Roll no 43320

Date __/__/____

Saathi

Assignment 3

Aim - To study & implement SHA-1 (Secure Hash Algorithm) using libraries

Objective - To implement & understand details of SHA 1

Theory -

The Secure Hash Algorithm was developed by NIST along with NSA. There are various versions of SHA like SHA-0, SHA-1, SHA-2, SHA-3

SHA-1

1. It works for any input message that is less than 2^{64} bits
2. The output of SHA is a message digest of 160 bits of length.
3. It 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.

Page No.

Roll no 43320

Date __/__/____

Saathi

steps for execution of SHA

step I Padding

adding padding to the original message such that length of message is 64 bits short of multiple of 512 padding unit will be added even if original message, itself satisfies the criteria.

step II Append Length

Padding is appended at the end with the length of message including or excluding length of padding.

step III Divide the input into six bit block

These blocks are input to the message digest

step IV Initialize chaining variables

Each chaining variable is 32 bit in length values of chaining variable

Roll no 43320

Saathi

Date __/__/____

variable	value in hex			
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

Steps Process block

1. Copy chaining variables - E into variables a-e
2. Divide current 512 bits in 16 sub block each with 32 bits
3. SHA has 4 rounds each with 20 steps OR Iteration

Round	Value of t	K[t] in hex
1	1 and 19	5A 82 79 99
2	20 and 39	6E D9 EB A1
3	40 and 59	8F 1B BC DC
4	60 and 79	CA 62 C1 D6

4. abcde (a-e) = e + Process P + $s^5(a)$ + w [to + K[t])

where

abcde : Register made up of five variables a, b, c, d, e

Page No.

Roll no 43320

Date __/__/____

K[t] = constant

Table 1

Round	Process
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 XOR c XOR d

Calculation of w[t]

For the first 16 blocks of w (t=0 to t=15), the contents of input message sub block m[t] becomes the content of w[t]

For remaining values

w[t] = [w[t-16] XOR w[t-14] XOR w[t-8] XOR w[t-3])

Conclusion

Thus, we studied and implemented the secure Hash Algorithm i.e. SHA-I

Page No.