Secure Hash Algorithm

El **SHA** (*Secure Hash Algorithm*, Algoritmo de *Hash* Seguro) es una familia de funciones hash de cifrado publicadas por el Instituto Nacional de Estándares y Tecnología (NIST). La primera versión del algoritmo fue creada en 1993 con el nombre de SHA, aunque en la actualidad se la conoce como **SHA-0** para evitar confusiones con las versiones posteriores. La segunda versión del sistema, publicada con el nombre de **SHA-1**, fue publicada dos años más tarde. Posteriormente se han publicado SHA-2 en 2001 (formada por diversas funciones: **SHA-224**, **SHA-256**, **SHA-384**, y **SHA-512**) y la más reciente, **SHA-3**, que fue seleccionada en una competición de funciones hash celebrada por el NIST en 2012. Esta última versión se caracteriza por ser la que más difiere de sus predecesoras.

A lo largo de su historia, se conocen algunos ataques a esta familia de algoritmos:

- En 1998 se encontró una vulnerabilidad para SHA-0, aunque esta no se podía extender a **SHA-1**. En cualquier caso, la NSA aumentó en ese momento la seguridad del **SHA-1**.
- En 2004 se encontró una debilidad matemática en SHA-1, que permitiría encontrar colisiones de hash más rápido. Sin embargo, este hallazgo resulta poco relevante, pues la complejidad de búsqueda de colisiones pasaría de 2^{80} a 2^{69}, algo que aún es computacionalmente inviable, requiriendo incluso más trabajo que MD5 (2^{64}).

SHA-1

SHA-1 ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo. No obstante, en el año 2004, un número de ataques significativos fueron divulgados sobre funciones criptográficas de *hash* con una estructura similar a SHA-1; lo que ha planteado dudas sobre la seguridad a largo plazo de SHA-1.

SHA-0 y SHA-1 producen una salida resumen de 160 bits (20 bytes) de un mensaje que puede tener un tamaño máximo de 2^{64} bits, y se basa en principios similares a los usados por el profesor Ronald L. Rivest del MIT en el diseño de los algoritmos de resumen de mensaje MD4 y MD5.

La codificación *hash* vacía para SHA-1 corresponde a:

```
SHA1("") = da39a3ee5e6b4b0d3255bfef95601890afd80709
```

CLAVE FORÁNEA

En el contexto de bases de datos relacionales, una clave foránea o clave ajena (o Foreign Key FK) es una limitación referencial entre dos tablas. La clave foránea identifica una columna o grupo de columnas en una tabla (tabla hija o referendo)

que se refiere a una columna o grupo de columnas en otra tabla (tabla maestra o referenciada). Las columnas en la tabla referendo deben ser la clave primaria u otra clave candidata en la tabla referenciada.

Los valores en una fila de las columnas referendo deben existir solo en una fila en la tabla referenciada. Así, una fila en la tabla referendo no puede contener valores que no existen en la tabla referenciada. De esta forma, las referencias pueden ser creadas para vincular o relacionar información. Esto es una parte esencial de la normalización de base de datos. Múltiples filas en la tabla referendo pueden hacer referencia, vincularse o relacionarse a la misma fila en la tabla referenciada. Mayormente esto se ve reflejado en una relación uno (tabla maestra o referenciada) a muchos (tabla hija o referendo).