A Description of the SHA-512

SHA-512 is a variant of SHA-256 which operates on eight 64-bitwords. The message to be hashed is first(1)padded with its length in such a way that the result is a multiple of 1024 bits long, and then(2)parsed in to 1024-bit message blocks

The message blocks are processed one at a time: beginning with fixed initial hash value H^0

The SHA-512 compression function operates on a 1024-bit message block and a 512-bit intermediate hash value. It is essentially a 512-bit block cipher algorithm

Which encrypts the intermediate hash value using the message block as key.

Hence there are two main components to describe:(1)the SHA-512 compression function, and(2)the SHA-512message schedule.