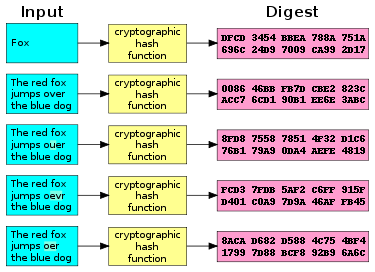
**FUNCIONES HASH**

Los **hash** o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

Estas funciones no tienen el mismo propósito que la criptografía simétrica y asimétrica, tiene varios cometidos, entre ellos está asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento.



**METODO DE DIVISIÓN**

La función de este método es dividir el valor de la llave entre un número apropiado, y después utilizar el residuo de la división como dirección relativa para el registro

**F(hash) = Llave % divisor.**

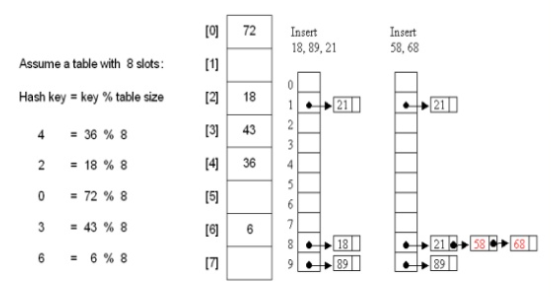
**Existen varios factores que deben considerarse para seleccionar el divisor:**

* **Divisor > n:** Suponiendo que solamente un registro puede ser almacenada en una dirección relativa dada.
* Seleccionarse el divisor de tal forma que la probabilidad de colisión sea mínima.



**Uso.**

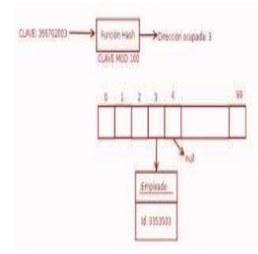
Cuándo la distribución de los valores de llaves no es conocida.



**Ejemplo:**

Si la tabla hash tiene tamaño m = 12 y la llave es k = 100, entonces

**h(k) = 100 mod 12 = 4**



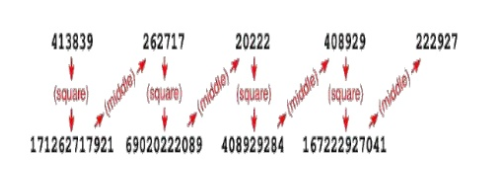
**METODO DE MEDIO CUADRADO**

Consiste en elevar al cuadrado la clave y tomar los dígitos centrales como dirección. El número de dígitos a tomar queda determinado por el rango del índice. Sea K la clave del dato a buscar, la función hash queda definida por la siguiente formula:

### H(K) = dígitos\_centrales (K^2) + 1

Las sumas de los dos dígitos centrales de la clave K (elevada al cuadrado) más 1, debe obtener un valor entre 1 y N (N, tamaño del arreglo)

**Uso:**

Puede aplicarse en archivos con factores de cargas bastantes bajas.

**Ejemplo:**

Sea N=100 al tamaño del arreglo.

Sea su dirección los números entre 1 y 100.

Sea K1 = 7259 una clave a la que se le debe asignar una posición en el arreglo.

**K1^2 = 52 693 081**

**H(K1) = (52 693 081) + 1 = 94**

 🡪 Colisión

**FUNCIÓN DE PLEGAMIENTO**

Se basa en dividir la clave en diferentes partes y la combinación de las partes es un modo conveniente usando a menudo suma o multiplicación para obtener el índice.

La clave se divide en varias partes **n1, n2, n3…nx,** donde cada parte tiene el mismo número de dígitos que la dirección especificada con la única posibilidad de excepción de la última parte.

**H(x) = n1 + n2 + n3 + … + x∞**

**Usos.**

* Búsquedas rápidas
* Control de archivos
* Asegurar la integridad de la información
* Firmas digitales
* Asegurar contraseñas

**Ejemplo:**

El número de identificación de los empleados es el campo clave de una empresa y consta de cuatro dígitos y las direcciones reales son 100. Se debe calcular las direcciones correspondientes por el método de plegamiento.

**Claves.**

* **2250**
* **1935**
* **3144**
* H(2250) = 22 + 50 = 72
* H(1935) = 19 + 35 = 54
* H(3144) = 31 + 44 = 75