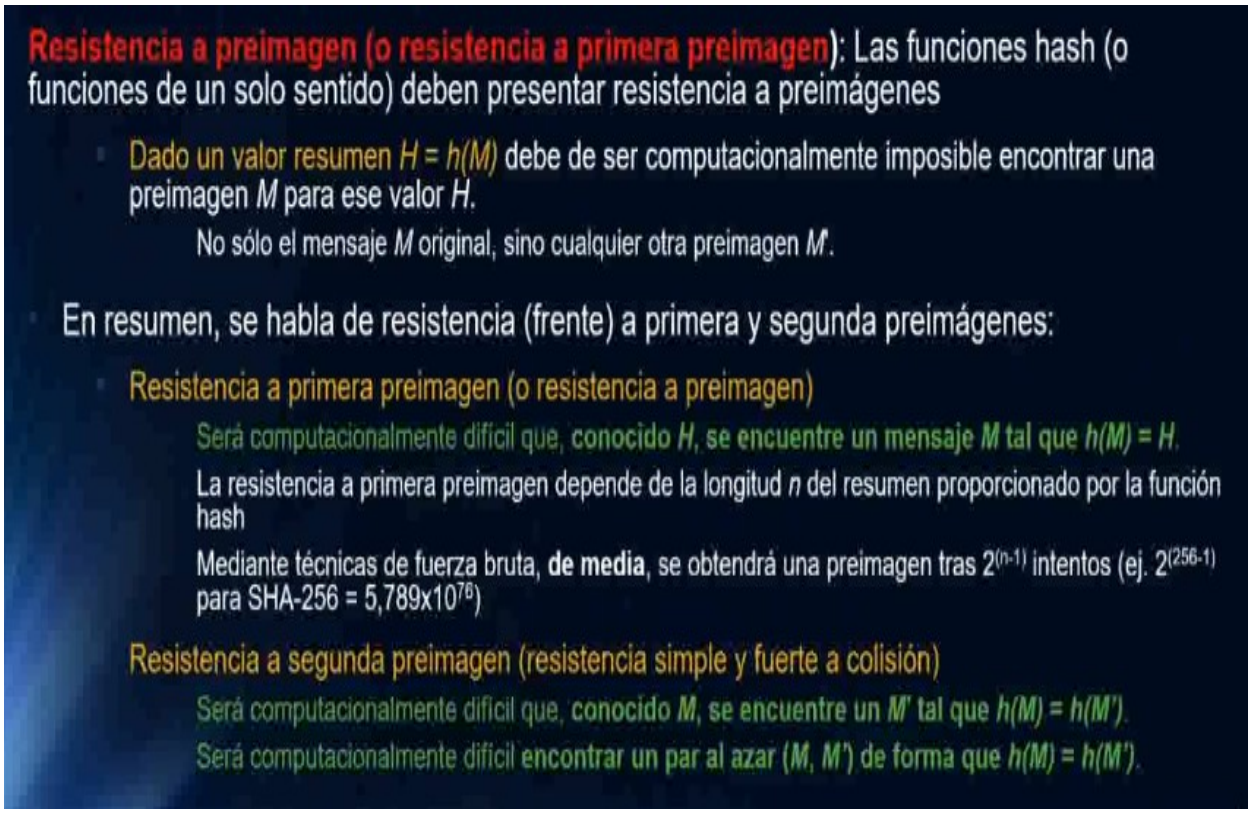
Hash

Una función hash criptografía, también conocida como función digesto o función resumen, es un algoritmo matemático que transforma un conjunto de datos de entrada en una salida de longitud fija. Esto nos puede llevar a conseguir que una entrada de gran tamaño tenga una salida de tamaño reducido.

