Proyecto CLCript
Cuadernos de Laboratorio de Criptografía. Entrega nº 2. Ultima actualización 06/05/19
Autor: Dr. Jorge Ramió Aguirre (@criptored)
Prácticas con algoritmos MD5 y SHA-1: relleno y endianess

- Software CriptoRes: http://www.criptored.upm.es/software/sw_m001h.htm
- Lectura de interés: https://en.wikipedia.org/wiki/Endianness
- Lectura de interés: https://en.wikipedia.org/wiki/Padding_(cryptography)
- Tablas y códigos: http://www.criptored.upm.es/descarga/Codigos_y_tablas_de_uso_frecuente_en_criptografia.pdf

Objetivos:
1. Observar cómo almacena la información en formato little endian la función hash MD5.
2. Observar cómo almacena la información en formato big endian la función hash SHA-1.
3. Observar cómo se indica el relleno y el tamaño del archivo en los hashes MD5 y SHA-1.

I. MD5: sistema little endian, relleno y tamaño archivo

Ejercicio 1)

1.1. Con el software CriptoRes, en modo "Seguimiento del algoritmo MD5" (lupa) y con seguimiento a "Nivel de Pasos", obtén el hash MD5 de este mensaje de 31 bytes: Hola, buenos días. ¿Cómo estás?

1.2. Comprueba la escritura en formato little endian de MD5 leyendo los bytes que aparecen en código hexadecimal (usa la tabla de códigos ASCII).

1.3. Marca el inicio del relleno (primer byte) que se ha usado en el cálculo del hash e indica cuántos bits y cuántos bytes son.

1.4. Marca las palabras que entregan el tamaño del archivo (o texto) y comprueba que el valor en hexadecimal indicado es la cantidad de bits en decimal del mensaje.

1.5. ¿Crees que es suficiente dejar 64 bits para el tamaño del archivo? Busca en Internet la cantidad de información que maneja Google o bien que se genera mundialmente.

1.6. Haz un esquema donde se indiquen los bytes del mensaje, los bytes usados para el relleno y los bytes reservados para el tamaño del archivo. Comprueba que la suma de ellos corresponde al tamaño de bloque que usa esta función hash.

1.7. ¿Por qué en la ventana de Datos Estadísticos al hacer el hash se nos indica que se han procesado 64 bytes?

Observación 1. El software CriptoRes entrega resúmenes correctos para archivos grandes de hasta una centena de MBytes.

Observación 2. Como en el seguimiento a "Nivel de Pasos" la información mostrada en binario ocupa mucho espacio (compruébalo), CriptoRes solamente muestra ese cálculo para el primer bloque. Es decir, el hash que muestra va a coincidir con el hash del archivo o texto de entrada, solamente si este último tiene como máximo un bloque. Por este motivo, como MD5 y SHA1 operan sobre bloques de 512 bits, para poder observar el relleno así como la indicación del tamaño del archivo de entrada, que sabemos éstos siempre estarán en el último bloque del hash, con CriptoRes sólo puede observarse con un mensaje que tenga como máximo 448 bits (512-64). Por este motivo, en este ejercicio se hace el seguimiento del hash MD5 y SHA-1 de un mensaje de 31 bytes, es decir 248 bits.

Observación 3. Por el mismo motivo, el seguimiento a "Nivel de Bloques" sólo se podrá realizar a archivos de hasta 10 KBytes, unos 150 bloques.

Comprueba tu trabajo:

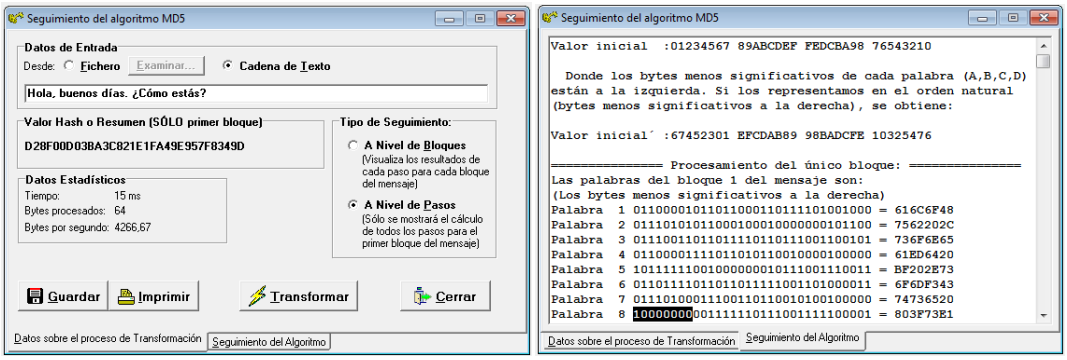

Figura 1. Seguimiento del hash MD5: inicio del relleno.

