

**Ex. No : 7**

**Date :**

## **SHA-1 Algorithm**

### **AIM:**

To Calculate the message digest of a text using the SHA-1 algorithm.

### **ALGORITHM:**

1. Append Padding Bits
2. Append Length - 64 bits are appended to the end
3. Prepare Processing Functions
4. Prepare Processing Constants
5. Initialize Buffers
6. Processing Message in 512-bit blocks (L blocks in total message)

### **PROGRAM:**

*sha1.java*

```
import java.security.*;
```

```
public class sha1 {  
    public static void main(String[] a) {  
        try {  
            MessageDigest md = MessageDigest.getInstance("SHA1");  
            System.out.println("Message digest object info:\n-----");  
            System.out.println("Algorithm=" + md.getAlgorithm());  
            System.out.println("Provider=" + md.getProvider());  
            System.out.println("ToString=" + md.toString());  
            String input = "";  
            md.update(input.getBytes());  
            byte[] output = md.digest();  
            System.out.println();  
            System.out.println("SHA1(\"" + input + "\")=" + bytesToHex(output));  
            input = "abc";  
            md.update(input.getBytes());  
            output = md.digest();  
            System.out.println();  
            System.out.println("SHA1(\"" + input + "\")=" + bytesToHex(output));  
            input = "abcdefghijklmnopqrstuvwxy";  
            md.update(input.getBytes());
```

```

        output = md.digest();
        System.out.println();
        System.out.println("SHA1(\"" + input + "\")=" + bytesToHex(output));
        System.out.println();
    } catch (Exception e) {
        System.out.println("Exception:" + e);
    }
}

private 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 (byte aB : b) {
        buf.append(hexDigit[(aB >> 4) & 0x0f]);
        buf.append(hexDigit[aB & 0x0f]);
    }

    return buf.toString();
}
}

```

### OUTPUT:

Message digest object info:

```

-----
Algorithm=SHA1
Provider=SUN version 12
ToString=SHA1 Message Digest from SUN, <initialized>

```

SHA1("")=DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

SHA1("abc")=A9993E364706816ABA3E25717850C26C9CD0D89D

SHA1("abcdefghijklmnopqrstuvwxyz")=32D10C7B8CF96570CA04CE37F2A19D84240D3A89

### RESULT:

Thus the *Secure Hash Algorithm (SHA-1)* has been implemented and the output has been verified successfully.