Practical No.7

Name: Bhairavi Narendra Rewatkar

Roll No.: DMET1221006

Subject: Blockchain Technology Laboratory

Date: 23/12/2024

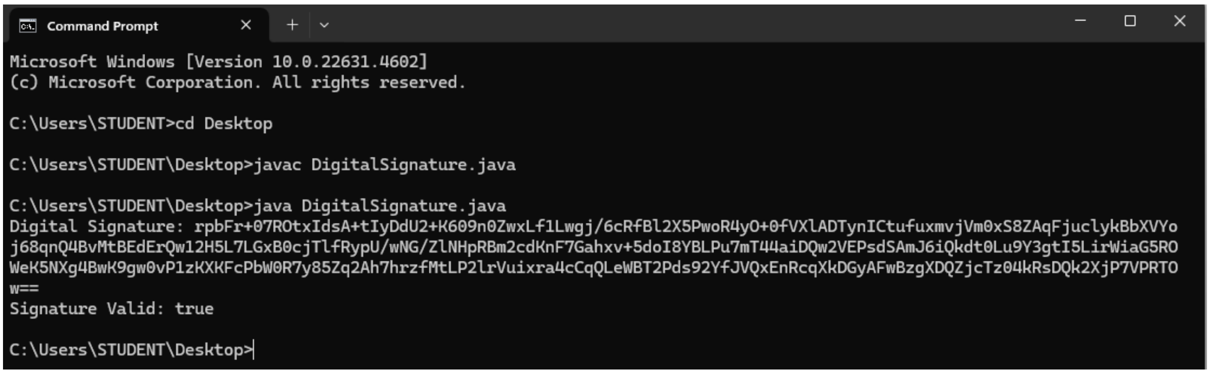
Title: Digital Signatures using Libraries

Aim: Write a program to implement digital signatures using java's cryptography libraries.

Source Code:

```
import java.security.*;
import java.util.Base64;

public class DigitalSignature {

    // Generate a key pair (public and private keys)
    public static KeyPair generateKeyPair() throws Exception {
        KeyPairGenerator keyGen = KeyPairGenerator.getInstance("RSA");
        keyGen.initialize(2048);
        return keyGen.generateKeyPair();
    }

    // Sign data using the private key
    public static byte[] signData(String data, PrivateKey privateKey) throws Exception {
        Signature signature = Signature.getInstance("SHA256withRSA");
        signature.initSign(privateKey);
        signature.update(data.getBytes("UTF8"));
        return signature.sign();
    }

    // Verify the signature using the public key
    public static boolean verifySignature(String data, byte[] signatureBytes, PublicKey publicKey)
throws Exception {
        Signature signature = Signature.getInstance("SHA256withRSA");
        signature.initVerify(publicKey);
        signature.update(data.getBytes("UTF8"));
        return signature.verify(signatureBytes);
    }

    public static void main(String[] args) throws Exception {
        // Generate a key pair
        KeyPair keyPair = generateKeyPair();
        String transaction = "Alice pays Bob 100 coins";

        // Sign the transaction
        byte[] signature = signData(transaction, keyPair.getPrivate());
        System.out.println("Digital Signature: " + Base64.getEncoder().encodeToString(signature));

        // Verify the transaction
        boolean isCorrect = verifySignature(transaction, signature, keyPair.getPublic());
        System.out.println("Signature Valid: " + isCorrect);
    }
}
```

Output:



```
Microsoft Windows [Version 10.0.22631.4602]
(c) Microsoft Corporation. All rights reserved.

C:\Users\STUDENT>cd Desktop

C:\Users\STUDENT\Desktop>javac DigitalSignature.java

C:\Users\STUDENT\Desktop>java DigitalSignature.java
Digital Signature: rpbFr+07ROtxIdsA+tIyDdU2+K609n0ZwxLf1Lwgj/6cRfBl2X5PwoR4yO+0fVXlADTynICtufuxmvjVm0xS8ZAqFjuclykBbXVYo
j68qnQ4BvMtBEdErQw12H5L7LGxB0cjTlfRypU/wNG/ZlNHpRBm2cdKnF7Gahxv+5doI8YBLPu7mT44aiDQw2VEPsdSAmJ6iQkdt0Lu9Y3gtI5LirWiaG5RO
WeK5NXg4BwK9gw0vP1zKXKFcPbW0R7y85Zq2Ah7hrzfMtLP2lrVuixra4cCqQLeWBT2Pds92YfJVQxEnRcqXkDGyAFwBzgXDQZjcTz04kRsDQk2XjP7VPRTO
w==
Signature Valid: true

C:\Users\STUDENT\Desktop>
```