**Análisis MD5**

MD5 es la quinta versión de MD (*Message Digest)*, la cual es una función matemática que toma como entrada un mensaje de longitud variable y a la salida arroja 128 bits que podría decirse que es un ‘resumen’ del mensaje de entrada. Esta función matemática cuenta con varias propiedades que la hacen muy útil.

* Es una función de una sola vía, es decir, a partir del resumen no es posible generar el mensaje original
* Hay un relación unívoca entre el mensaje original y el resumen
* No importa el tamaño del mensaje, la salida siempre será del mismo tamaño. 128 bits

Este algoritmo tiene como propósito validar la autenticidad e integridad de la información de un mensaje mediante una firma digital. Debido a que hay un relación unívoca, se puede a dar a conocer públicamente el resumen del mensaje que se quiere transmitir, para que de ésta manera las personas puedan verificar que la información es verídica y de una fuente confiable.

Este tipo de algoritmos son conocidos como *no reversibles,* ya que no es posible restaurar la información original a partir del resumen, por lo que lo hace seguro contra ataques donde se intente usar operaciones inversas. El proceso para generar se realiza en varios pasos.

1. Rellenar con bits

El mensaje de entrada es separado en bloques de 512 bits, en caso de que el último bloque tenga una longitud menor a 512 bits, éste se rellena con un bit ‘1’ seguido de todos los ‘0’s necesarios.

1. Agregar la longitud del mensaje

Después del proceso anterior, se agregan 64 bits al final, los cuales representan la longitud en bits del mensaje original. Este número es representado con 2 dígitos de 32 bits. Con lo anterior se logra que el mensaje tenga una longitud múltiplo de 512.

1. Inicialización de los parámetros MD5

Cuatro enteros de 32 bits, llamados variables de encadenamiento, se inicializan con valores hexadecimales.

1. Operaciones con bits

Se definen 4 funciones que operan con tres enteros de 32 bits, las cuales arrojaran valores independientes de acuerdo a las entradas

1. Transformación

Se realizan tanto ciclos como grupos de 512 bits se tengan después de los pasos anteriores. En cada ciclo de realizaran las operaciones del paso 4 con los bits de cada bloque y se van actualizando los valores de los parámetros del paso 3. Al final, la salida serán estos 4 parámetros concatenados en cascada.

A pesar de lo anterior, MD5 es susceptible a ataques con fuerza bruta, sin embargo, entre más grande sea el mensaje el ataque requerirá de un mayor costo computacional. Estos ataques van destinados a encontrar 2 mensajes con el mismo resumen o a partir de un resumen hallar el mensaje.

**Conclusión**

A pesar de tener bases matemáticas sólidas, MD5 es un algoritmo susceptible a ataques, por lo que no es confiable usarlo para garantizar confidencialidad en un mensaje. Es por eso que éste método es muy usado para firmas digitales, ya que su desempeño es muy bueno para garantizar la integridad de un mensaje.

Aún con esto, el algoritmo tiene brechas de seguridad significativas, sin embargo, el costo computacional de romper el algoritmo es elevado, el cual sólo puede ser costeado por grandes empresas o gobiernes que cuente con los recursos y equipo necesario para hacerlo.