**Documentation on SHA -512**

SHA-512( (Secure Hash Algorithm -512) is a secure hash function that produces a fixed-size output of 512 bit or 64 byte from an input message .

The key components used in the SHA-512 implementation are :

1. **Constants (K):** The constant "k" are set of specific (80) constants used during the computation of the hash.
2. **Initial Hash values(Hash\_Values):** These are the initial hash values for SHA-512. These values will be updated as each block of the message is processed.
3. **SHA-512 Functions:**

* **Ch(e, f, g):** Ch function is bitwise operation used during the compression step of the algorithm. e, f, and g are 64-bit words, which are part of the state of the hash function during processing.
* **Maj(a, b, c):**It is another function which is used for bitwise operation during compression step of the function which operates on a, b ,c (64 bit inputs).
* **rotr (x,n):** rotr function (right circular shift) is a bitwise operation that rotates the bits of a 64-bit word x to the right by n positions.
* **summation\_a(a):** summation\_a function performs a specific bitwise operation on a 64-bit word a.
* **summation\_e(e):** summation\_e function involves bitwise operations on a 64-bit word e.
* **sigma\_0(word):** This function involves specific bitwise operations on a 64-bit word ‘word’
* **sigma\_1(word):** This function also involves specific bitwise operations on a 64-bit word ‘word’.
* **addition\_modulo\_2\_64(value):** The addition\_modulo\_2\_64 function is used to perform addition modulo 2^64 on a given value. The padding includes a '1' bit followed by '0' bits and the original message length.
* **divide\_to\_blocks(message):** The divide\_to\_blocks function is used to divide a padded message into blocks of 1024 bits (128 bytes) each.
* **compression\_function(message):** This function is responsible for processing a 1024-bit (128-byte) block of the padded message during the hash computation and also updates the internal state of the hash function based on the input block.

1. **USAGE:**

**A screen shot of a computer program

Description automatically generated**

This part of the code take an input message pads the message ,divides the blocks and then initiates SHA hashing process and prints the final 512 bit hash value.

.