SHA-256

April 21, 2023

SHA-256 I

- SHA 256 is a part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm.
- Published in 2001, it was a joint effort between the NSA and NIST to introduce a successor to the SHA 1 family, which was slowly losing strength against brute force attacks.

Note : A hash function, also referred to as digest or fingerprint, is like a unique signature for a data file or text.

SHA-256 II

- The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits.
- It cannot be read or decrypted, as it only allows for a one-way cryptographic function.

How it works ? I

- There are several steps involved in using SHA-256, including pre-processing a file or text into binary, initializing hash values and round constants, creating a message schedule, compressing, modifying final values, and completing a string concatenation to get all the bits together. More detail
- SHA-256 is one of the most secure and popular hash algorithms. It can be used to scramble and manipulate data irreversibility, which means the input cannot be derived from the 256-bits-long output of SHA-256

Is SHA-256, I

An improvement in hashing ?

- SHA-256 is one of the most secure hashing functions when compared to other hashing functions. Some U.S. government agencies are required to protect certain sensitive data with SHA-256.
- The highly secure structure of the SHA-256 hash makes it a strong barrier against cyberattacks.

Is SHA-256, I

still being used?

SHA-256 is still relevant and is being used today in various applications, including blockchain, cryptocurrency, Secure Sockets Layer (SSL) certificates, and more.

- In blockchain and cryptocurrency applications, SHA-256 is used for proof of work, mining, and creation of cryptocurrency addresses.
  - SHA-256 is part of the process required by the miner to produce hash values for new blocks that are created.
  - Similarly, SHA-256 is required for the public key required to create new Bitcoin addresses.

Is SHA-256, II

still being used?

- The SSL certificate is a type of security technology used to establish an encrypted link between a client and a server.
  - It allows for secure communication for web services and websites.
  - The SSL certification contains certain cryptographic elements that use SHA-256, which has become the industry standard.