Secure Hash Algorithm-1

The output of SHA-1 message digest is 160 bits in length, which is 32 bits more than MD5.

SHA is designed to be computationally infeasible to

a) obtain the original message, given its message digest.
b) find two messages producing the same message digest.

Working of SHA-1

Step 1 : Padding

Like MD5, the first step in SHA is add padding to the end of the original message in such a way that the length of the message is 64 bits short of a multiple of 512.

The padding bits are always added, even if the message is already 64 bits short of a multiple pf 512.

Working of SHA-1

Step 2 : Append Length

The length of the message excluding the length of the padding is now calculated and appended to the end of the padding as a 64 bit block.

Working of SHA-1

Step 3 : Divide the Input

The input message is now divided into blocks, each of length 512 bits. These blocks become the input to the message-digest processing logic.

Working of SHA-1

Step 4 : Initialize Chaining Variables

5 Chaining variables, A,B,C,D and E are initialized each of 32 bits.

In SHA, the variables A through D have the same values as they had in MD5, additionally, E is initialized as HEX C3 D2 E1 F0.

Working of SHA-1

Step 5 : Process Blocks

Step 5.1 : Copy the Chaining variables A-E into variables a-e. The combination of a-e, called abcde will be considered as a single register for storing the temporary intermediate as well as final results.

Working of SHA-1

Step 5 : Process Blocks

Step 5.2 : Divide the current 512 bit block into 16 sub blocks each consisting of 32 bits.

Working of SHA-1

Step 5 : Process Blocks

Step 5.3 : SHA has 4 rounds, each consisting of 20 steps.
Each round takes the current 512 bit block, the register abcde and a constant K[t], t ranging from 0-79.

It then updates the contents of the register abcde using the SHA algorithm steps.

A major difference is the fact that we had 64 different constants defined as K in MD5, Here we have only 4 constants defined for K[t]. one used in each of the 4 rounds.

Working of SHA-1

Step 5 : Process Blocks

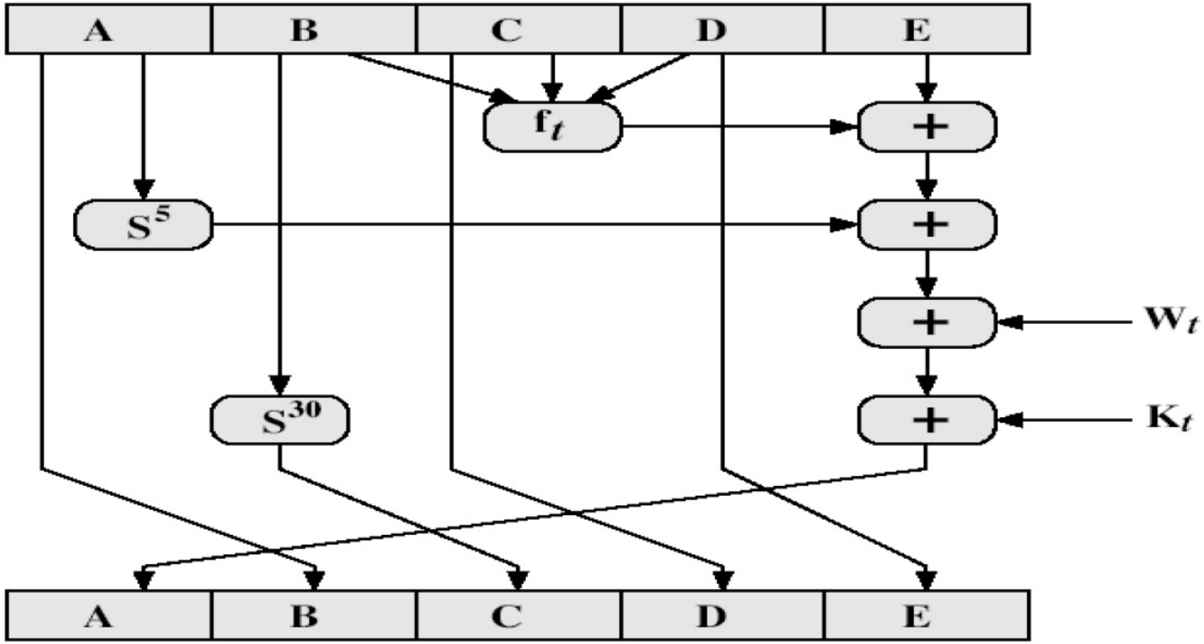
Step 5.3 :

Round	Value of t between	K[t] in Hexadecimal
1	1 and 19	5A 92 79 99
2	20 and 39	6E D9 EB A1
3	40 and 59	9F 1B BC DC
4	60 and 79	CA 62 C1 D6

Working of SHA-1

Step 5 : Process Blocks

Step 5.4 : SHA consists of 4 rounds, each consisting of 20 iterations. This makes it a total of 80 iterations.



Working of SHA-1

Step 5 : Process Blocks

Step 5.4 : Process P in each SHA-1 Round

Round	Process P
1	(b AND c) OR ((NOT b) AND (d))
2	b XOR c XOR d
3	(b AND c) OR (b AND d) OR (c AND d)
4	(b AND c) OR ((NOT b) AND (d))

Working of SHA-1

Step 5 : Process Blocks

Step 5.4 : Calculation of W[t]

The values of W[t] is calculated as follows:

For the first 16 words of W (i.e t=0 to t=15), the contents of the input message sub-block become the contents of W[t] straightaway.

