SECURE HASH ALGORITHM (SHA)

The most widely used hash function has been the Secure Hash Algorithm (SHA). SHA was developed by the National Institute of Standards and Technology (NIST) and published as a federal information processing standard (FIPS 180) in 1993.SHA is based on the hash function MD4, and its design closely models MD4. Three new versions of SHA, with hash value lengths of 256, 384, and 512 bits, known as SHA-256, SHA-384, and SHA-512, respectively. Collectively, these hash algorithms are known as SHA-2.

SHA-512 Logic

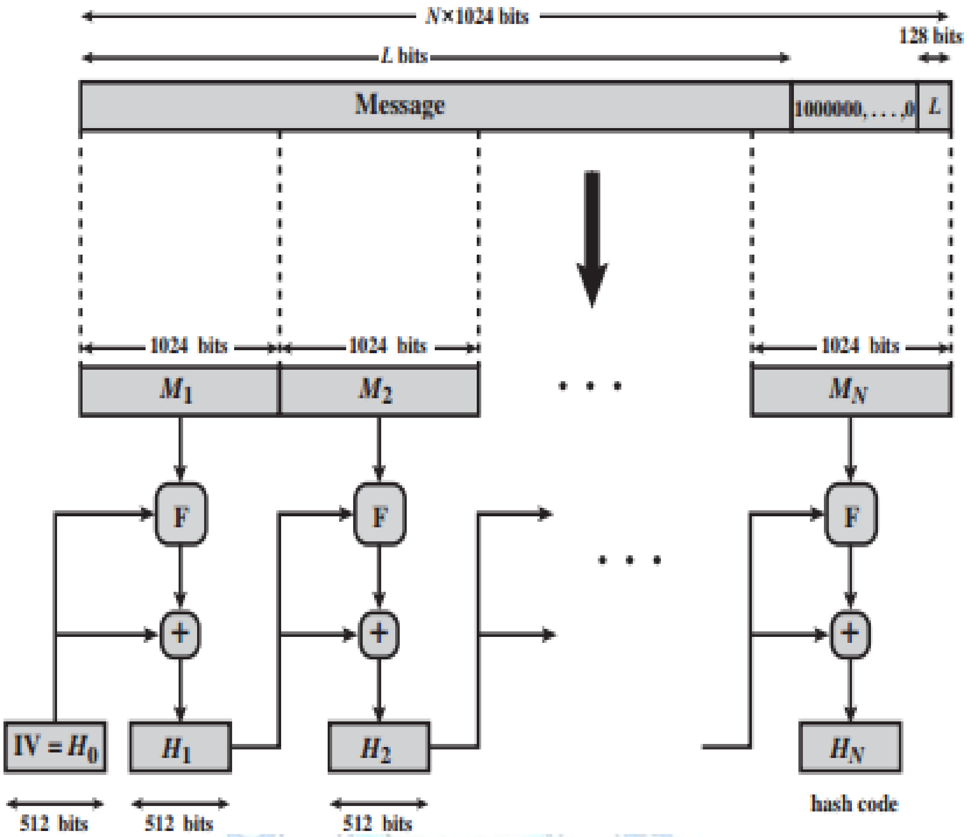
Message Digest Generation Using SHA-512

The algorithm takes as input a message with a maximum length of less than bits 2^{128} bits and produces as output a 512-bit message digest. The input is processed in 1024-bit blocks. The processing consists of the following steps.

Step 1 Append padding bits. The message is padded so that its length is congruent to 896 modulo 1024 of 1 to 1024. The padding consists of a single 1 bit followed by the necessary number of 0 bits.

