ASSIGNMENT-3

AIM: To study & implement SHA-1

OBJECTIVE: To implement & understand details of SHA-1 (secured Hash algorithm)

THEORY:

- SHA works with any i/p message that is less than 2^{64} bits in length. The o/p of SHA-1 is a message digest which is 160 bits in length.

- Important steps in execution of SHA-1

i. Padding:
This step is add padding to the end of original message in such a way that length of message is 64 bits short of multiple of 512.

ii. Append length:
Length of message excluding length of padding is now calculated & appended to the end of padding as 64 bit block.

iii. Divide the i/p into 52 bit block.
The i/p message is now divided into blocks, 1 each of 512 bits & these blocks become the i/p to message digest processing logic.

iv. Initialise chaining variables:
5 chaining variables are initialised, each having length of 32 bits.

A	01	23	45	67
B	89	AB	CD	EF
C	FE	DC	BA	98
D	76	54	32	10
E	C3	D2	E1	F0

v. Process Block :

- Copy chaining variable E into a-e. The combination of a-e called abcde will be considered as single register for storing the results.

- Now divide the current 512 bits blocks into 16 sub blocks each ~~considering~~ consisting of 32 bits

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

$$abcde = (e + \text{process } P + S^5(a) + W[t] + K[t]),\ a,\ S^{30}(b),\ c,\ d$$

where abcde = register

P = logical operation

S^t = circular left shift of 32 bits sub blocks by t bits

$W[t]$ = A 32-bit value derived from 32 bit sub block

$K[t]$ = one of constraints defined earlier.

- Required Classes:
  Class message digest : provides applications the functionalities of messages direct algo. Message directs & secure one-way hash function that take data & output hash value.

- Required Methods:
  - getInstance (string algorithm)
    Generates message digest object that implements specific digest algorithm.

  - getInstance (string algorithm, string provider)
    Generates message digest object that Implements specific algorithm if available.

  - update (byte [] input)
    Updates digest using specified array of objects.bytes

CONCLUSION:
We learnt about SHA-1 & its working & successfully implemented it.