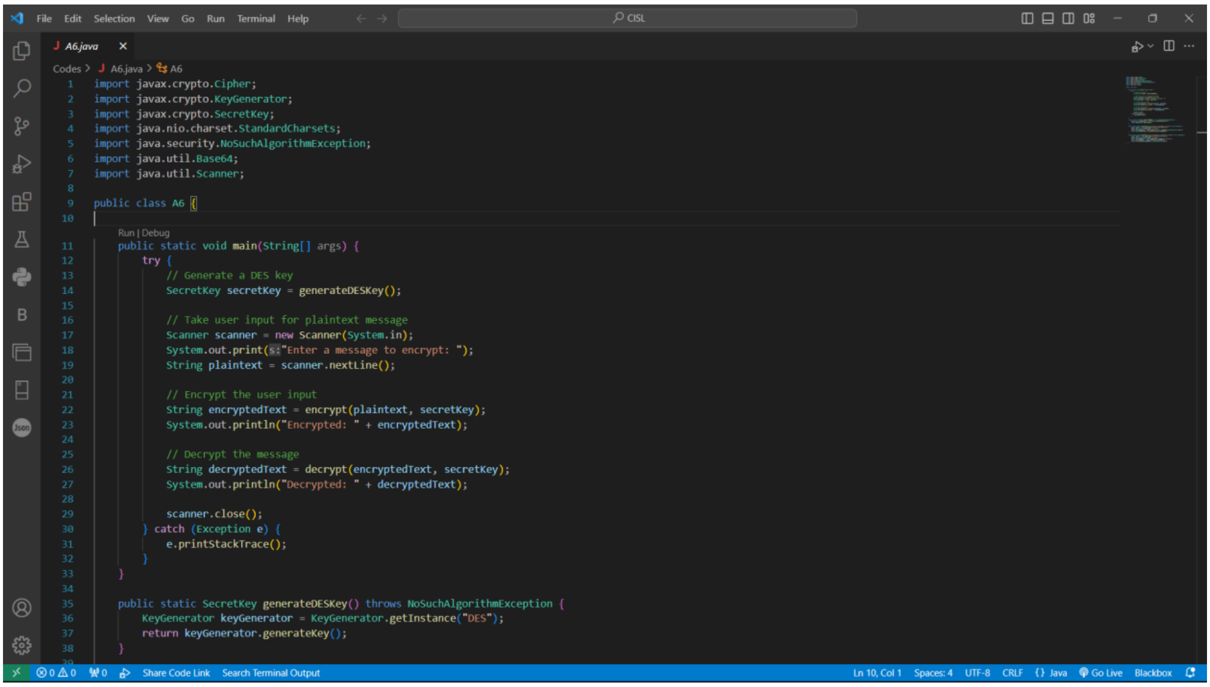
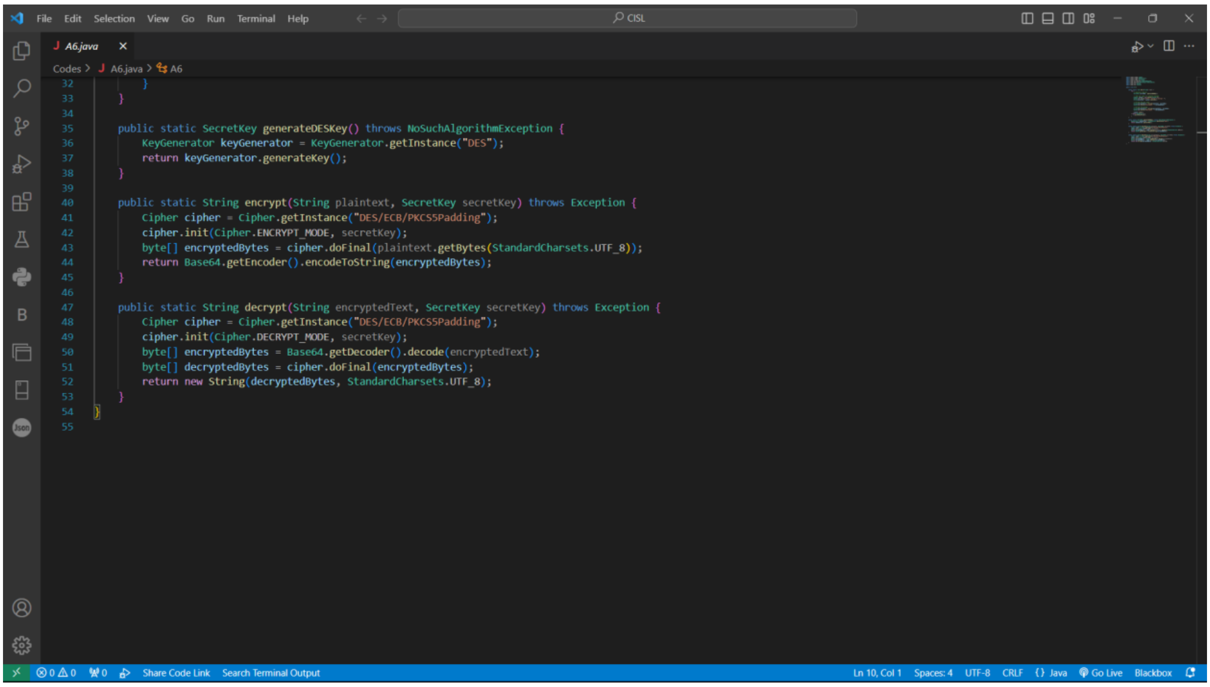
6. Write a Java program to implement the DES algorithm logic.