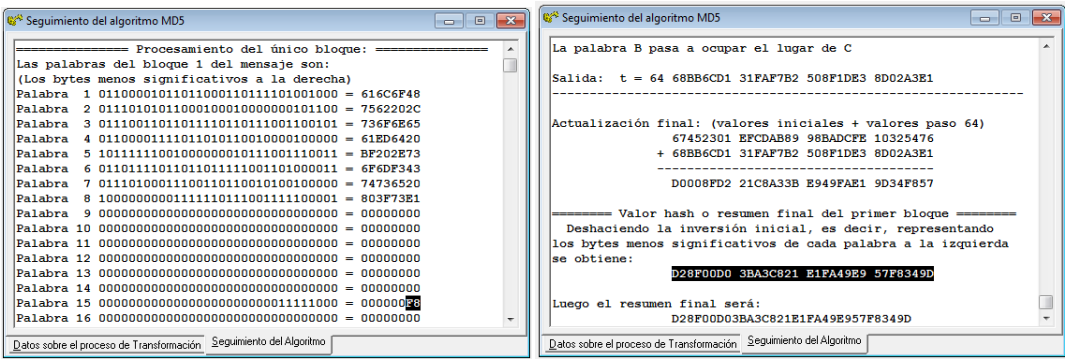

Figura 2. Seguimiento del hash MD5: tamaño del archivo.

II. SHA-1: sistema big endian, relleno y tamaño archivo

Ejercicio 2)

2.1. Repite la práctica anterior, calculando ahora el hash SHA-1 del mensaje y realizando su seguimiento.

Hola, buenos días. ¿Cómo estás?

Comprueba tu trabajo:

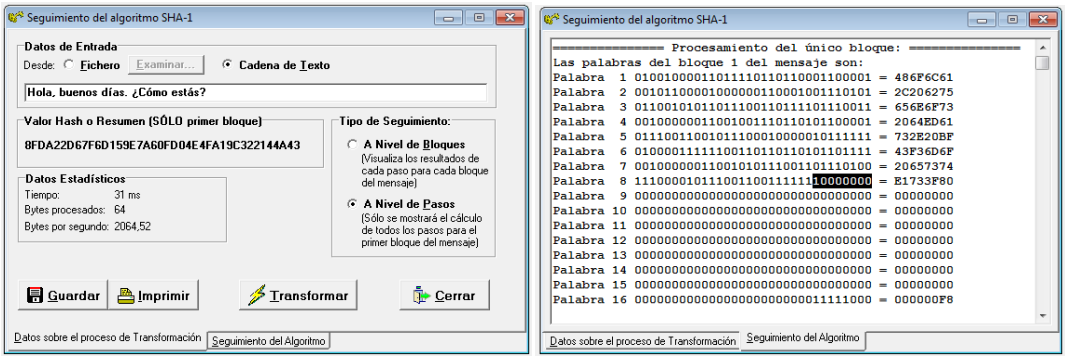

Figura 3. Seguimiento del hash SHA-1: inicio del relleno.

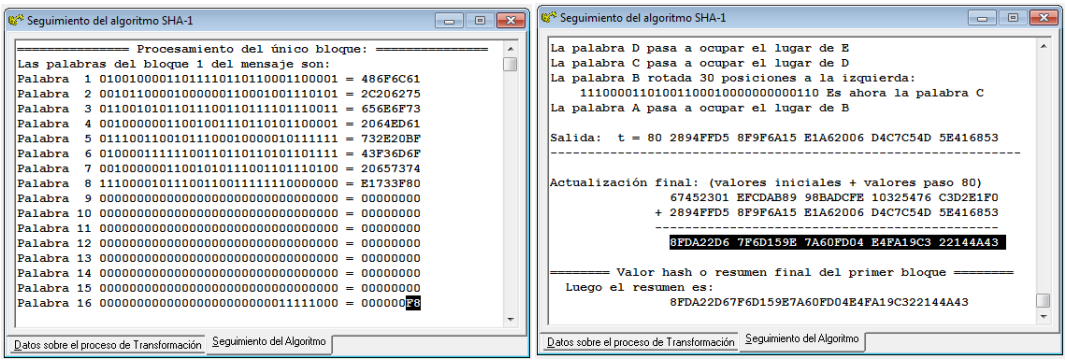

Figura 4. Seguimiento del hash SHA-1: tamaño del archivo.

Puedes utilizar esta documentación, otros libros, material multimedia y software de prácticas generados en Criptored, todos de libre distribución en Internet, para poder demostrar que entiendes y sabes cómo trabaja la criptografía, logrando la nueva certificación técnica profesional CriptoCert Certified Crypto Analyst, reconocida por el Centro Criptológico Nacional CCN de España, disponible desde el mes de abril de 2019.

Encontrarás más información sobre esta certificación y correo de contacto en el sitio web: https://www.criptocert.com

Madrid, 6 de mayo de 2019
Dr. Jorge Ramió Aguirre