Working of SHA-1

Step 5 : Process Blocks

Step 5.4 : Calculation of W[t]

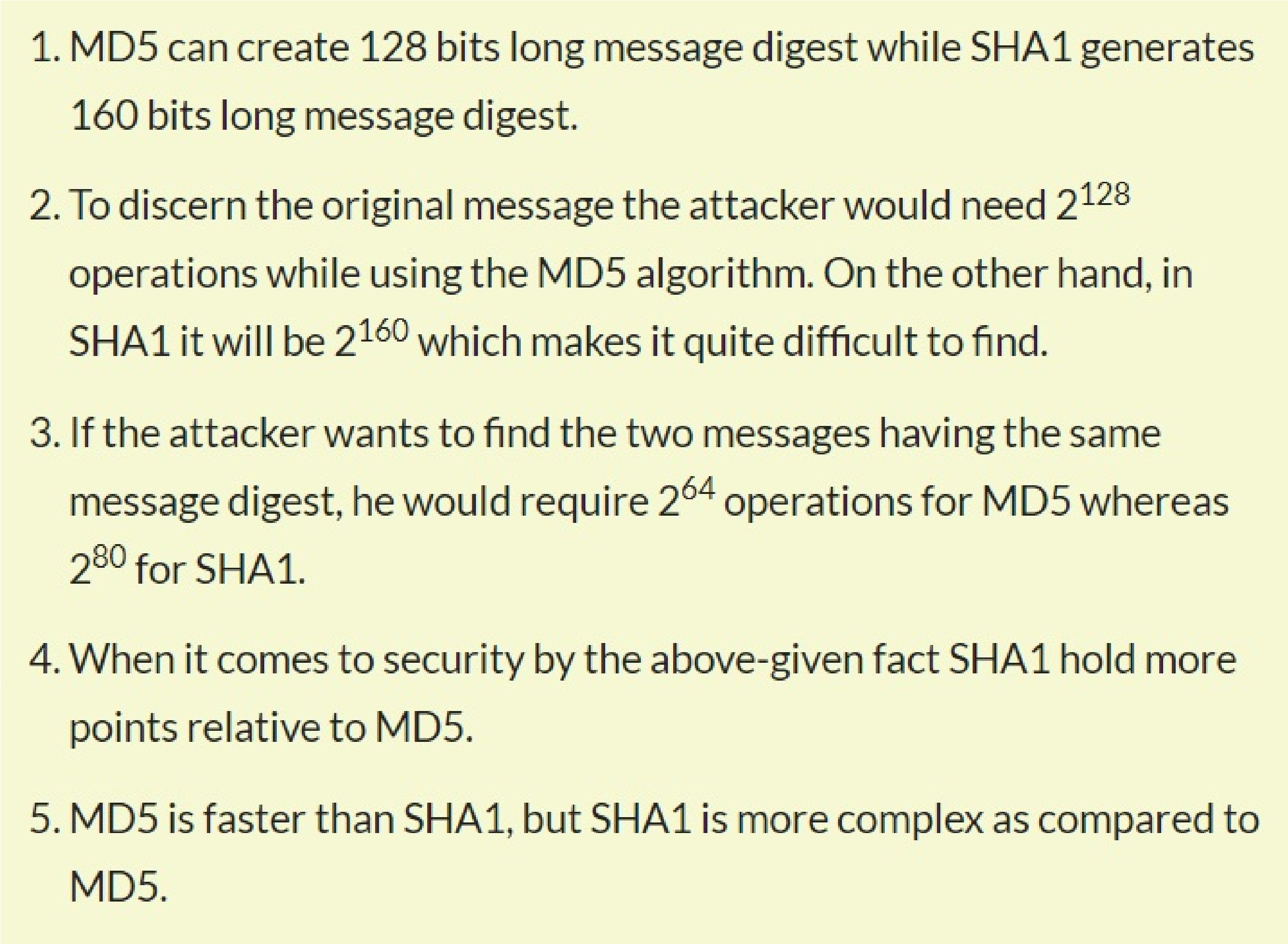
The values of W[t] is calculated as follows:

For the first 16 words of W (i.e t=0 to t=15), the contents of the input message sub-block become the contents of W[t] straightaway.

The remaining 64 values are calculated using the equation:

W[t] = s^1 (W[t-16] XOR W[t-14] XOR W[t-8] XOR W[t-3])

MD5 vs SHA-1



1. MD5 can create 128 bits long message digest while SHA1 generates 160 bits long message digest.
2. To discern the original message the attacker would need 2^{128} operations while using the MD5 algorithm. On the other hand, in SHA1 it will be 2^{160} which makes it quite difficult to find.
3. If the attacker wants to find the two messages having the same message digest, he would require 2^{64} operations for MD5 whereas 2^{80} for SHA1.
4. When it comes to security by the above-given fact SHA1 hold more points relative to MD5.
5. MD5 is faster than SHA1, but SHA1 is more complex as compared to MD5.