SHA-512 HASHING ALGORITHM

The SHA-512 (Secure Hash Algorithm 512-bit) is a cryptographic hash function that takes an input message and produces a 512-bit (64-byte) hash value. It is commonly used for data integrity verification and password storage.

Functions:

1. right_rotate(n: int, bits: int)-> int
  - Purpose: Rotates an integer right by a given number of bits.
  - Parameters:
    - `n`: The integer to rotate.
    - `bits`: The number of bits to rotate.
  - Returns: The rotated integer.

2. sha512(message: str)-> str
  - Purpose: Computes the SHA-512 hash of a given message.
  - Parameters:
    - message: The input message as a string.
  - Returns: The SHA-512 hash as a hexadecimal string.

Class: SHA512Hasher

This class encapsulates the SHA-512 hashing process, making it convenient to compute the hash of input messages while hiding the underlying implementation details.

Methods:

1. __init__(self)
  - Initializes the SHA-512 hasher with initial hash values and constants.

2. right_rotate(self, n: int, bits: int)-> int
  - Rotates an integer right by a given number of bits.

3. padding_msg(self, message: bytes)-> bytes
  - Pads the input message to a length multiple of 128 bytes.

4. divide_into_blocks(self, padded_msg: bytes)-> List[bytes]
  - Divides the padded message into 128-byte blocks.

5. sigma_0(self, x: int)-> int
  - SHA-512 Sigma function 0.

6. sigma_1(self, x: int)-> int
  - SHA-512 Sigma function 1.

7. ch(self, e: int, f: int, g: int)-> int
  - SHA-512 choice function.

8. maj(self, a: int, b: int, c: int)-> int
  - SHA-512 majority function.

9. a_summation(self, a: int)-> int
  - SHA-512 summation function for A.

10. e_summation(self, e: int)-> int
  - SHA-512 summation function for E.

11. compute(self, message: bytes)-> str
  - Computes the SHA-512 hash of the given message.
  - Parameters:
    - message: The input message as bytes.
  - Returns: The SHA-512 hash as a hexadecimal string.

12.sha512(self, message: str)-> str
  - Computes the SHA-512 hash of a message using the SHA-512 algorithm.
  - Parameters:
    - message: The input message as a string.
  - Returns: The SHA-512 hash as a hexadecimal string.

This documentation provides an overview of the SHA-512 hashing algorithm, its functions, and the `SHA512Hasher` class that encapsulates the algorithm.

Output: