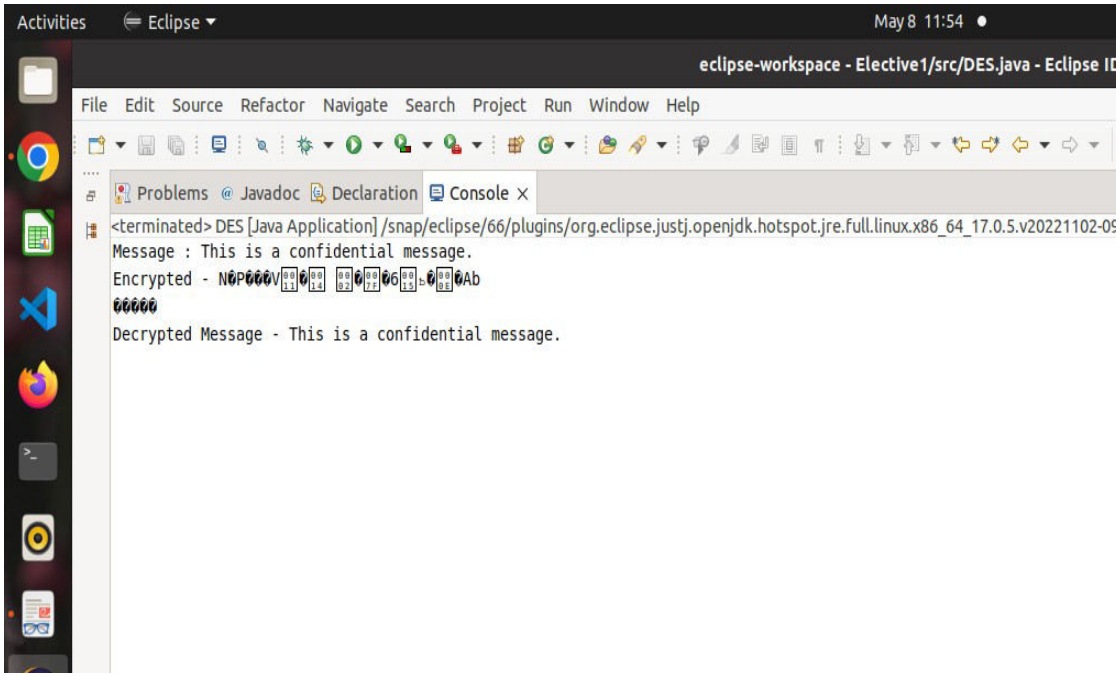
Assignment 3

Title: Data Encryption Standard (DES)

Code:

```
import java.util.*;
import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.DESKeySpec;
import java.io.*;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.spec.InvalidKeySpecException;

class DES{
    public static void main(String[] args) throws IOException,
NoSuchAlgorithmException, InvalidKeyException, InvalidKeySpecException,
NoSuchPaddingException, IllegalBlockSizeException, BadPaddingException {


        String  message="This is a confidential message.";
        byte[] myMessage =message.getBytes();


        KeyGenerator Mygenerator = KeyGenerator.getInstance("DES");
        SecretKey myDesKey = Mygenerator.generateKey();


        Cipher myCipher = Cipher.getInstance("DES");


        myCipher.init(Cipher.ENCRYPT_MODE, myDesKey);
        byte[] myEncryptedBytes=myCipher.doFinal(myMessage);



        myCipher.init(Cipher.DECRYPT_MODE, myDesKey);
        byte[] myDecryptedBytes=myCipher.doFinal(myEncryptedBytes);


        String encrypteddata=new String(myEncryptedBytes);
        String decrypteddata=new String(myDecryptedBytes);

        System.out.println("Message : "+ message);
        System.out.println("Encrypted - "+ encrypteddata);
        System.out.println("Decrypted Message - "+ decrypteddata);
    }
}
```

OUTPUT:


Activities
Eclipse
May 8 11:54
eclipse-workspace - Elective1/src/DES.java - Eclipse ID
File Edit Source Refactor Navigate Search Project Run Window Help
Problems Javadoc Declaration Console
<terminated> DES [Java Application] /snap/eclipse/66/plugins/org.eclipse.justj.openjdk.hotspot.jre.full.linux.x86_64_17.0.5.v20221102-09
Message : This is a confidential message.
Encrypted - N
Decrypted Message - This is a confidential message.