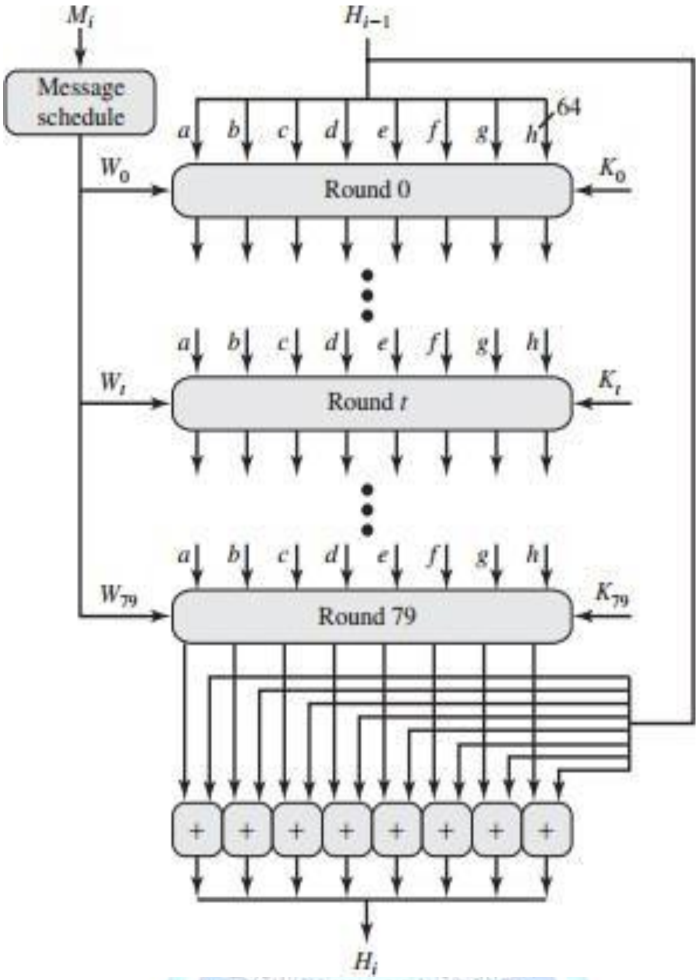
Step 2 Append length. A block of 128 bits is appended to the message. This block is treated as an unsigned 128-bit integer (most significant byte first) and contains the length of the original message (before the padding).

The outcome of the first two steps yields a message that is an integer multiple of 1024 bits in length. The expanded message is represented as the sequence of 1024-bit blocks *M*1, *M*2, Á , *MN* , so that the total length of the expanded message is *N* * 1024 bits



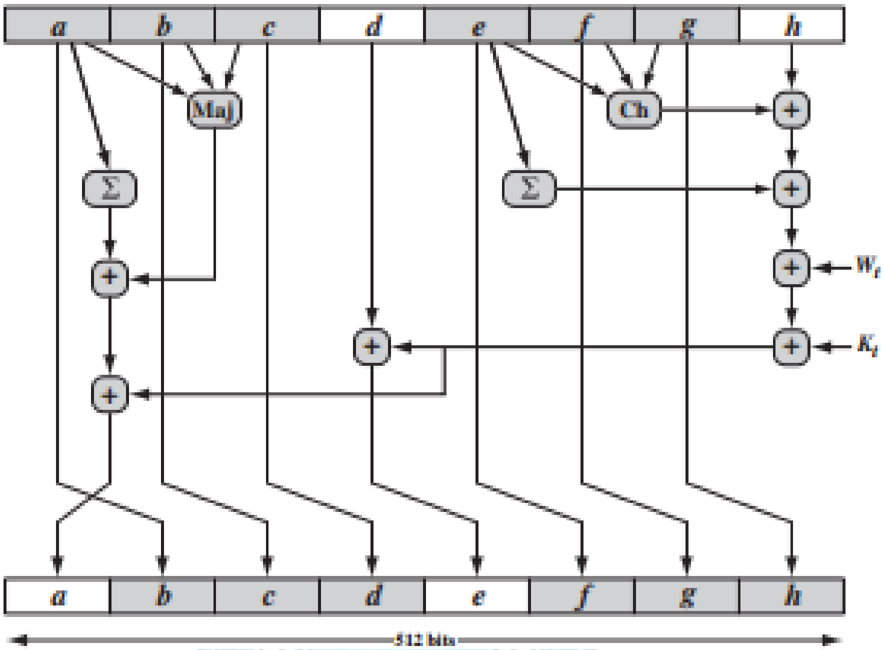
Step 3 Initialize hash buffer. A 512-bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers (a, b, c, d, e, f, g, h).These registers are initialized to the following 64-bit integers (hexadecimal values) These values are stored in **big-endian** format, which is the most significant byte of a word in the low-address (leftmost) byte position.

Step 4 Process message in 1024-bit (128-word) blocks. The heart of the algorithm is a module that consists of 80 rounds; Each round takes as input the 512-bit buffer value, ABCDEFGH, and updates the contents of the buffer. At input to the first round, the buffer has the value of the intermediate hash value, *Hi*-1).



SHA-512 Processing of a Single 1024-Bit Block

Step 5 Output. After all 1024-bit blocks have been processed, the output from the N th stage is the 512- bit message digest. Thus, in the first 16 steps of processing, the value of Wt is equal to the corresponding word in the message block. For the remaining 64 steps, the value of Wt consists of the circular left shift by one bit of the XOR of four of the preceding values of Wt , with two of those values subjected to shift and rotate operations.



Compression Function