Ex. No : 8 Date :	Digital Signature Standard

AIM:

To implement the SIGNATURE SCHEME - Digital Signature Standard.

ALGORITHM:

1. Create a KeyPairGenerator object.
2. Initialize the KeyPairGenerator object.
3. Generate the KeyPairGenerator. ...
4. Get the private key from the pair.
5. Create a signature object.
6. Initialize the Signature object.
7. Add data to the Signature object
8. Calculate the Signature

PROGRAM:

```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.Signature;
import java.util.Scanner;

public class CreatingDigitalSignature {
  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"));
   }
}
```

OUTPUT:

```
Enter some text
Hi how are you
Digital signature for given text: 0=@gRD???-?.???? /yGL?i??a!?
```

RESULT:

Thus the Digital Signature Standard Signature Scheme has been implemented and the output has been verified successfully.