**Practical IV**

**Roll No: 07 Date: 10/10/22**

**Aim: Program to implement AES algorithm for file encryption and decryption.**

**CODE:**

package prac3;

import java.io.BufferedReader;

import java.io.BufferedWriter;

import java.io.File;

import java.io.FileNotFoundException;

import java.io.FileReader;

import java.io.FileWriter;

import java.io.IOException;

import java.io.UnsupportedEncodingException;

import java.security.MessageDigest;

import java.security.NoSuchAlgorithmException;

import java.util.Arrays;

import javax.crypto.Cipher;

import javax.crypto.spec.SecretKeySpec;

import javax.xml.bind.DatatypeConverter;

\* @author Shubham Khedaskar

\*/

public class aespracfour {

private static SecretKeySpec secretKey;

private static byte[] key;

public static void setKey(final String myKey) {

MessageDigest sha = null;

try {

key = myKey.getBytes("UTF-8");

sha = MessageDigest.getInstance("SHA-1");

key = sha.digest(key);

key = Arrays.copyOf(key, 16);

secretKey = new SecretKeySpec(key, "AES");

} catch (NoSuchAlgorithmException | UnsupportedEncodingException e) {

e.printStackTrace();

}

}

public static String encrypt(final String strToEncrypt, final String secret) {

try {

setKey(secret);

Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");

cipher.init(Cipher.ENCRYPT\_MODE, secretKey);

return DatatypeConverter.printBase64Binary(cipher.doFinal(strToEncrypt.getBytes("UTF-8")));

//return Base64.getEncoder().encodeToString(cipher.doFinal(strToEncrypt.getBytes("UTF-8")));

} catch (Exception e) {

System.out.println("Error while encrypting: " + e.toString());

}

return null;

}

public static String decrypt(final String strToDecrypt, final String secret) {

try {

setKey(secret);

Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5PADDING");

cipher.init(Cipher.DECRYPT\_MODE, secretKey);

return new String(cipher.doFinal(DatatypeConverter.parseBase64Binary(strToDecrypt)));

} catch (Exception e) {

System.out.println("Error while decrypting: " + e.toString());

}

return null;

}

public static void main(String[] args) throws FileNotFoundException, IOException{

final String secretKey = "java";

String encryptedString; //= encrypt(originalString, secretKey) ;

String decryptedString; //= decrypt(encryptedString, secretKey) ;

//System.out.println(encryptedString);

//System.out.println(decryptedString);

File file = new File("C:\\Users\\Shubham Khedaskar\\Documents\\textreadfile.txt");

BufferedReader br = new BufferedReader(new FileReader(file));

String st;

System.out.print("--TextToBeEncrypted--\n");

while ((st = br.readLine()) != null){

System.out.println(st);

FileWriter fw=new FileWriter("C:\\Users\\Shubham Khedaskar\\Documents\\textwritefile1.txt", true);

BufferedWriter out = new BufferedWriter(fw);

encryptedString = encrypt(st, secretKey) ;

System.out.println("Encrypted String Line : "+encryptedString);

out.write(encryptedString);

out.newLine();

out.close();

fw.close();

}

System.out.print("--DecryptedText--\n");

File file1 = new File("C:\\Users\\Shubham Khedaskar\\Documents\\textwritefile1.txt");

BufferedReader br1 = new BufferedReader(new FileReader(file1));

String st1;

while ((st1 = br1.readLine()) != null){

//System.out.println(st1);

decryptedString = decrypt(st1, secretKey) ;

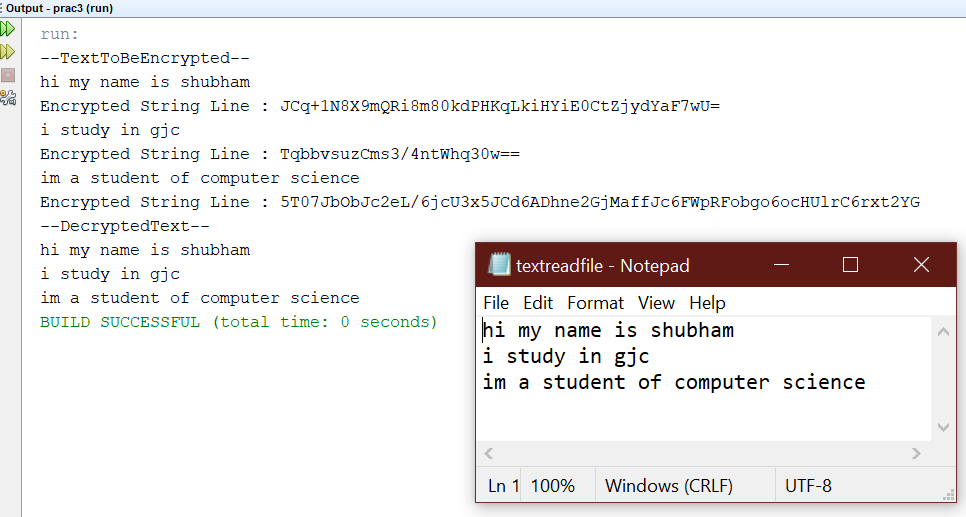
System.out.println(decryptedString);

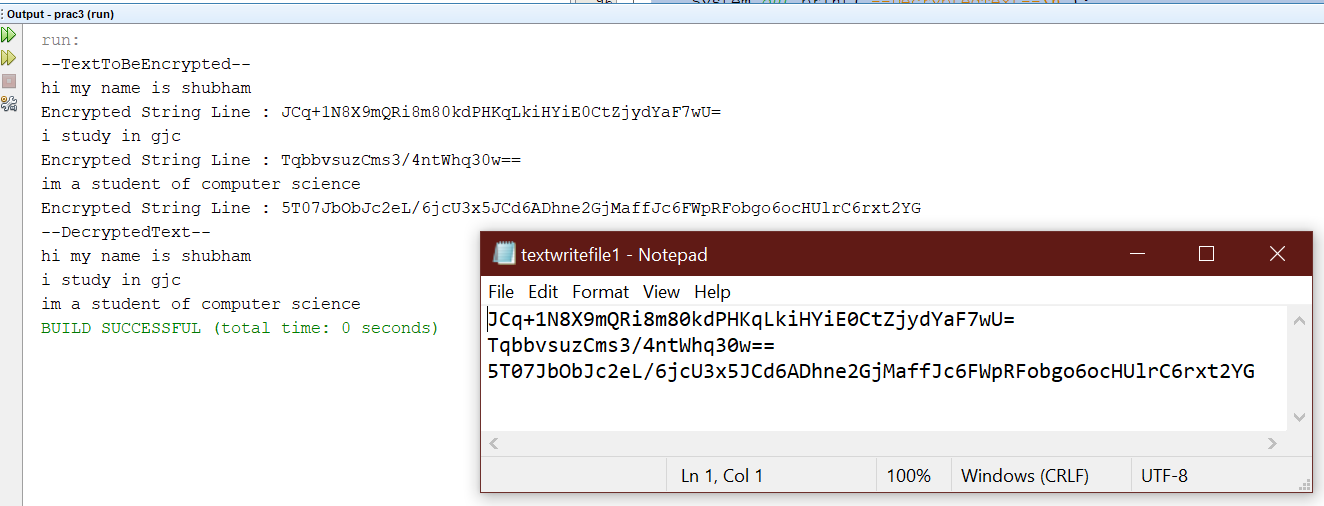
}

}

}

**OUTPUT**

****

****