




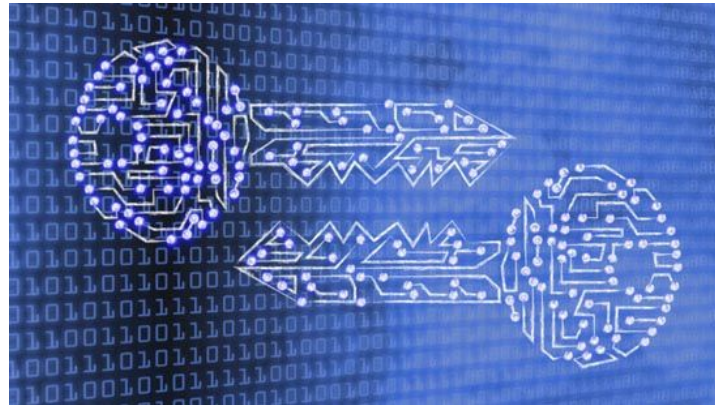
0800fc577294c34e0b28ad2839435945

(Hash)  
Hernández Alejandro  
Ramírez Simón



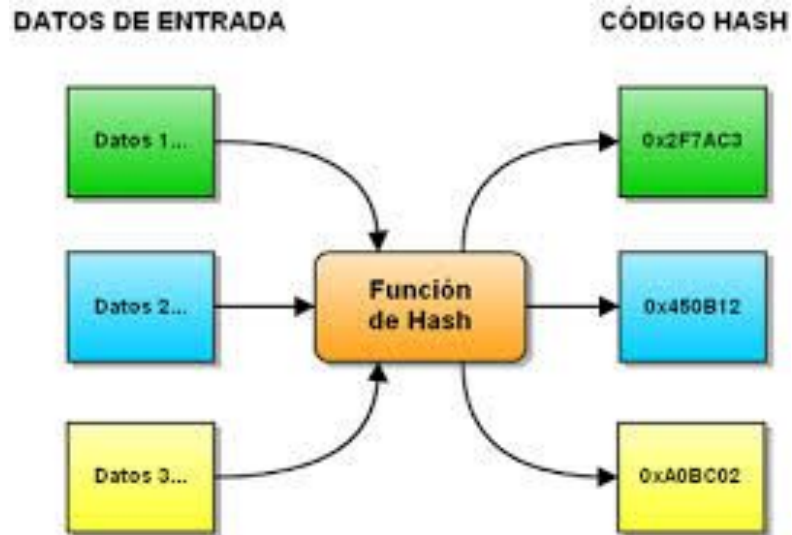
## CRIPTOGRAFÍA

La criptografía es la disciplina que se encarga del estudio de códigos secretos o llamados también códigos cifrados (en griego kriptos significa secreto y gráhos, escritura).



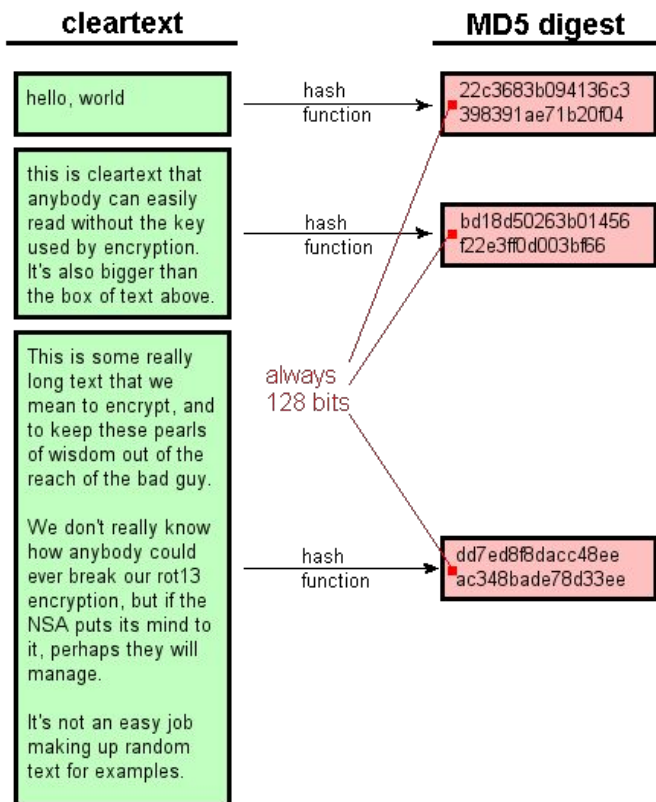
## HASH

Una Hash es una función que mapea (resume) una cadena de datos en una salida con una longitud fija.



