Name: Rameshwar Gosavi
Roll No.: 331
Batch: B

Title: Write a Java/C/C++/Python program to implement DES algorithm

```
import java.nio.charset.StandardCharsets;
import
java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.spec.InvalidKeySpecException;
import java.util.Base64;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.DESKeySpec;
import javax.crypto.spec.IvParameterSpec;

public class DESExample {

    public static void main(String[] args) throws
Throwable {
        String plainText = "Hello, World!";
        String secretKey = "mysecret";
        String encryptedText = encrypt(plainText,
secretKey);
        String decryptedText =
decrypt(encryptedText, secretKey);
        System.out.println("Plain Text: " +
plainText);
        System.out.println("Encrypted Text: " +
encryptedText);
```

```
        System.out.println("Decrypted Text: " +
decryptedText);
    }

    public static String encrypt(String plainText,
String secretKey)
            throws NoSuchAlgorithmException,
NoSuchPaddingException, InvalidKeyException,
InvalidKeySpecException, IllegalBlockSizeException,
BadPaddingException,
InvalidAlgorithmParameterException {
        byte[] iv = { 0, 0, 0, 0, 0, 0, 0, 0 };
        IvParameterSpec ivspec = new
IvParameterSpec(iv);

        DESKeySpec keySpec = new
DESKeySpec(secretKey.getBytes(StandardCharsets.UTF_
8));
        SecretKeyFactory keyFactory =
SecretKeyFactory.getInstance("DES");
        SecretKey key =
keyFactory.generateSecret(keySpec);

        Cipher cipher =
Cipher.getInstance("DES/CBC/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, key,
ivspec);

        byte[] encryptedBytes =
cipher.doFinal(plainText.getBytes(StandardCharsets.
UTF_8));
        String encryptedText =
Base64.getEncoder().encodeToString(encryptedBytes);

        return encryptedText;
    }
```

```
    public static String decrypt(String
encryptedText, String secretKey)
            throws NoSuchAlgorithmException,
NoSuchPaddingException, InvalidKeyException,
Throwable {
        byte[] iv = { 0, 0, 0, 0, 0, 0, 0, 0 };
        IvParameterSpec ivspec = new
IvParameterSpec(iv);

        DESKeySpec keySpec = new
DESKeySpec(secretKey.getBytes(StandardCharsets.UTF_
8));
        SecretKeyFactory keyFactory =
SecretKeyFactory.getInstance("DES");
        SecretKey key =
keyFactory.generateSecret(keySpec);

        Cipher cipher =
Cipher.getInstance("DES/CBC/PKCS5Padding");
        cipher.init(Cipher.DECRYPT_MODE, key,
ivspec);

        byte[] encryptedBytes =
Base64.getDecoder().decode(encryptedText);
        byte[] decryptedBytes =
cipher.doFinal(encryptedBytes);
        String decryptedText = new
String(decryptedBytes, StandardCharsets.UTF_8);

        return decryptedText;
    }

}
```