SHA-1 (Secure Hash Algorithm 1) es una función de hash criptográfica que toma una entrada y produce un hash de 160 bits (20 bytes) de largo. Fue desarrollado por la Agencia de Seguridad Nacional (NSA) de Estados Unidos y publicado por el Instituto Nacional de Estándares y Tecnología (NIST) como un estándar del gobierno de los EE. UU. (FIPS PUB 180-1) en 1995.

### Características Principales

- \*\*Longitud del Hash\*\*: SHA-1 produce un hash de 160 bits (20 bytes).

- \*\*Determinístico\*\*: El mismo mensaje de entrada siempre produce el mismo hash.

- \*\*Rápido\*\*: SHA-1 es eficiente en términos de tiempo de cómputo.

- \*\*Propiedades Criptográficas\*\*: SHA-1 está diseñado para ser resistente a la colisión, al preimagen y a los segundos preimagenes, aunque estas propiedades se han visto comprometidas con el tiempo.

### Uso Común

SHA-1 ha sido ampliamente utilizado en diversas aplicaciones, incluyendo:

- \*\*Certificados digitales\*\*: Utilizado en la firma de certificados digitales.

- \*\*Sistemas de control de versiones\*\*: Empleado en sistemas como Git para asegurar la integridad de los datos.

- \*\*Protocolos de seguridad\*\*: Utilizado en protocolos de seguridad como TLS/SSL.

### Vulnerabilidades

A lo largo de los años, se han encontrado varias vulnerabilidades en SHA-1 que comprometen su seguridad:

- \*\*Colisiones\*\*: SHA-1 ya no se considera seguro contra ataques de colisión. Una colisión ocurre cuando dos entradas diferentes producen el mismo hash. En 2005, investigadores demostraron que era posible encontrar colisiones en SHA-1 más rápido que con un ataque de fuerza bruta.

- \*\*Ataques Prácticos\*\*: En 2017, Google y CWI Amsterdam anunciaron el primer ataque práctico contra SHA-1, conocido como SHAttered, que mostró una colisión real de SHA-1 usando técnicas avanzadas y una gran cantidad de poder de cómputo.

Debido a estas vulnerabilidades, se ha desaconsejado el uso de SHA-1 en aplicaciones de seguridad críticas. Se recomienda el uso de funciones de hash más seguras, como SHA-256 o SHA-3.

### Reemplazos

Dado que SHA-1 ya no se considera seguro, se han adoptado otros algoritmos más robustos:

- \*\*SHA-2\*\*: Incluye SHA-224, SHA-256, SHA-384 y SHA-512, que ofrecen mayor seguridad.

- \*\*SHA-3\*\*: Publicado por NIST en 2015, se basa en el algoritmo Keccak y proporciona una seguridad mejorada y diferente arquitectura en comparación con SHA-2.

### Conclusión

SHA-1 ha sido un pilar en la criptografía durante muchos años, pero debido a sus vulnerabilidades conocidas, es crucial migrar a algoritmos más seguros como SHA-256 o SHA-3 para garantizar la integridad y seguridad de los datos.