GHARDA FOUNDATION'S

GHARDA INSTITUTE OF TECHNOLOGY

Department of Computer Engineering

Evaluation Sheet

Class: T.E Computer Engineering **Sem:** VI

Subject: Cryptography and System Security

Experiment No: 9

Date:

Title of Experiment: For varying message sizes, test integrity of message using MD-5, SHA-1 and analyse the performance of the two protocols. Use crypt APIs.

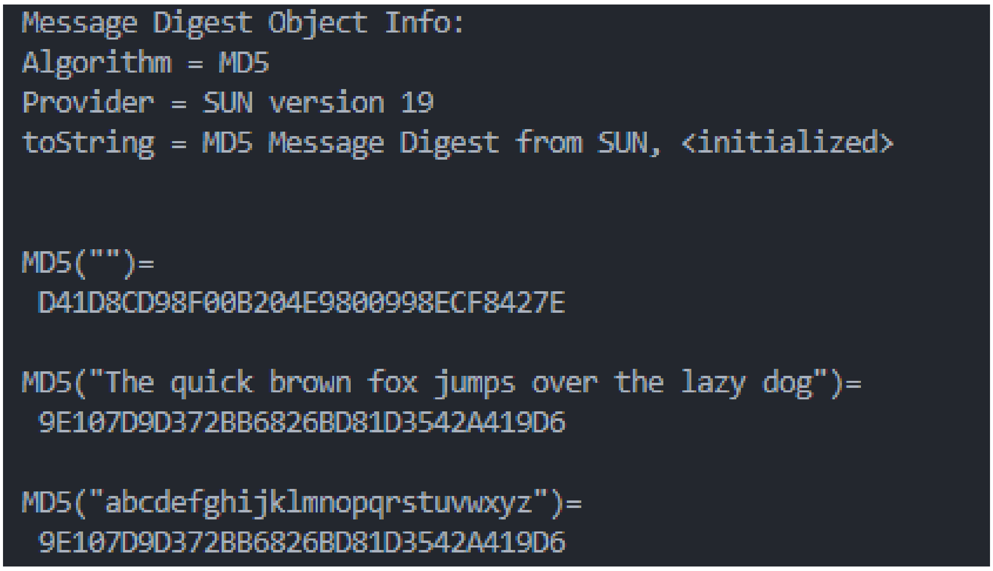
Sr. No.	Evaluation Criteria	Max Marks	Marks Obtained
1	Practical Performance	12	
2	Oral	2	
3	Timely Submission	1	
	Total	15	

Signature of Subject Teacher
[Vijesh M.Nair]

Program Code –

```
package Code;
import java.security.*;

class md5 {
    public static void main(String[] a) {

        try {
            MessageDigest md = MessageDigest.getInstance("MD5");
            System.out.println("Message Digest Object Info: ");
            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("MD5(\"" + input + "\")=");
            System.out.println(" " + bytesToHex(output));

            input = "The quick brown fox jumps over the lazy dog";
            md.update(input.getBytes());
            output = md.digest();
            System.out.println();
            System.out.println("MD5(\"" + input + "\")=");
            System.out.println(" " + bytesToHex(output));

            input = "abcdefghijklmnopqrstuvwxyz";
            md.update(input.getBytes());
            System.out.println();
            System.out.println("MD5(\"" + 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 buf.toString();
    }
}
```

Output –



```
Message Digest Object Info:
Algorithm = MD5
Provider = SUN version 19
toString = MD5 Message Digest from SUN, <initialized>


MD5("")=
 D41D8CD98F00B204E9800998ECF8427E

MD5("The quick brown fox jumps over the lazy dog")=
 9E107D9D372BB6826BD81D3542A419D6

MD5("abcdefghijklmnopqrstuvwxyz")=
 9E107D9D372BB6826BD81D3542A419D6
```