

NAME	N.AASRITH
ROLL NO	22R21A05P6
CLASS AND YEAR	CSE-D 4th YEAR 1st SEM
WEEK NUMBER	WEEK 4

**PROBLEM STATEMENT:** Write a java program to implement the DES algorithm logic.

**PROGRAM:**

```
import java.io.*;
import java.security.spec.KeySpec;
import java.util.Base64;
import javax.crypto.*;
import javax.crypto.spec.DESedeKeySpec;

public class DES {
    private static final String UNICODE_FORMAT = "UTF8";
    public static final String DESEDE_ENCRYPTION_SCHEME = "DESEde";
    private KeySpec myKeySpec;
    private SecretKeyFactory mySecretKeyFactory;
    private Cipher cipher;
    byte[] keyAsBytes;
    private String myEncryptionKey;
    private String myEncryptionScheme;
    SecretKey key;
    static BufferedReader br = new BufferedReader(new InputStreamReader(System.in));

    public DES() throws Exception {
        myEncryptionKey = "ThisIsSecretEncryptionKey"; // 24 characters = 192 bits
        myEncryptionScheme = DESEDE_ENCRYPTION_SCHEME;
        keyAsBytes = myEncryptionKey.getBytes(UNICODE_FORMAT);
        myKeySpec = new DESedeKeySpec(keyAsBytes);
        mySecretKeyFactory = SecretKeyFactory.getInstance(myEncryptionScheme);
        cipher = Cipher.getInstance(myEncryptionScheme);
        key = mySecretKeyFactory.generateSecret(myKeySpec);
    }

    public String encrypt(String unencryptedString) {
        String encryptedString = null;
        try {
            cipher.init(Cipher.ENCRYPT_MODE, key);
            byte[] plainText = unencryptedString.getBytes(UNICODE_FORMAT);
            byte[] encryptedText = cipher.doFinal(plainText);
        } catch (Exception e) {
            e.printStackTrace();
        }
        return Base64.getEncoder().encodeToString(encryptedText);
    }
}
```

```
        encryptedString = Base64.getEncoder().encodeToString(encryptedText);
    } catch (Exception e) {
        e.printStackTrace();
    }
    return encryptedString;
}

public String decrypt(String encryptedString) {
    String decryptedText = null;
    try {
        cipher.init(Cipher.DECRYPT_MODE, key);
        byte[] encryptedText = Base64.getDecoder().decode(encryptedString);
        byte[] plainText = cipher.doFinal(encryptedText);
        decryptedText = new String(plainText, UNICODE_FORMAT);
    } catch (Exception e) {
        e.printStackTrace();
    }
    return decryptedText;
}

public static void main(String[] args) throws Exception {
    System.out.print("Enter the string: ");
    String stringToEncrypt = br.readLine();
    DES myEncryptor = new DES();
    String encrypted = myEncryptor.encrypt(stringToEncrypt);
    String decrypted = myEncryptor.decrypt(encrypted);
    System.out.println("\nString To Encrypt : " + stringToEncrypt);
    System.out.println("\nEncrypted Value : " + encrypted);
    System.out.println("\nDecrypted Value : " + decrypted);
}
}
```

### Output:

#### Output

Enter the string: week4CNSlab

String To Encrypt : week4CNSlab

Encrypted Value : 7Pqvqe3nXBmBB5vtUX0XHQ==

Decrypted Value : week4CNSlab