Name: Anish Kulkarni
Roll Number: 43227

Page No.
Date: / /

Assignment 1.

SHA 1.

Aim: To study and implement SHA 1 (Secure Hash Algorithm)

Objective: To implement and understand details of SHA 1 (Secure Hash Algorithm).

Theory:

SHA 1 works with any message that is less than 2^{64} bits in length.
Output of SHA 1 is a message digest, 160 bits in length.

SHA is designed to be computationaly infeasible to
1. Obtain original message, given message digest.
2. Find 2 messages producing same message digest.

It consists of the following steps:

1. Padding
   Padding to make length 64 bits short of multiple of 512.
   Padding is always added.
2. Append length
   Length appended in the form of 64 bit block.
3. Divide input
   Input divided into 512 bit blocks.
4. Initialize chaining variables
   Each chaining variable has 32 bit length.
5. Process block
   Copy chaining variables E into A-E
   Divide current 512 bit block into 16 sub blocks, each of 32 bits.
   SHA has 4 rounds of 20 iterations. Each step updates current register with current block.
   Mathematical representation of iteration process

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

Name: Anish Kulkarni
Roll No. 43227

Page No. _____
Date : / /

Required classes:

1. class MessageDigest (java.security.MessageDigest)

This class provides functionalities of message digest algorithms like SHA1. Message ~~dis~~ digests are secure one way hash functions.

Required methods:

getInstance(String algorithm)
Generates message digest object of specified algorithm.

digest()
Returns hash value after applying message digest algorithm.

Conclusion:
Thus successfully studied and implemented SHA1 (Secure Hash Algorithm).