Assignment - 03

Roll NO : 43236

Aim :- To study and implemant the SHA - 1 (secare Hashing Algorithm)

Theory :- The national inshitende of standard thechnilogy along with NSA developed the serene hashing algorithm . SHA works with any input message that is less that 2^{64} rimits in length

SHA Parameters:-

~~SHA - 1~~

message digital size	SHA - 1	SHA - 256	SHA - 384	SHA - 512
↪	160	256	384	512
message size	$<2^{64}$	$<2^{64}$	$<2^{120}$	$<2^{128}$
Block size.	512	512	1024	1024
word size	32	32	64	64
No of rounds	80	64	80	80

Steps for SHA :-

- Padding: first step is to add padding to the digital message in 64 bit, short of multiple of 512, padding is always added

- Append Length - The length of message excluding the length of padding is calculated and appended at

- Divide the input into 512 bit block the input message is now divided into block each of length 512 bits

- Initialize variable, chaining variables A to E are initialized

Conclusion :-

In this assignment we have studied and implemented the SHA-1 algorithm