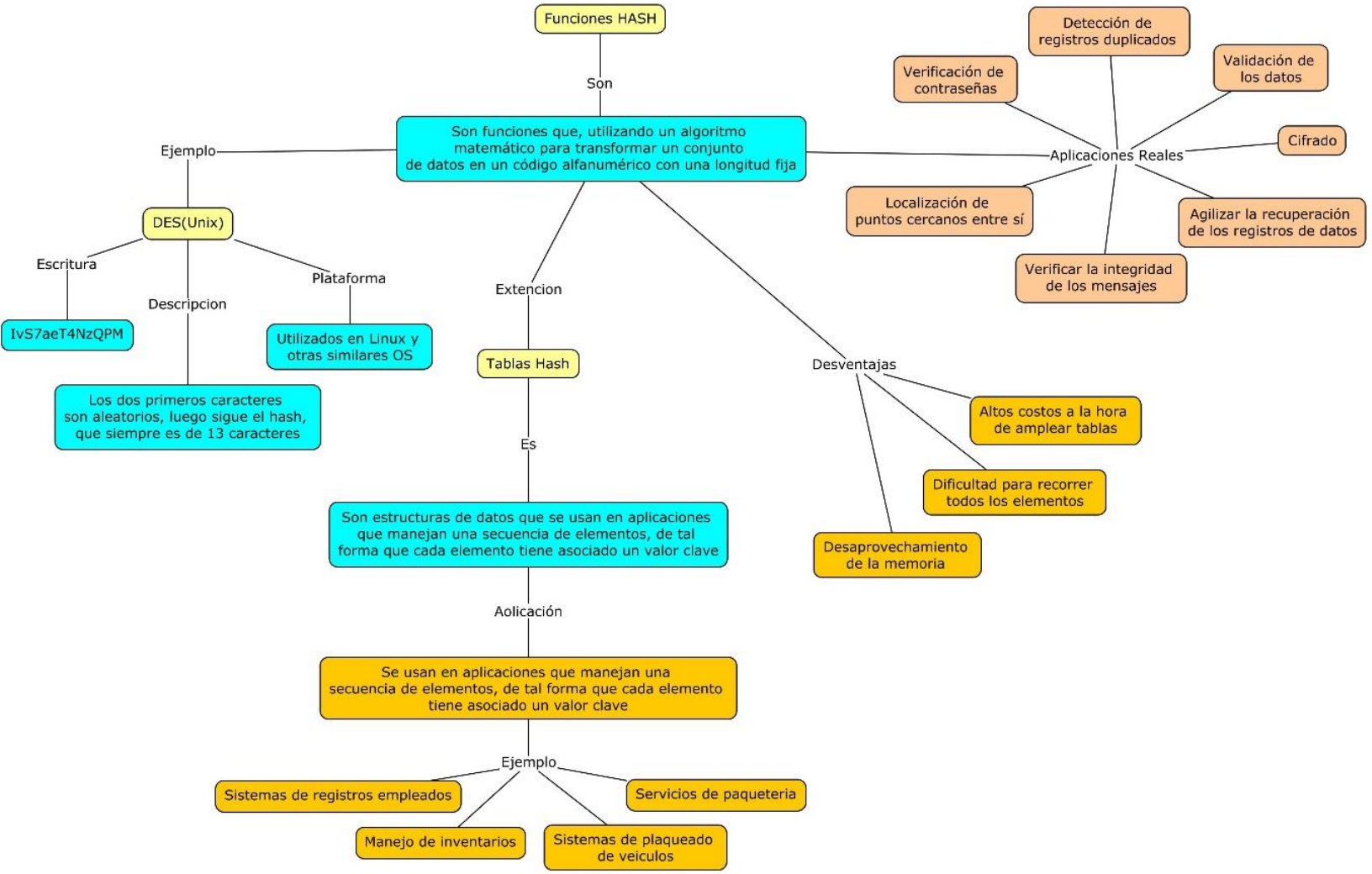
Son estructuras de datos que se usan en aplicaciones que manejan una secuencia de elementos, de tal forma que cada elemento tiene asociado un valor clave, que es un número entero positivo perteneciente a un rango de valores, relativamente pequeño. En estas organizaciones, cada uno de los elementos ha de tener una clave que identifica de manera unívoca al

elemento, tienen como finalidad realizar las operaciones fundamentales de búsqueda y eliminación de un registro en un tiempo de ejecución constante.

6.- ¿Qué aplicaciones reales tienen dichas tablas?

Se usan en aplicaciones que manejan una secuencia de elementos, de tal forma que cada elemento tiene asociado un valor clave, que es un número entero positivo perteneciente a un rango de valores, relativamente pequeño. En estas organizaciones, cada uno de los elementos ha de tener una clave que identifica de manera unívoca al elemento. Por ejemplo, el campo número de matrícula del conjunto de alumnos puede considerarse un campo clave para organizar la información relativa al alumnado de una universidad. El número de matrícula es único, hay una relación biunívoca, uno a uno, entre el campo y el registro alumno. Puede suponerse que no existen, simultáneamente, dos registros con el mismo número de matrícula.

Mapa Conceptual



Referencias

Aguilar, L. J. (2008). *Estructura de datos java.* Aravaca Madris: MCGRAW-HILL/INTERAMERICANA DE ESPAÑA, S. A. U.

G2K. (28 de 11 de 2019). *G2K conectados Siempre*. Obtenido de https://www.g2khosting.com/blog/tipos-de-hash/

IBM. (31 de 07 de 2013). *IBM KNOWLEDGE CENTER*. Obtenido de https://www.ibm.com/support/knowledgecenter/es/SSULQD_7.1.0/com.ibm.nz.sqltk.doc/c_sqlext_hashing.html

Valdecasas, G. G. (22 de 02 de 2018). *CYSAE*. Obtenido de https://www.cysae.com/funciones-hash-cadena-bloques-blockchain/