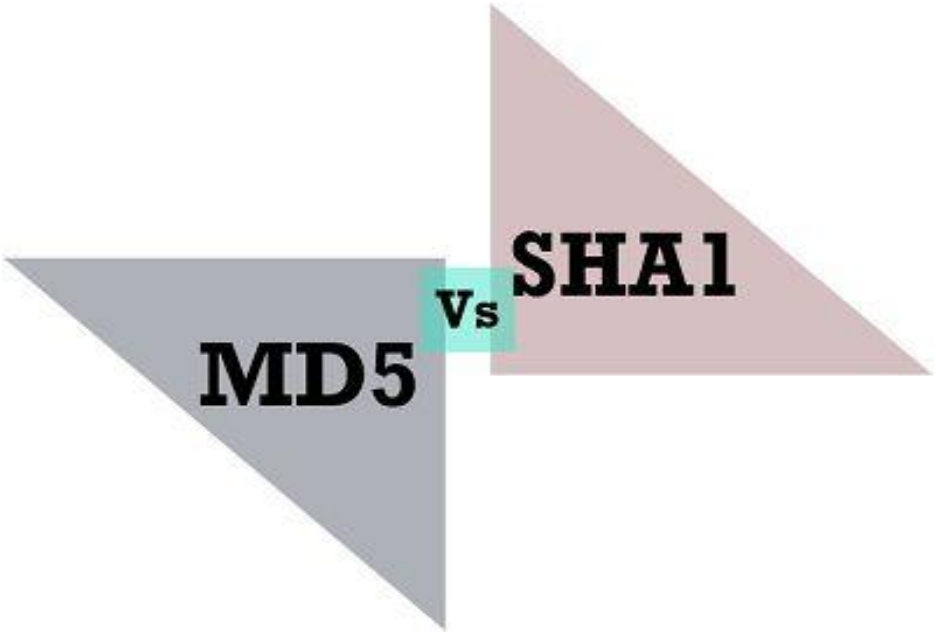


SHA | | MD5

Antonio Manuel Nuñez Campallo | ASIR | 21/01/25

Algoritmos SHA y MD5

Crea un fichero plano con extensión .txt y escribe en su interior el texto "Esto es una prueba". Usando la aplicación Cryptools, abre el fichero y ejecuta las opciones que se encuentran en Cifrar/Descifrar.

Se obtendrán dos ficheros cifrados, uno a través del algoritmo SHA y, otro, usando el al goritmo MD5. Analiza las diferencias más importantes que se puedan dar entre ambos.

SHA – 256

SHA-256 es un algoritmo de hash criptográfico que convierte cualquier mensaje en un valor fijo de 256 bits. Su propósito principal es garantizar la integridad de los datos.

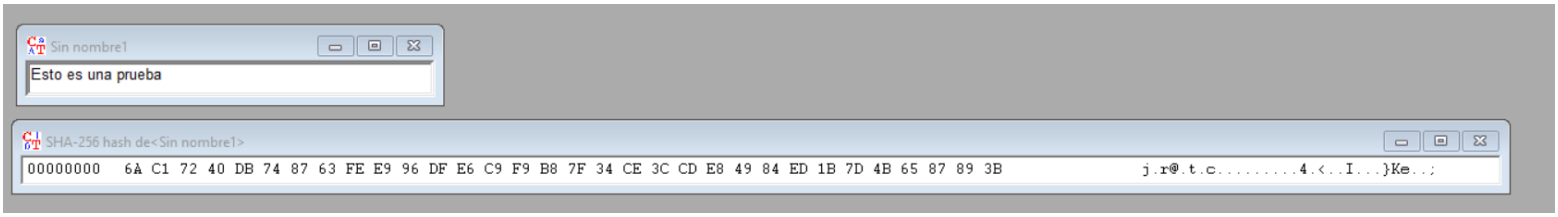
Pasos básicos:

1. **Preprocesamiento**: Se añade relleno al mensaje para que sea múltiplo de 512 bits, incluyendo su longitud original.
2. **División en bloques**: El mensaje se divide en bloques de 512 bits.
3. **Procesamiento**: Cada bloque pasa por 64 rondas de operaciones lógicas y matemáticas utilizando constantes y valores iniciales.
4. **Generación del hash**: Los valores intermedios se combinan para formar el hash final de 256 bits.

Características:

- Siempre produce el mismo hash para el mismo mensaje.
- Cambios mínimos en el mensaje generan hashes completamente diferentes.
- Es unidireccional y resistente a colisiones.

Se utiliza en seguridad, firmas digitales y blockchain.



MD5

MD5 es un algoritmo de hash que transforma cualquier mensaje en un resumen fijo de 128 bits. Se diseñó para verificar la integridad de los datos, pero es considerado inseguro hoy en día.

Pasos básicos:

1. **Preprocesamiento**: Se añade relleno al mensaje y su longitud en 64 bits.
2. **División**: Se divide el mensaje en bloques de 512 bits.
3. **Procesamiento**: Cada bloque pasa por 64 operaciones que actualizan cuatro valores iniciales (A, B, C, D).
4. **Resultado**: Los valores finales se concatenan para obtener el hash de 128 bits.

Características:

- Es rápido y produce siempre el mismo hash para el mismo mensaje.
- Es vulnerable a colisiones, por lo que no se recomienda para usos criptográficos.