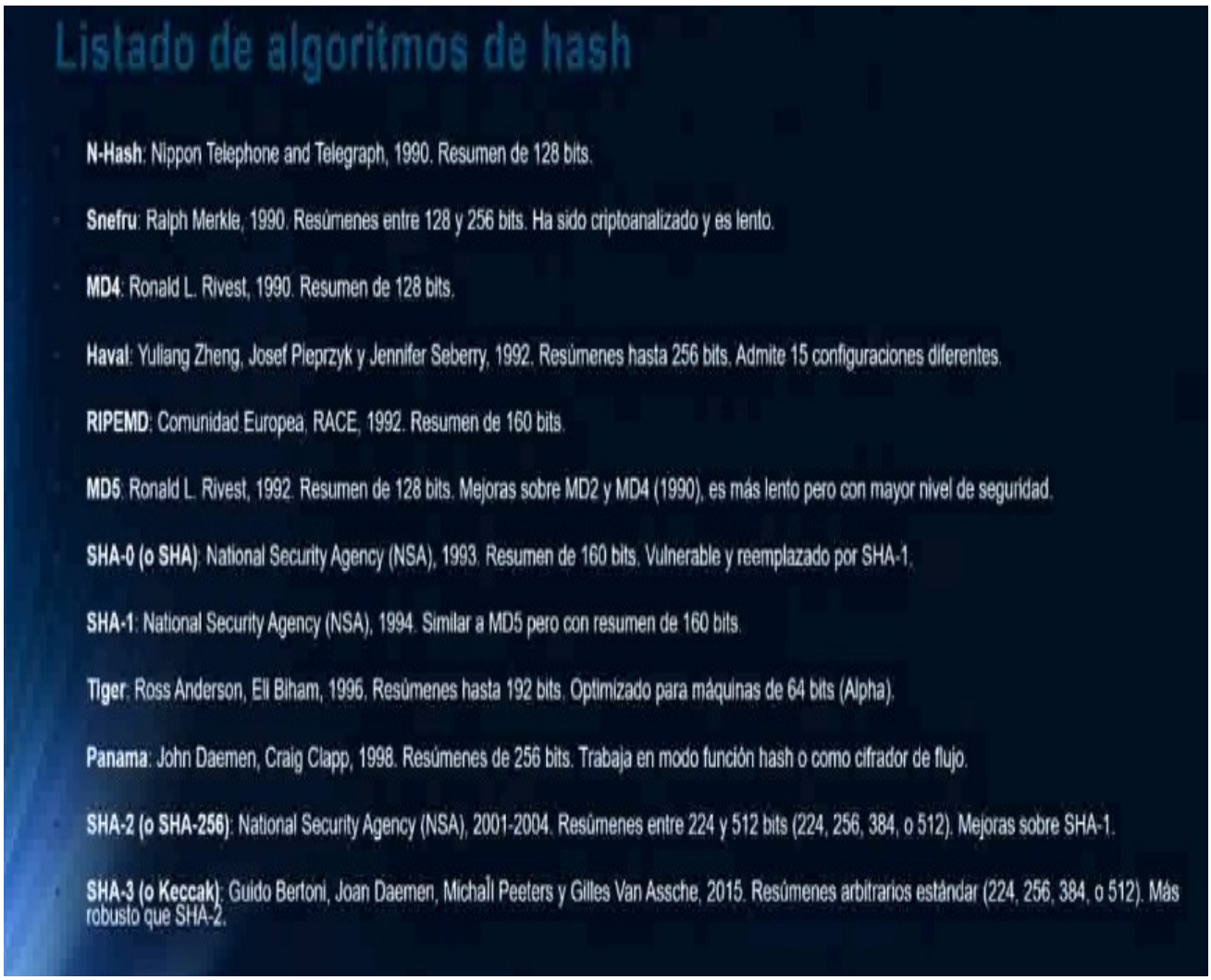
Ejemplos de funciones hash criptográficas son: MD5, SHA-1, SHA-2(SHA-256,….), SHA-3, BLAKE2, etc.…. El tamaño del hash H=h(M) dependerá del algorimo de hash utilizado. Por ejemplo el MD5 es de 128 bits, el SHA-1 es de 160 bits, el SHA-2 de 256 bits…..

Propiedades de las funciones hash:

- Facilidad de cálculo.
- Propiedad unidireccionalidad (de un sólo sentido): dada la salida no debe ser fácil de encontrar la entrada. Aunque con los ataques de diccionario (fuerza bruta) se puede conseguir obtener.
- Propiedad de compresión.
- Propiedad de difusión.
- Propiedad de no predictibilidad.
- Resistencia a preimagen (o resistencia a primera preimagen).
- Resistencia simple a colisiones (o resistencia a segunda preimagen).
- Resistencia fuerte a colisiones.



Mínimos cambios en una entrada pueden producir máximos cambios en la salida.

