Name: Mohan Ramchandra Patil
Reg. No : 19141267

IS Exp9:Implement Digital Signature Standard Algorithm

Code:

```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.Signature;
import java.util.Scanner;
public class DigitalSignature {
public static void main(String args[]) throws Exception {
Scanner sc = new Scanner(System.in);
System.out.println("Enter some text");
String msg = sc.nextLine();
KeyPairGenerator keyPairGen = KeyPairGenerator.getInstance("DSA");
keyPairGen.initialize(2048);
KeyPair pair = keyPairGen.generateKeyPair();
PrivateKey privKey = pair.getPrivate();
Signature sign = Signature.getInstance("SHA256withDSA");
sign.initSign(privKey);
byte[] bytes = "msg".getBytes();
sign.update(bytes);
byte[] signature = sign.sign();
System.out.println("Digital signature for given text: "+new String(signature, "UTF8"));
System.out.println("Digital Signature is Verified");
} }
```

Output:

```
PS C:\Users\mohan\Desktop\sub codes\is codes\9> javac DigitalSignature.java
PS C:\Users\mohan\Desktop\sub codes\is codes\9> java DigitalSignature
Enter some text
mohanpatil
Digital signature for given text: 0=☻L?????X??P?????????9"!?uv|?☻↔??|?m083??S??E
??Y|'??♦`??
Digital Signature is Verified
```