Program:

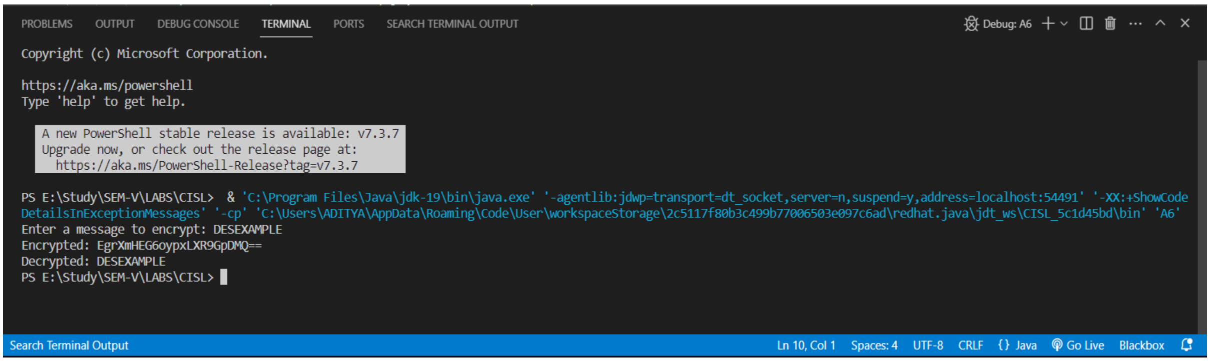


```java
import javax.crypto.Cipher;
import javax.crypto.KeyGenerator;
import javax.crypto.SecretKey;
import java.nio.charset.StandardCharsets;
import java.security.NoSuchAlgorithmException;
import java.util.Base64;
import java.util.Scanner;

public class A6 {

    public static void main(String[] args) {
        try {
            // Generate a DES key
            SecretKey secretKey = generateDESKey();

            // Take user input for plaintext message
            Scanner scanner = new Scanner(System.in);
            System.out.print(s:"Enter a message to encrypt: ");
            String plaintext = scanner.nextLine();

            // Encrypt the user input
            String encryptedText = encrypt(plaintext, secretKey);
            System.out.println("Encrypted: " + encryptedText);

            // Decrypt the message
            String decryptedText = decrypt(encryptedText, secretKey);
            System.out.println("Decrypted: " + decryptedText);

            scanner.close();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    public static SecretKey generateDESKey() throws NoSuchAlgorithmException {
        KeyGenerator keyGenerator = KeyGenerator.getInstance("DES");
        return keyGenerator.generateKey();
    }
```



```java
        }
    }

    public static SecretKey generateDESKey() throws NoSuchAlgorithmException {
        KeyGenerator keyGenerator = KeyGenerator.getInstance("DES");
        return keyGenerator.generateKey();
    }

    public static String encrypt(String plaintext, SecretKey secretKey) throws Exception {
        Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
        cipher.init(Cipher.ENCRYPT_MODE, secretKey);
        byte[] encryptedBytes = cipher.doFinal(plaintext.getBytes(StandardCharsets.UTF_8));
        return Base64.getEncoder().encodeToString(encryptedBytes);
    }

    public static String decrypt(String encryptedText, SecretKey secretKey) throws Exception {
        Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
        cipher.init(Cipher.DECRYPT_MODE, secretKey);
        byte[] encryptedBytes = Base64.getDecoder().decode(encryptedText);
        byte[] decryptedBytes = cipher.doFinal(encryptedBytes);
        return new String(decryptedBytes, StandardCharsets.UTF_8);
    }
}
```

Output:



```
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

   A new PowerShell stable release is available: v7.3.7
   Upgrade now, or check out the release page at:
     https://aka.ms/PowerShell-Release?tag=v7.3.7

PS E:\Study\SEM-V\LABS\CISL>  & 'C:\Program Files\Java\jdk-19\bin\java.exe' '-agentlib:jdwp=transport=dt_socket,server=n,suspend=y,address=localhost:54491' '-XX:+ShowCode
DetailsInExceptionMessages' '-cp' 'C:\Users\ADITYA\AppData\Roaming\Code\User\workspaceStorage\2c5117f80b3c499b77006503e097c6ad\redhat.java\jdt_ws\CISL_5c1d45bd\bin' 'A6'
Enter a message to encrypt: DESEXAMPLE
Encrypted: EgrXmHEG6oypxLXR9GpDMQ==
Decrypted: DESEXAMPLE
PS E:\Study\SEM-V\LABS\CISL> 
```