ED\_T3\_ACT1: Función hash

Eduardo Martín-Sonseca

1. Que es una suma De comprobaciónes o check sum

Una suma de verificación o checksum, también conocida como suma de chequeo, es una función matemática de redundancia cuyo principal objetivo es el de detectar cambios malintencionados o accidentales en una transmisión de datos con el fin de proteger la integridad de la información.

1. ¿Qué es una función hash?

Una función criptográfica 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.

1. ¿Qué es MD5?

El MD5 (algoritmo de resumen de mensajes) es un protocolo criptográfico que se usa para autenticar mensajes y verificar el contenido y las firmas digitales. El MD5 se basa en una función hash que verifica que un archivo que ha enviado coincide con el que ha recibido la persona a la que se lo ha enviado. Anteriormente, MD5 se usaba para el cifrado de datos, pero ahora se utiliza principalmente para la autenticación.

1. ¿Y Sha?

Algoritmo de Hash Seguro o Secure Hash Algorithm (SHA) es una familia de funciones que sirve para generar códigos hash y que fue desarrollada por el Instituto Nacional de Estándares y Tecnología para tener un estándar federal de procesamiento de información en EE. UU. Una de las características principales de los algoritmos SHA es la no reflexividad.

* Utiliza la aplicación WinMD5, que calcula el valor resumen de un documento utilizando el algoritmo MD5.
  + Crea un documento prueba.txt con el contenido “El grupo de 1º DAM es muy simpático!!!”
  + Calcula su valor hash

7d5cb91a3d622b3fc3b119f4611e151a

* + Crea su archivo MD5
  + Modifica el documento
  + Comprueba con el MD5 que creaste ¿Qué ocurre?
* Utiliza la aplicación Hasher y calcula el valor resumen del mismo documento utilizando distintos algoritmos. ¿Coinciden los valores hash? ¿Por qué?

No coinciden ya que los algoritmos para hallar la cadena son distintos. Obviamente el MD5 del Hasher coincide con el anterior MD5.