2. Characteristics and Assessment of Performance

MD-2:- MD-2 takes a message equal to an arbitrary number of 8-bit bytes and produces a 128 bit message digest. It cannot handle a message that is not an integral number of bytes, though it would be simple to modify MD-2, or to have a convention for bit padding message before feeding it to MD-2 [5]. The basic idea behind MD-2 is as follows:

- The input to MD-2 is a message whose length is an arbitrary number of bytes.
- The message is padded according to specified conventions, to be a multiple of 16 bytes.
- A 16 byte quantity, which MD-2 calls a checksum, is appended to the end. This checksum is a strange function of the padded message defined specifically for MD-2.
- Final pass- The message is processed, 16 bytes at a time, each time producing an intermediate result for the message digest. Each intermediate value of the message digest depends on the previous intermediate value and the value of the 16 bytes of the message being processed.

MD-4:- MD-4 was designed to be 32 bit word oriented. MD-4 can handle message with an arbitrary number of bits. Like MD-2 it can be computed in a single pass, though MD-4 needs more intermediate states [5].

- In MD-4 message digest to be computed is a 128 bit quantity (four 32 bit words). The message is processed in 512 bits (sixteen 32 bit words) blocks. The message digest is initialized to a fixed value, and then each stage of the message digest computation takes the current value of the message digest and modifies it using the next block of the message. The final result is the message digest for the entire message.
- Each stage makes 3 passes over the message block. Each block has a slightly different method of mangling the message digest. At the end of the stage, each word of the mangled message digest is added to its pre-stage value (which becomes the pre-stage value for the next stage). Therefore, the current value of the message digest must be saved at the beginning of the stage so that it can be added in at the end of the stage. Each stage starts with a 16 word message block and a 4 word message digest value [6].

MD-5:-MD-5 was designed to be somewhat more 'conservative' than MD-4 in terms of being less concerned with speed and more concerned with security. It is very similar to MD-4. The major differences are:

- MD-4 takes 3 passes over each 16 byte chunk of the message. MD-5 makes 4 passes over each 16 byte chunk.
- The functions are slightly different, as are the number of bits in the shifts.
- MD-4 has one constant which is used for each message word in pass 2, and a different constant used for the entire 16 message words in pass 3. No constant is used in pass 1.

MD-5 uses a different constant for each message word on each pass. Since there are 4 passes, each of which deals with 16 message words, there are 64 32-bit word constants used in MD-5.

The message digest in MD-5 is a 128 bit quantity (four 32-bit words). Each stage consists of computing a function based on the 512 bit message chunk and the message digest to produce a new intermediate value for the message digest. The value of the message digest is the result of the output of the final block of message.

Each stage in MD-5 takes four passes over the message block. At the end of the stage, each word of the modified message digest is added to the corresponding pre-stage message digest value [5].

SHA: This Standard specifies five secure hash algorithms, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. All five of the algorithms are iterative, one-way hash functions that can process a message to produce a condensed representation also called as a message digest.

Each algorithm can be described in two stages**:** preprocessing and hash computation. Preprocessing involves padding a message, parsing the padded message into m-bit blocks, and setting initialization values to be used in the hash computation. The hash computation generates a message schedule from the padded message and uses that schedule, along with functions, constants, and word operations to iteratively generate a series of hash values. The final hash value generated by the hash computation is used to determine the message digest. The five algorithms differ most significantly in the security strengths that are provided for the data being hashed. Here, only 3 of them SHA-1, SHA-256 and SHA-512 described in detail because SHA-224 and SHA-384 are almost same as SHA-256 and SHA-512 respectively [8].

3. Case Study and Results

(A) Tools Used in Simulation

For the simulation of the described work, laptop with core-i5 64-bit microprocessor at 2.4 GHz, having 4GB RAM is used as machine, while the MATLAB 7.8 launched in February 2009, as a 64-bit software is employed. For the compilation of the report, Microsoft Office 2007 is used with their tools like Equation Editor, Visio and Picture Manager.

(B) Results

The conventional and proposed work are correctly simulated and output of the conventional Message Digests has been cross checked with published example in FIPS-180-3 [5]. Among several available parameters regarding the performance, a few are taken into account and analyzed after the simulation. These parameters are Message Digest calculation time, number of CPU cycles consumed. As the security parameters, some of the randomness tests have been performed to check the results with strict avalanche criteria.

(1) Hash Calculation Time

The message digest calculation time is one of the very important parameter while observing performance of any algorithm. The observed time is in seconds.