## Propiedades

- Unidireccional
- Comportamiento aparentemente aleatorio
- Resistente a Colisiones  
(Paradoja de cumpleaños)



Paradoja de cumpleaños

23 personas - 50% de que dos cumplan años el mismo día

-Hash ( mensaje verdadero)=Hash ( mensaje falso)

Un hash es de 64 bits tendría  $2^{64}$  posibles valores, pero bastaría generar  $2^{32}$  para que apareciera uno que cumpliera con la condición anterior.

Un hash de 128 bits ( MD5) implica hacer  $2^{64}$  mensajes, pero hash de 160 bits implica  $2^{80}$  (por ahora fuera de el rango posible por simple aplicación del LPC).

$$P = 1 - \left(1 - \frac{1}{365}\right)^{\frac{n(n-1)}{2}}$$



# Ejemplos:

0cc175b9c0f1b6a831c399e269772661

→ a

fc3ff98e8c6a0d3087d515c0473f8677

→ hello world!


86fb269d190d2c85f6e0468ceca42a20

→ Hello world!



f6d5fcec889c01f3ec9fbcf6680e985e

0f89a4876f24d165c621fcde2f777e4e

→ 

5addaa1f23ff8d855655bb20cf324046

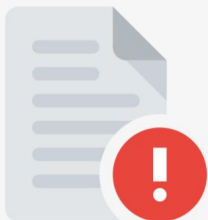
→ `^~@ ♀ ☺ ☹ ♥ ♦ ♣ ♠ ◻ ◻ ◻ ◻ ♂ ♀ 🎵 🎵 ☀ ▶ ◀ ⬆ ⬆ !!



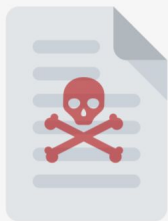
Good doc



SHA-1



3713..42



Bad doc



SHA-1



3713..42

Collision - **same** hashes

## Potentially Impacted Systems



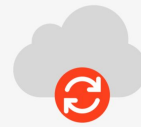
Document  
signature



HTTPS  
certificate



Version  
control (git)



Backup  
System

# ¿Cómo funciona?

El MD5 es un algoritmo de codificación de 128 bits que genera un hash hexadecimal de 32 caracteres, independientemente de la longitud de la palabra de entrada. Este algoritmo no es reversible, siendo normalmente imposible encontrar la palabra original a partir de un MD5. Nuestra herramienta emplea una amplia base de datos con el fin de aumentar al máximo las posibilidades de encontrar la palabra inicial. ¡No tiene más que introducir el MD5 que desee testar en el formulario de arriba para probar el descodificador!

Palabras de la base de datos : 1,139,689,399,522



# Descifrar un MD5

Introduzca su MD5 y cruce los dedos :

fc3ff98e8c6a0d3087d515c0473f8677|

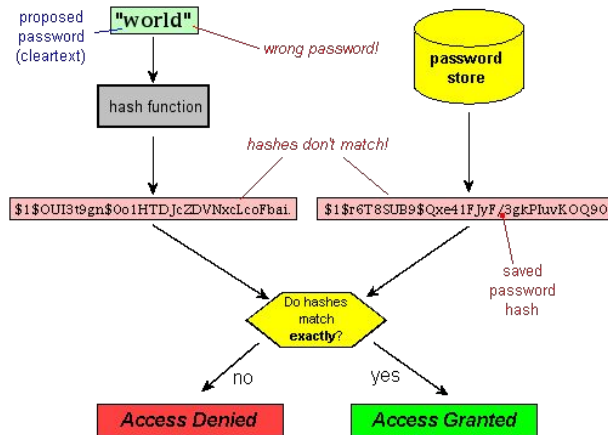
Descifrar

**Encontrado : hello world!**

(hash = fc3ff98e8c6a0d3087d515c0473f8677)

## Aplicaciones

- Verificación de la integridad de un archivo.
- Contraseña hash
- Firmas digitales



