- FUNCIONES HASH

I. Complete el enunciado con las siguientes Herramientas:

- Software REMAKE CriptoRes o Software SAMCript. Editor Hexed.it: https://hexed.it/

I. MD5: sistema little endian, relleno y tamaño archivo Ejercicio 1)

1.1. Usando el botón de generación de resumen, encuentre el hash MD5 del mensaje M = Hola. Para el mismo mensaje, repita el resumen para SHA-1, SHA-256 y SHA-512.

1.2. Busque en su computador el archivo RemakeCriptoRes, encuentre el hash MD5, el hash SHA-1, SHA-256 y SHA-512. Repita un par de veces la operación de resumen y compare la velocidad de cálculo de cada función.

1.3. Obtenga la función hash MD5 de M = Prueba 122 del hash. Abra otra ventana y encuentre ahora el hash de M = Prueba 123 del hash. Observe que los mensajes difieren sólo en un bit (2 = 0011 0010; 3 = 0011 0011).

1.4. Abra la calculadora de Windows dos veces y copie el hexadecimal de cada hash en cada una, cambie luego a binario. Haga un XOR entre los dos valores y compruebe que con cambiar sólo un bit del mensaje, el hash cambia más de la mitad de bits. Recuerde que estas calculadoras trabajan con 64 bits. Asegúrese que ambos valores tengan el mismo número de bits.

1.5. Para el mensaje M = 123, encuentre el hash MD5 a través del botón de seguimiento. Abra la pestaña del seguimiento del algoritmo y observe que se ha operado con un solo bloque.

1.6. Active la opción A Nivel de Pasos y vuelva a calcular el hash. Observe los valores 313233 (hexadecimal de 123) y luego el valor 80 que significa un relleno (1 seguido de ceros). Al final verá un bloque de 64 bits (últimas dos palabras) cuyo valor es 18. Con la calculadora de Windows compruebe que ese valor en decimal corresponde a 24, los 3 bytes del mensaje.

1.7. Observe ahora el relleno y el número de bits para el hash MD5 del mensaje M = En este caso tenemos 232 bits. Compruebe este valor.

1.8. Si el mensaje tiene exactamente 512 bits, siempre se incluye un bloque con relleno. Compruébelo con el mensaje de 64 bytes M = Y en este caso habrá siempre un bloque extra como ya se ha dicho. Recuerde: h = 68 y o = 6F. Observe que a nivel de pasos no se ve relleno (se muestra sólo el primer bloque) y que a nivel de bloques muestra el procesamiento de dos bloques.

1.9. Compruebe gráficamente la paradoja del cumpleaños pinchando en el icono con figura de tarta. Primero indique 5 iteraciones y acepte las opciones por defecto de un seguimiento preciso de cada cumpleaños. A continuación introduzca otros números, juegue un poco con las opciones del programa y observe que el valor medio de intentos es cercano a 23

1.10. Con el software RemakeCriptoRes, 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?

Comprueba tu trabajo:

```
Valor inicial  :01234567 89ABCDEF FEDCBA98 76543210

  Donde los bytes menos significativos de cada palabra (A,B,C,D)
están a la izquierda. Si los representamos en el orden natural
(bytes menos significativos a la derecha), se obtiene:

Valor inicial´ :67452301 EFCDAB89 98BADCFE 10325476

================ Procesamiento del único bloque: ================
Las palabras del bloque 1 del mensaje son:
(Los bytes menos significativos a la derecha)
Palabra  1 01100001011011000110111101001000 = 616C6F48
Palabra  2 01110101011000100010000000101100 = 7562202C
Palabra  3 01110011011011110110111001100101 = 736F6E65
Palabra  4 01100001111011010110010000100000 = 61ED6420
Palabra  5 10111111001000000010111001110011 = BF202E73
Palabra  6 01101111011011011111001101000011 = 6F6DF343
Palabra  7 01110100011100110110010100100000 = 74736520
Palabra  8 10000000001111110111001111100001 = 803F73E1
```

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

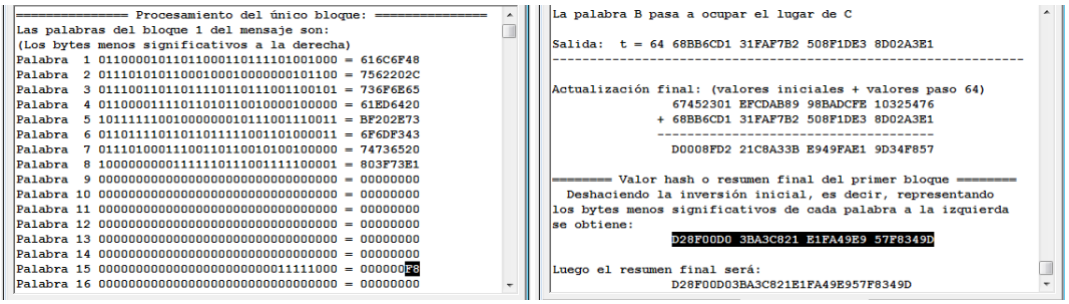

Figura 2. Seguimiento del hash MD5: tamaño del archivo.

