43308
Ayan Gadpal

Page :
Date : / /

Assignment 3

Aim: To study and implement the SHA-1

Theory

The national institute of standard and technology along with NSA developed the secure hashing algorithm 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.

- Steps for SHA

a) Padding

first step is to add padding to the orignal message in such a way that length of the message is 64 bit short of a multiple of 512. Padding is always added

b) Append length

The length of the message excluding the length of the padding is now calculated and appended at the end of the padding block.

c) Divide input into 512 bit block

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

d) Initialize chaining Variable

5 chaining variables A to E are initialized. Each chaining variable is 32 bits in length.

Page :
Date : / /

Required classes

i) Message digest.

It is collection of all algorithm such as MD5 or SHA. It performs all the the steps depending on the instance called.

Conclusion

We studied and implemented the SHA-1 algorithm.