NAME	N.AASRITH
ROLL NO	22R21A05P6
CLASS AND YEAR	CSE-D 4th YEAR 1st SEM
WEEK NUMBER	WEEK 5

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

PROGRAM:

```java
import java.io.*;
import java.security.Key;
import javax.crypto.Cipher;
import javax.crypto.CipherOutputStream;
import javax.crypto.KeyGenerator;
import java.util.Base64;
public class BlowFish {
    public static void main(String[] args) throws Exception {
        KeyGenerator keyGenerator = KeyGenerator.getInstance("Blowfish");
        keyGenerator.init(128);
        Key secretKey = keyGenerator.generateKey();
        Cipher cipherOut = Cipher.getInstance("Blowfish/CFB/NoPadding");
        cipherOut.init(Cipher.ENCRYPT_MODE, secretKey);
        Base64.Encoder encoder = Base64.getEncoder();
        byte iv[] = cipherOut.getIV();
        if (iv != null) {
            System.out.println("Initialization Vector of the Cipher: " +
encoder.encodeToString(iv));
        }
        FileInputStream fin = new
FileInputStream("C:\\Users\\ACER\\Documents\\CNSLab\\inputFile.txt");
        FileOutputStream fout = new
FileOutputStream("C:\\Users\\ACER\\Documents\\CNSLab\\outputFile.txt");
        CipherOutputStream cout = new CipherOutputStream(fout, cipherOut);
        int input;
        while ((input = fin.read()) != -1) {
            cout.write(input);
        }
        fin.close();
        cout.close();
    } }
```
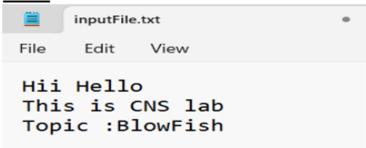
MARRI LAXMAN REDDY GROUP OF INSTITUTIONS

MLR INSTITUTE OF TECHNOLOGY
(UGC AUTONOMOUS)
Affiliated to JNTUH,Approved by AICTE
Laxman Reddy Avenue, Dundigal, Hyderabad-500 043, Telangana, India

NBA NATIONAL BOARD OF ACCREDITATION

ACCREDITED WITH GRADE A NAAC

INPUT:

inputFile.txt

File   Edit   View

Hii Hello
This is CNS lab
Topic :BlowFish

OUTPUT:

```
C:\Users\ACER\Documents\CNS Lab>javac BlowFish.java

C:\Users\ACER\Documents\CNS Lab>java BlowFish
Initialization Vector of the Cipher: xcxRDtqZc6w=
```

outputFile.txt   ×   +

File   Edit   View

⯑⯑Ã⯑⯑⯑⯑c⯑z⯑a⯑⯑%⯑q` k⯑Z8⯑n{⯑⯑k⯑F⯑⯑C⯑⯑⯑⯑y