SHA-512 Hashing code Documentation

Introduction:

SHA-512, which stands for Secure Hash Algorithm 512-bit, is a member of the SHA-2 family of cryptographic hash functions.It is designed to produce a fixed-size, 512-bit hash value(64 bytes) regardless of size or content of the input data.SHA-512 is widely used in various security applications and protocols to ensure data integrity and authentication.

Key Characteristics

- **Bit Length:** SHA-512 produces a fixed-size hash output of 512 bits (64 bytes).

- **Block Size:** The algorithm processes input data in blocks of 1024 bits (128 bytes).

Operation Overview

1. Padding the Message:

- Input messages undergo a padding process, ensuring a specific format is met.
- Padding includes appending a '1' bit, followed by '0' bits, and concluding with the original message length in bits.

2. Breaking into Blocks:

- Padded messages are divided into blocks of 1024 bits each.

3. Initializing Hash Values:

- SHA-512 has eight initial hash values (H0 to H7), derived from the fractional parts of the square roots of prime numbers.

4. Message Schedule:

- For each block, a message schedule of 80 64-bit words is created.
- The schedule includes both direct block-derived words and words calculated using a recurrence relation.

5. Compression Function (Main Loop):

- The main loop processes each block through 80 rounds.
- Each round involves bitwise operations, circular right shifts, and logical functions.

6. Updating Hash Values:

- Hash values (H0 to H7) are continually updated based on the calculations in the compression function.

7. Final Hash:

- After processing all blocks, the final hash value is obtained by concatenating the eight 64-bit hash values.

Security:

- **Collision Resistance:** SHA-512 provides a high level of collision resistance, making it computationally infeasible to find two different inputs producing the same hash.

- **Current Security Status:** As of my last knowledge update in January 2022, SHA-512 is considered secure for most cryptographic purposes.

Use Cases

- **Digital Signatures**:SHA-512 is commonly used in digital signature algorithms for ensuring the integrity and authenticity of messages.

- **Password Hashing:** It is employed in password hashing algorithms to securely store user passwords.

- **Certificate Authorities:** SHA-512 is used in digital certificates to sign and verify the authenticity of the certificate.

Conclusion:

SHA-512 stands as a robust and widely accepted cryptographic hash function, offering a high level of security and reliability in various security applications.