Miramontes Sarabia Luis Enrique

Septiembre 10, 2019

Message Digest 5 (MD5)

Message Digest describe una función matemática que puede tomar una entrada de longitud variable y producir una salida de longitud fija, en caso de MD5, se produce una salida de 128-bits que es usada para firmas digitales. MD5 es el sucesor de MD4, es un algoritmo desarrollado por Ronald Rivest y el MIT Computer Science Laboratory en 1992, se publicó en forma de artículo para la Internet Engineering Task Force, el algoritmo hace uso de una serie de algoritmos no lineales para hacer operaciones circulares, para que en caso de ataque no se pueda restaurar los datos originales. En criptografía se le conoce como un algoritmo no reversible que puede prevenir efectivamente la fuga de datos causada por operaciones inversas.

El algoritmo consiste en dividir la entrada en bloques de 512-bits, cada bloque se divide otra vez en dieciséis bloques de 32-bits, después de usa serie de procesamiento se obtiene una salida de cuatro bloques de 32-bits, con estas salidas organizadas en cascada se aplica un algoritmo para generar un valor has de 128-bits. Cuando se necesita tener un padding se añade hasta que la longitud del bloque de 512-bits es congruente con 448 modulo 512 y consiste en un ‘1’ seguido de los necesarios ‘0’s.

MD5 necesita parámetros de inicialización, se ocupan cuatro parámetros hexadecimales con valores fijos, estos serán posteriormente usados en el procedimiento de transformación. Se tienen cuatro operaciones a nivel bit que consisten en NOT, AND, OR y XOR.

El proceso principal de transformación consiste en cuatro rondas, cada ronda consta de 16 operaciones y el número de veces que se realice este proceso será dependiente de la longitud de entrada. En el caso de 512-bits se realizarán 64 pasos. El procedimiento consiste en sumas utilizando las operaciones a nivel bit mencionadas anteriormente y desplazamientos a la izquierda

MD5 tiene colisiones, en 2010 se publicó una colisión single-block, consistía en dos mensajes de 64-bytes con el mismo hash MD5, por motivos de seguridad no anunciaron el tipo de ataque utilizado.

Miramontes Sarabia Luis Enrique

Como conclusión MD5 ya no es seguro cuando se quiere usarlo para firmas digitales o en procesos muy críticos de seguridad, el encontrar colisiones en mensajes de 64-bytes parece ser un problema bastante grande, ya que en 64 bytes ya puede entrar bastante información relevante, ya sea contraseñas, credenciales u otro dato relevante. Aunque quizá sigue siendo útil cuando es usado en archivos muy grandes, como sería un checksum de un archivo pesado para verificar que no haya sido alterado al momento de la transacción, ya sea de manera intencional o accidental. Aunque sea útil considero que es más sensible usar funciones hash más modernas, como es el caso de SHA.