IMPLEMENTATION OF SHA-512

Implementation of SHA-512 can be done by using C Programming Language.

**SHA-512 Algorithm Overview:**

SHA-512 (Secure Hash Algorithm 512-bit) is a cryptographic hash function that takes an input message and produces a fixed-size 512-bit hash value (64 bytes). The algorithm operates on blocks of data, and these blocks are processed sequentially. The main steps in each block's processing are:

**Initialize Hash Values (H):**

Initialize eight 64-bit hash values (A-H) which are specific constants defined by the SHA-512 standard.

**Message Padding:**

Pad the message to a multiple of the block size (128 bytes for SHA-512). The padding includes the original message length.

**Processing Blocks:**

Divide the padded message into blocks (each 128 bytes) and process each block through the SHA-512 transformation.

**SHA-512 Transformation:**

This is a complex operation involving multiple bitwise operations, additions, and logical functions applied to the data block and the current hash values.

**Update Hash Values:**

Update the hash values (A-H) based on the SHA-512 transformation results.

**Output:**

The final hash value is the concatenation of the updated hash values (A-H).

**Code Structure and Classes Used:**

The provided C code doesn't use explicit classes, but it uses functions to encapsulate different parts of the SHA-512 algorithm. Here's a brief explanation of the main functions and their roles:

**sha512\_transform:**

Performs the SHA-512 block transformation. This function applies the core SHA-512 operations to a block of data and updates the hash state.

**sha512\_init:**

Initializes the SHA-512 context by setting the initial hash values and resetting other internal variables.

**sha512\_update:**

Updates the SHA-512 context with new data, incorporating it into the hash calculation.

**sha512\_final**:

Finalizes the hash calculation, adding padding as necessary and obtaining the final hash value.

**sha512:**

A wrapper function that initializes the context, updates it with the provided data, and finalizes the hash calculation to obtain the final SHA-512 hash.