Ex. No : 3 Date :	Data Encryption Standard (DES) Algorithm (User Message Encryption)

AIM:

To use Data Encryption Standard (DES) Algorithm for a practical application like User Message Encryption.

ALGORITHM:

1. Create a DES Key.
2. Create a Cipher instance from Cipher class, specify the following information and separated by a slash (/).
    a. Algorithm name
    b. Mode (optional)
    c. Padding scheme (optional)
3. Convert String into ***Byte[]*** array format.
4. Make Cipher in encrypt mode, and encrypt it with ***Cipher.doFinal()*** method.
5. Make Cipher in decrypt mode, and decrypt it with ***Cipher.doFinal()*** method.

PROGRAM:

DES.java

```
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;

public class DES
{
        public static void main(String[] argv) {

                try{
         System.out.println("Message Encryption Using DES Algorithm\n------ ");
                        KeyGenerator keygenerator = KeyGenerator.getInstance("DES");
         SecretKey myDesKey = keygenerator.generateKey();
                        Cipher desCipher;
```

```
                desCipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
                desCipher.init(Cipher.ENCRYPT_MODE, myDesKey);
                byte[] text = "Secret Information ".getBytes();
                System.out.println("Message [Byte Format] : " + text);
                System.out.println("Message : " + new String(text));
                byte[] textEncrypted = desCipher.doFinal(text);
                System.out.println("Encrypted Message: " + textEncrypted);
                desCipher.init(Cipher.DECRYPT_MODE, myDesKey);
                byte[] textDecrypted = desCipher.doFinal(textEncrypted);
                System.out.println("Decrypted Message: " + new
String(textDecrypted));

            }catch(NoSuchAlgorithmException e){
                e.printStackTrace();
            }catch(NoSuchPaddingException e){
                e.printStackTrace();
            }catch(InvalidKeyException e){
                e.printStackTrace();
            }catch(IllegalBlockSizeException e){
                e.printStackTrace();
            }catch(BadPaddingException e){
                e.printStackTrace();
            }

        }
}
```

OUTPUT:

```
Message Encryption Using DES Algorithm
------------------------------------------------------
Message [Byte Format] : [B@4dcbadb4
Message : Secret Information
Encrypted Message: [B@504bae78
Decrypted Message: Secret Information
```

RESULT:

Thus the java program for DES Algorithm has been implemented and the output verified successfully.