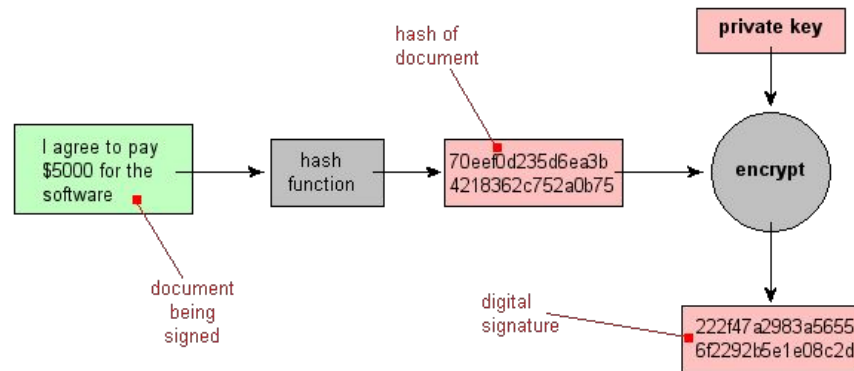
## ProFTPD

Highly configurable GPL-licensed FTP server software

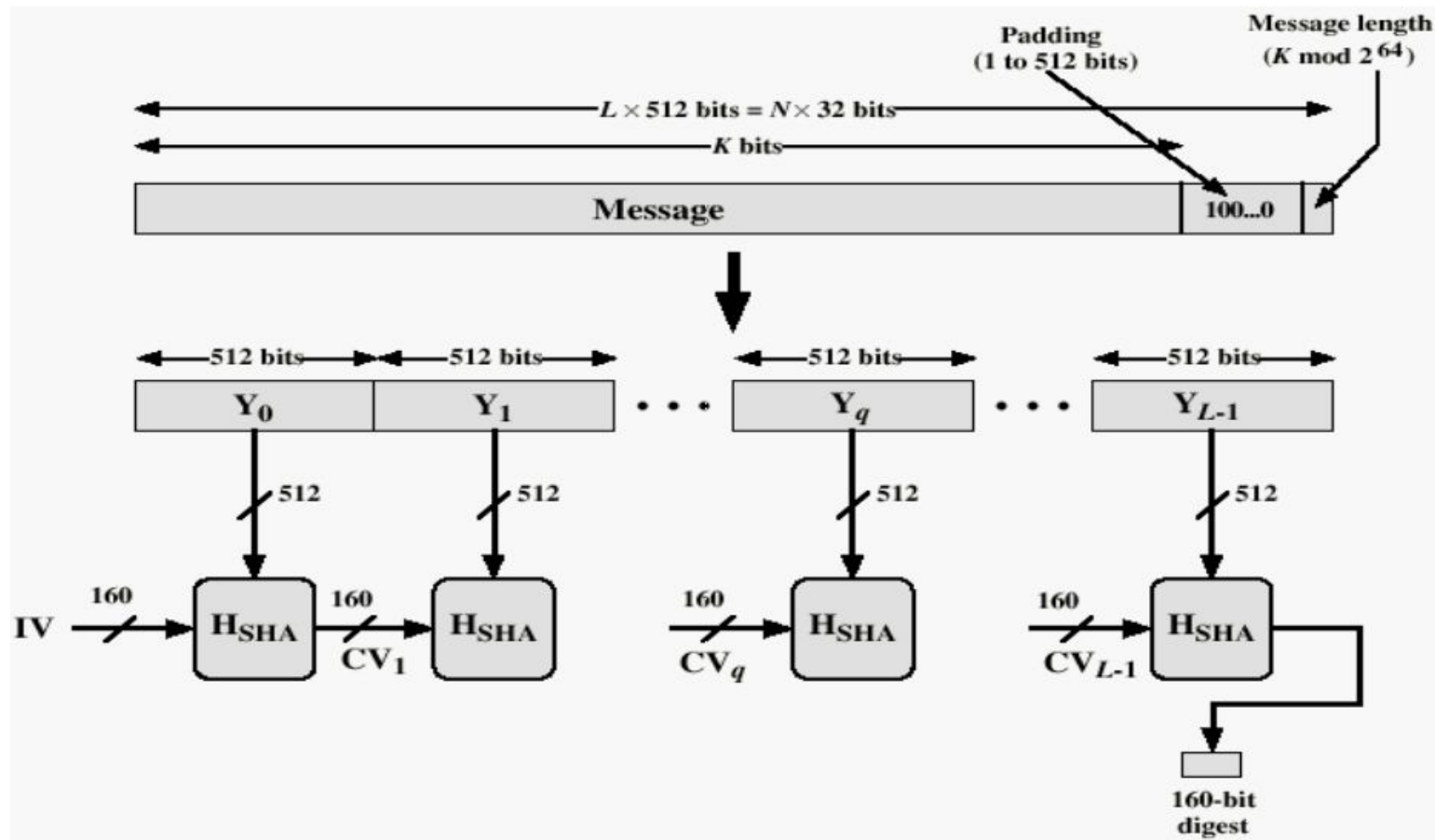
### MD5 sums and PGP signatures of release files

