Sno:7	**Experiment name:** Digest text using the SHA-1 algorithm	**Date:**

Aim: Calculate the message digest of a text using the SHA-1 algorithm

Description: SHA-1 or Secure Hash Algorithm-1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. This hash value is known as a message digest.To calculate cryptographic hashing value in Java, Message Digest Class is used, under the package java.security.

Algorithm:

Sun provides SHA1 algorithm in Java under JCE (Java Cryptography Extension) package, which is included in JDK 1.5. Sun's implementation of SHA1 can be accessed through a generic class called MessageDigest.

Here are the some main methods of MessageDigest class:

- getInstance("SHA1") - Returns a message digest object represents a specific implementation of SHA1 algorithm.
- getProvider() - Returns the provider name.
- update(bytes) - Updates the input message by appending a byte array at the end.
- digest() - Performs SHA1 algorithm on the current input message and returns the message digest as a byte array.
- reset() - Resets the input message to an empty byte string format.

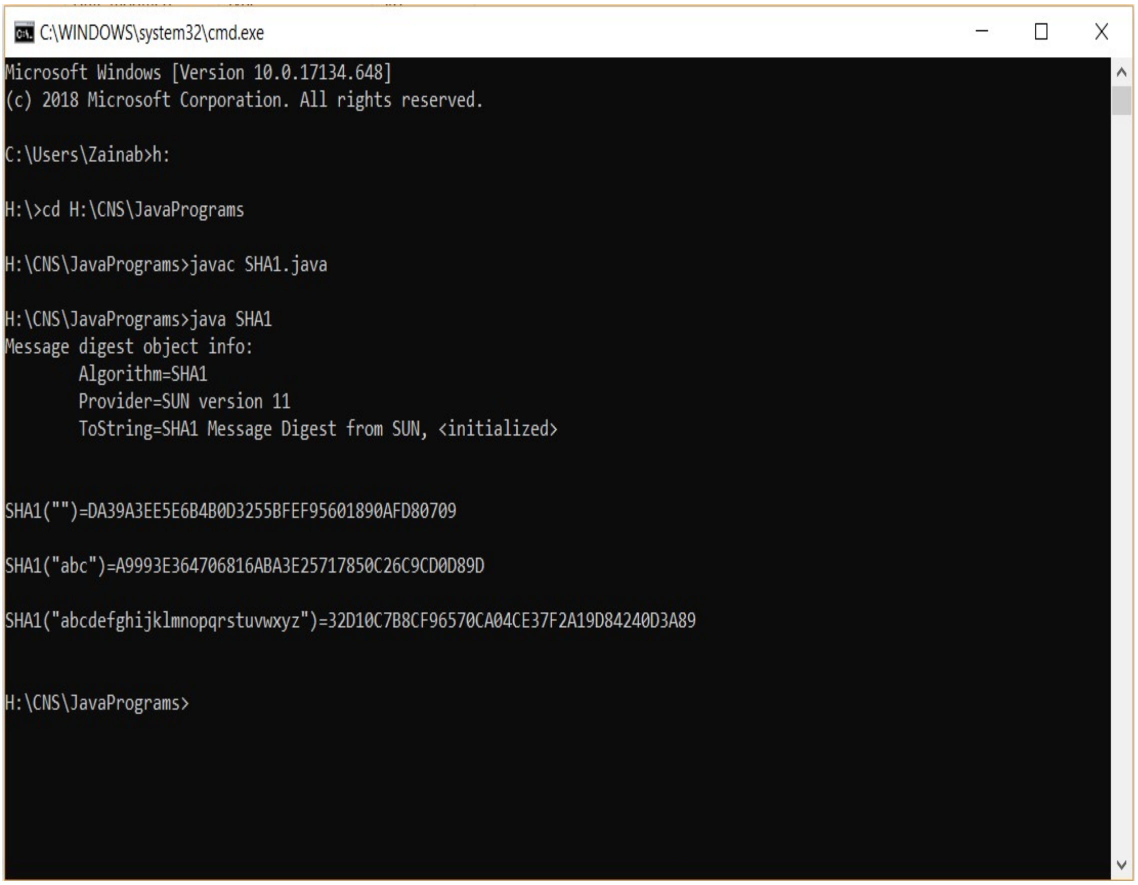
Here we have implemented SHA – 1 using JAVA Programming Language here is the snap view and prototype of SHA program. The program inherited by java.security and basis class of security features

Source Code:

```
import java.security.*;
class SHA1
{
        public static void main(String[] a)
        {
                try
                {
                        MessageDigest mds = MessageDigest.getInstance("SHA1");
                        System.out.println("Message digest: ");
                        System.out.println(" Used Algorithm =
                        "+mds.getAlgorithm());
```

```
            System.out.println(" Provider for the algorithm =
            "+mds.getProvider());
            System.out.println(" Convert it toString =
            "+mds.toString());
            String input = ""; mds.update(input.getBytes());
            byte[] output = mds.digest();
            System.out.print("SHA1(\""+input+"\") =");
            System.out.println(" "+bytesToHex(output));
            input = "abcd"; md.update(input.getBytes());
            output = mds.digest();
            System.out.print("SHA1(\""+input+"\") =");
            System.out.println(" "+bytesToHex(output));
            input = "1234567890";
            mds.update(input.getBytes());
            output = mds.digest();
            System.out.print("SHA1(\""+input+"\") =");
            System.out.println(" "+bytesToHex(output));
        }
        catch (Exception e)
        {
            System.out.println("Exception: "+e);
        }
    }
    public static String bytesToHex(byte[] b)
    {
        char hexDigit[] = {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C',
        'D', 'E', 'F'};
        StringBuffer buf = new StringBuffer();
        for (int j=0; j<b.length; j++)
        {
            buf.append(hexDigit[(b[j] >> 4) & 0x0f]);
            buf.append(hexDigit[b[j] & 0x0f]);
        } //return the elements inside the buffer
        return buf.toString();
    }
}
```

Output:



```
Microsoft Windows [Version 10.0.17134.648]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Zainab>h:

H:\>cd H:\CNS\JavaPrograms

H:\CNS\JavaPrograms>javac SHA1.java

H:\CNS\JavaPrograms>java SHA1
Message digest object info:
        Algorithm=SHA1
        Provider=SUN version 11
        ToString=SHA1 Message Digest from SUN, <initialized>


SHA1("")=DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

SHA1("abc")=A9993E364706816ABA3E25717850C26C9CD0D89D

SHA1("abcdefghijklmnopqrstuvwxyz")=32D10C7B8CF96570CA04CE37F2A19D84240D3A89


H:\CNS\JavaPrograms>
```

Result: Successfully completed SHA -1 algorithm.