SHA-1: sistema big endian, relleno y tamaño archivo ejercicio 2

2.1. Repite la práctica anterior, calculando ahora el hash SHA-1 SHA-256 y SHA-512del mensaje y realizando su seguimiento.

M Hola, buenos días. ¿Cómo estás?

Comprueba tu trabajo:

```
================ Procesamiento del único bloque: ================
Las palabras del bloque 1 del mensaje son:
Palabra  1 01001000011011110110110001100001 = 486F6C61
Palabra  2 00101100001000000110001001110101 = 2C206275
Palabra  3 01100101011011100110111101110011 = 656E6F73
Palabra  4 00100000011001001110110101100001 = 2064ED61
Palabra  5 01110011001011100010000010111111 = 732E20BF
Palabra  6 01000011111100110110110101101111 = 43F36D6F
Palabra  7 00100000011001010111001101110100 = 20657374
Palabra  8 11100001011100110011111110000000 = E1733F80
Palabra  9 00000000000000000000000000000000 = 00000000
Palabra 10 00000000000000000000000000000000 = 00000000
Palabra 11 00000000000000000000000000000000 = 00000000
Palabra 12 00000000000000000000000000000000 = 00000000
Palabra 13 00000000000000000000000000000000 = 00000000
Palabra 14 00000000000000000000000000000000 = 00000000
Palabra 15 00000000000000000000000000000000 = 00000000
Palabra 16 00000000000000000000000011111000 = 000000F8
```

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

```
================ Procesamiento del único bloque: ================
Las palabras del bloque 1 del mensaje son:
Palabra  1 01001000011011110110110001100001 = 486F6C61
Palabra  2 00101100001000000110001001110101 = 2C206275
Palabra  3 01100101011011100110111101110011 = 656E6F73
Palabra  4 00100000011001001110110101100001 = 2064ED61
Palabra  5 01110011001011100010000010111111 = 732E20BF
Palabra  6 01000011111100110110110101101111 = 43F36D6F
Palabra  7 00100000011001010111001101110100 = 20657374
Palabra  8 11100001011100110011111110000000 = E1733F80
Palabra  9 00000000000000000000000000000000 = 00000000
Palabra 10 00000000000000000000000000000000 = 00000000
Palabra 11 00000000000000000000000000000000 = 00000000
Palabra 12 00000000000000000000000000000000 = 00000000
Palabra 13 00000000000000000000000000000000 = 00000000
Palabra 14 00000000000000000000000000000000 = 00000000
Palabra 15 00000000000000000000000000000000 = 00000000
Palabra 16 00000000000000000000000011111000 = 000000F8

La palabra D pasa a ocupar el lugar de E
La palabra C pasa a ocupar el lugar de D
La palabra B rotada 30 posiciones a la izquierda:
    11100001101001100010000000000110 Es ahora la palabra C
La palabra A pasa a ocupar el lugar de B

Salida:  t = 80 2894FFD5 8F9F6A15 E1A62006 D4C7C54D 5E416853
----------------------------------------------------------------

Actualización final: (valores iniciales + valores paso 80)
                67452301 EFCDAB89 98BADCFE 10325476 C3D2E1F0
              + 2894FFD5 8F9F6A15 E1A62006 D4C7C54D 5E416853
              ----------------------------------------
                8FDA22D6 7F6D159E 7A60FD04 E4FA19C3 22144A43

======== Valor hash o resumen final del primer bloque ========
  Luego el resumen es:
                8FDA22D67F6D159E7A60FD04E4FA19C322144A43
```

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

2.2 Para el mensaje M = 123, encuentre ahora el hash SHA-1 a través del botón de seguimiento. Abra la pestaña del seguimiento del algoritmo y observe que se ha operado con un solo bloque. Observe el vector ABCDE.

2.3 Active la opción A Nivel de Pasos y vuelva a calcular el hash. Compare la representación del valor 123 en hexadecimal (313233) con el resultado de MD5, notación little-endian versus big-endian.

2.4 Observe que en SHA-1 no se reservan los últimos 64 bits para indicar el tamaño del archivo.

2.5 SHA-1 no acepta mensajes de tamaño mayores que 264 bits. Aunque pudiera parecer una limitación, ¿a cuántos bytes correspondería este valor?