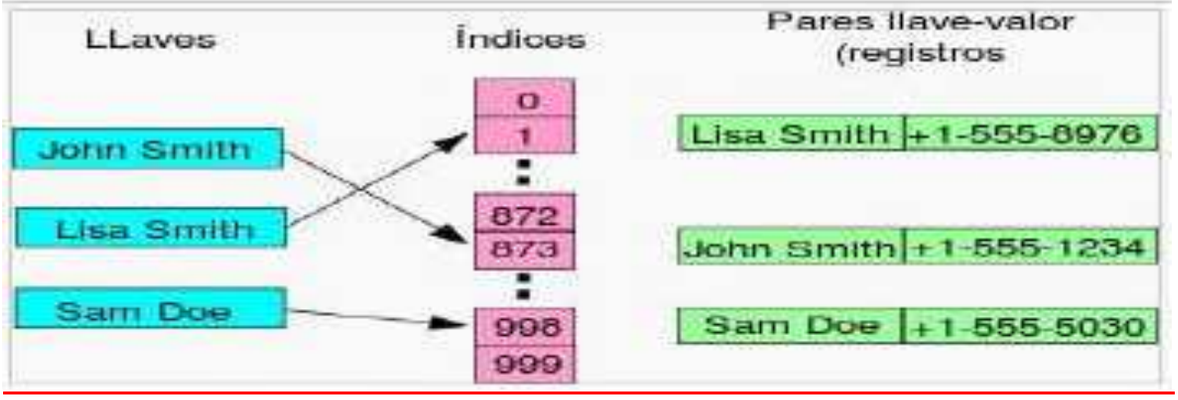
Conceptos Básicos:

1. **Funciones basadas en algoritmos que obtienen un resumen de fichero /mensaje (un texto, una imagen, …).**

2. **El resumen es único para el mensaje** (o por lo menos las probabilidades son muy pequeñas).

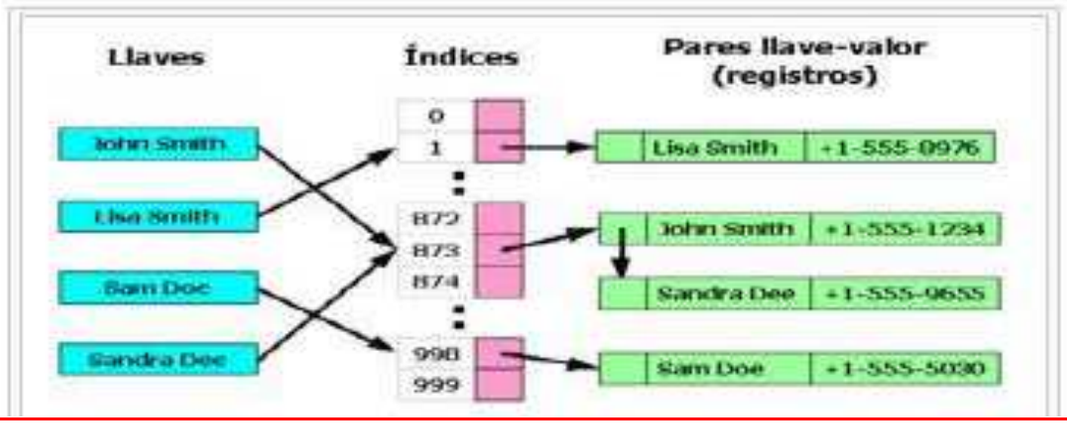
3. **Son funciones de un solo sentido: conocido el resumen no se puede conocer el fichero/mensaje.**

Ejemplo de Tabla Hash



http://spi1.nisu.org/recop/al02/orestesc/funciones_hash.html

Ejemplo de Colisiones.



Algoritmos

1. **Función Hash Ideal:** es fácil de generar, es muy difícil generar el mensaje a partir de hash (difícil de encontrar dos mensajes con el mismo hash)

2. **MD5**
   - Muy utilizado para verificar los ficheros descargados a través de la red
   - Protección contra malware
   - Protección contra la corrupción del fichero.
   - Procesa el texto en bloques de 512 bits y produce resúmenes de 128 bits

3. **SHA**
   - Más seguro
   - Procesa el texto en bloques de 512 bits y produce 160 bits

4. **Tanto MD5 como SHA-1 están en entredicho.**

5. **Alternativas:** Familia SHA-2, Whirlpool, ...

Aplicaciones

1. **Verificación de la integridad de mensajes y archivos** ➔ Informática forense

2. **Verificación de contraseñas** ➔ Un mecanismo muy extendido de autenticación de usuarios consiste en solicitar una contraseña y comprobar si es correcta antes de autorizar el acceso.

3. **Generación de claves y derivación de subclaves** ➔ Las funciones hash criptográficas se han usado ampliamente para generar claves adecuadas que poder usar en un cifrador de flujo o de bloque.

Ejemplos de hashes de mensajes relacionados con distintas funciones de la familia SHA.

Algoritmo	Mensaje	Hash
SHA-1	Cripto	63522e723f931302d5a3946180f41b51ce5ad4bb
	Crypto	fcf7ea87204ea629adcb68c3ccf592c0eb81a700
SHA-2 (224)	Cripto	94656c4d0dddbe1c2cde0603244d5fe7cc94a9de a36593eaac18df09
	Crypto	d2be9445eb944aa6f12664c39fde22fd457b447e 3d8e01fc4fbcd6e7
SHA-2 (256)	Cripto	d9389a3461380f5fdb6807efac49aaa147cc9381 10daf41f9c39192f0167fbd3
	Crypto	f96db04ed9317354273d43d1a816746ccc2b843f 31443d771c8a1b157fb00ceb
SHA-2 (384)	Cripto	222b1a002a0523e0d72a55e17bc15d6237dc0b23 56e08f7b22537bef3eff063caf42792a86e24e2f 412f12f23294b055
	Crypto	c0173e88d8d4e81630863d80d160cfc6f29d2b05 efcf17875c86b6810dc5f32a9afcb0b1e943fe75 bea7958f0baa5544
SHA-2 (512)	Cripto	4cfb5d226182b9f67c86dfdbc37c4921e739026b e4899f5c35613d29cae74537b7251fea67ae259f 0015284eb7d5fa3cb8cec1811ddf75c2f932d8e4 357c53f5
	Crypto	ac9195c053cde2f5b5f87c8e10790e16f71124dd fdcb8d2c3c163dfc49fadfabfa57da5936c12454 b52bbffb1ce225db472e8ee2a877340da3091419 8825d18d6