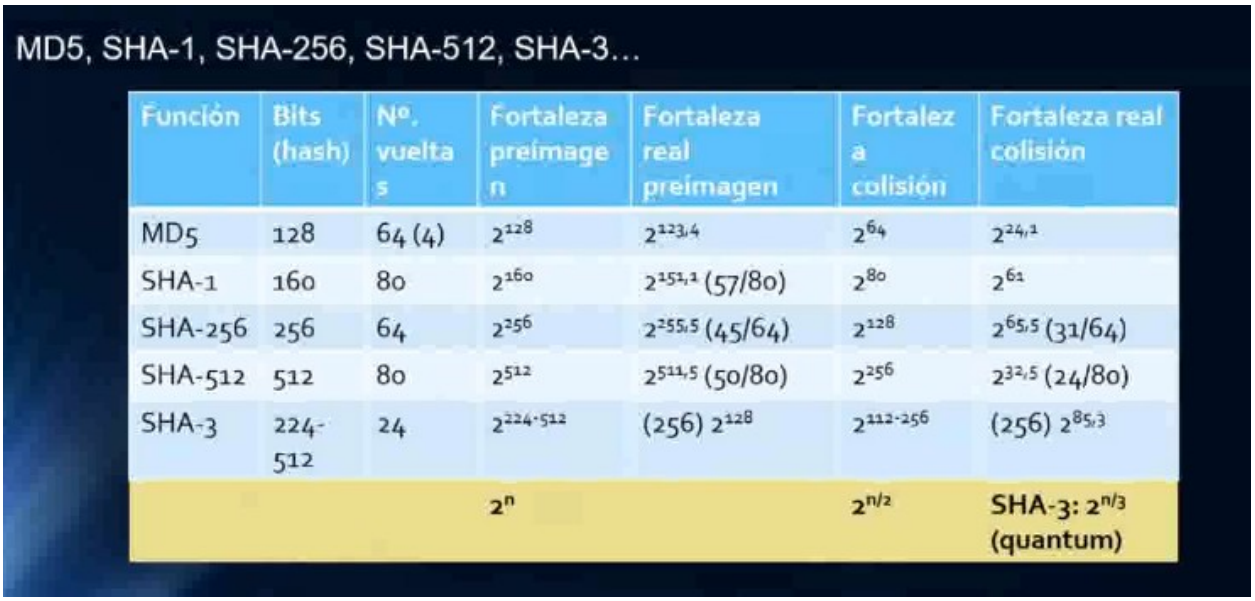


¿Qué algoritmo de hash debería utilizar y con qué longitud?

Pues a diferencia de como ocurre con los algoritmos de cifra simétricos, por ejemplo, la elección de la longitud del hash viene impuesta (en la mayoría de los escenarios) por la función de hash utilizada.

En la actualidad se recomienda el uso de SHA-2, es decir, SHA-256 o superior (SHA.384 o SHA-512), no se debería usar MD5 o SHA-1. Si lo que queremos es anticiparnos a usos futuros, se podría hacer uso de SHA-3(256,384 o 512 bits) o de BLAKE2.

Comparativa de algunos algoritmos Hash:



Función	Bits (hash)	Nº. vueltas	Fortaleza preimagen	Fortaleza real preimagen	Fortaleza colisión	Fortaleza real colisión
MD5	128	64 (4)	2^{128}	$2^{123,4}$	2^{64}	$2^{24,1}$
SHA-1	160	80	2^{160}	$2^{151,1}$ (57/80)	2^{80}	2^{61}
SHA-256	256	64	2^{256}	$2^{255,5}$ (45/64)	2^{128}	$2^{65,5}$ (31/64)
SHA-512	512	80	2^{512}	$2^{511,5}$ (50/80)	2^{256}	$2^{32,5}$ (24/80)
SHA-3	224-512	24	$2^{224-512}$	(256) 2^{128}	$2^{112-256}$	(256) $2^{85,3}$
			2^{n}		$2^{n/2}$	SHA-3: $2^{n/3}$ (quantum)

Ejemplo de utilización de hashcat:

Cómo utilizar hashcat con un hash de tipo 6 que se corresponde con sha512 para eso utilizamos la opción -m 1800 y la opción -a 0 le indica que vamos a usar sobre el fichero a crackear fichero.txt con un diccionario de contraseñas que está almacenado en la ruta */usr*share/wordlist/rockyou.txt

hashcat -m 1800 -a 0 fichero.txt /usr/share/wordlists/rockyou.txt

Calulador de hash:

https://md5hashing.net/