ASSIGNMENT 3

Title : to study and implement SHA-1 (Secure Hash Algorithm)

Theory :

Secure Hash Algorithm: SHA works with any input message that is less than 2^{64} bits in length. The output of SHA-1 is a message digest which is 160 bits in length. The word secure in SHA was decided based on two features. SHA is designed to be computationally infeasible to:
1) Obtain the original message, given its message digest
2) Find two messages producing the same message digest

Steps in SHA :

1) Padding - Add padding to the end of the original message in such a way that the length of the message is 64 bits short of multiples of 512.

2) Append length - The ~~to~~ length of the message excluding the padding ~~in~~ is calculated and appended to the end of the padding as a 64 bit block.

3) Divide the input into 512 bit block. The input message is divided into blocks of 512 bit each.

4) Initialize chaining variables - The chaining variables throughout are initialized each 32 bit in length

5) Process block :

i) Copy chaining variables A - D into variable a-e
ii) Divide the current 512 bit block into 16 sub-blocks
iii) SHA has 4 steps consisting of 20 steps each. Each round takes the current 512 bit block, the register abcde and a constant K[t] as inputs. ~~It~~ It then updates the contents of the register abcde using SHA algorithm steps.

Example :

~~Eg.~~ Input - hello world
Output - 2aae6c35c94fcfb415dbe9 54 408 b9ce91 ee846ed

Conclusion :

Thus we have thoroughly studied SHA and implemented SHA-1 using libraries.