Códigos y criptografía: Curso 2021-2022

Práctica 7: Función hash, MD5

En la práctica debéis implementar un programa que obtenga el MD5 de cualquier mensaje que se solicite.

Para poder implementar el código se proporciona un esqueleto del programa junto con alguna indicación que pudiera ser de ayuda. No es necesario seguir una a una todas las indicaciones. Si consideráis que hay una vía alternativa en alguna fase del código podéis aplicarla.

Dada la dificultad y el número de rondas que se ejecutan, no parece funcional proporcionar un ejemplo que nos indique paso a paso las salidas que debemos obtener. No obstante, existen calculadoras virtuales de código MD5 que nos van a permitir comprobar si el resultado final es válido y os proporciono aquí algunos ejemplos en los que se muestra como un paso intermedio como queda el mensaje en bytes tras su preparación (es decir, al añadirle el 1, los 0's necesarios y los 64 bits que representan la longitud del mensaje).

Ejemplos:

```
>> md5

Introduce the message:
'alma'

message =
[1634561121  128  0  0  0  0  0  0  0  0  0  0  0  0  32  0]

md5 =
'ebbc3c26a34b609dc46f5c3378f96e08'
```

```
>> md5

Introduce the message:
'clase'

message =
[1935764579  32869  0  0  0  0  0  0  0  0  0  0  0  0  40  0]

md5 =
'a788e21b2906dfdac17a8792dcd6fae2'
```

```
>> md5

Introduce the message:
'En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho ...
    tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, ...
    rocín flaco y galgo corredor.'

message =
Columns 1 through 5
1965059653   1970020462   544366951   1814062436   1632444513

Columns 6 through 10
1634231150   1701060652   2037736224   1869488239   1701995117

Columns 11 through 15
544173600   1701410161   1629515634   1685221219   1701671521

Columns 16 through 20
1869488172   543254560   1751348589   1769218159   1869639013

Columns 21 through 25
1702195488   1986623008   1965056493   1768431726   1735156068

Columns 26 through 30
1701060719   1936682016   543515680   2054054252   1852121185

Columns 31 through 35
1953718560   1701604457   539783026   1918985313   1629512039

Columns 36 through 40
1734964334   539779445   3982716786   1818632302   544170849

Columns 41 through 45
1634148473   544171884   1920102243   1919902821   32814

Columns 46 through 48
0   1416   0

md5 =
'5060f6cce9c0aa9645c28c55dc318312'
```