#### MD5 Digest Hashes

417e41092610816bd203c3766e96f23b [proftpd-1.2.8p.tar.bz2](#)  
abf8409bbd9150494bc1847ace06857a [proftpd-1.2.8p.tar.gz](#)  
7c85503b160a36a96594ef75f3180a07 [proftpd-1.2.9.tar.bz2](#)  
445fbf24e2ec300800a184eb81296bda [proftpd-1.2.9.tar.gz](#)  
d834bb822816a2ce483cc2ef1a9533e7 [proftpd-1.2.10rc3.tar.bz2](#)  
1e306d2f54ea92895ecff6659498b911 [proftpd-1.2.10rc3.tar.gz](#)



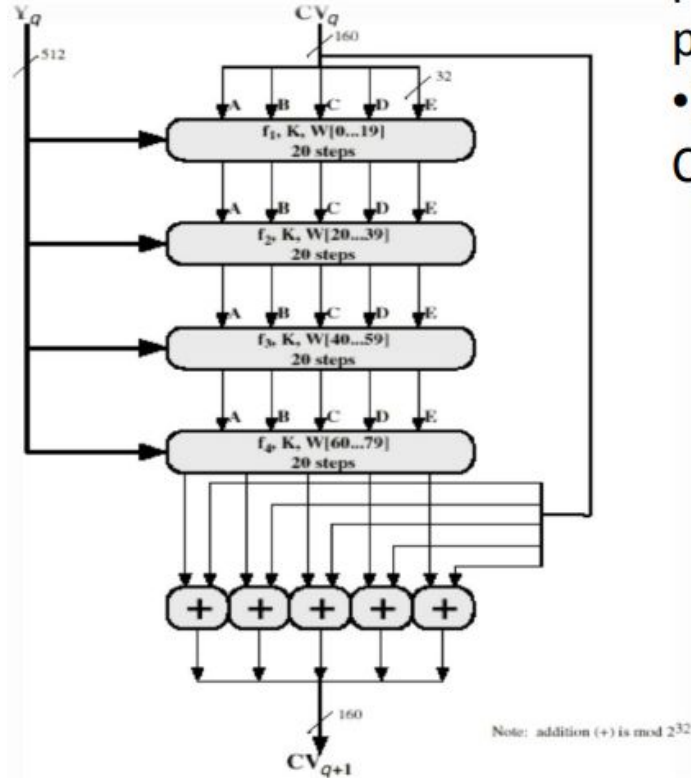
# SHA-1



# Un bloque de la función Hsha

- Cada función está compuesta por 4 etapas, cada una de 20 pasos.
- Los valores iniciales de A, B, C, D, E son los siguientes:

**A=67452301**  
**B=EFCDAB89**  
**C=98BADCFE**  
**D=10325476**  
**E=C3D2E1F0**

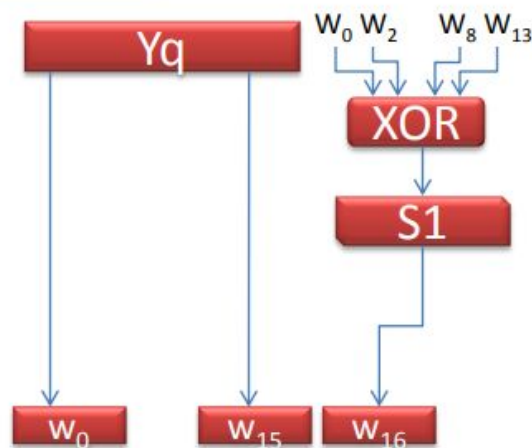


A,B,C,D	Palabras del Buffer
t	Paso ( 0-19
F	Función F
S	Rotación de k bits a la izq.
W	Palabra de 32 bits derivada de la entrada del bloque

# Función Hsha

$$A, B, C, D, E \leftarrow (E + f(t, B, C, D) + S^5(A) + W_t + K_t), A, S^{30}(B), C, D$$

Paso t	Kt	FUNCIÓN f
0-19	5A827999	(B&C)+(B&D)
20-39	6ED9EBA1	B xor C xor D
40-59	8F1BBCDC	(B&C)+(B&D)+(C&D)
60-79	CA62C1D6	B xor C xor D



$$W_t = S^1(W_{t-16} \oplus W_{t-8} \oplus W_{t-3}) \quad \text{Éc.1}$$

## Referencias:

Para convertir cadenas con hash (md5)

<http://www.md5.cz/>

Definición y aplicaciones

<http://unixwiz.net/techtips/iguide-crypto-hashes.html>

“La criptografía clasica”, Santiago Fernández, Abril 2004, <https://s3.amazonaws.com/>

“Introducción a la criptografía”, Reinaldo Mayol Arnao, Octubre 2012, <http://www.eslared.net/>

“Desencriptar cadenas MD5”

<https://www.md5online.es>