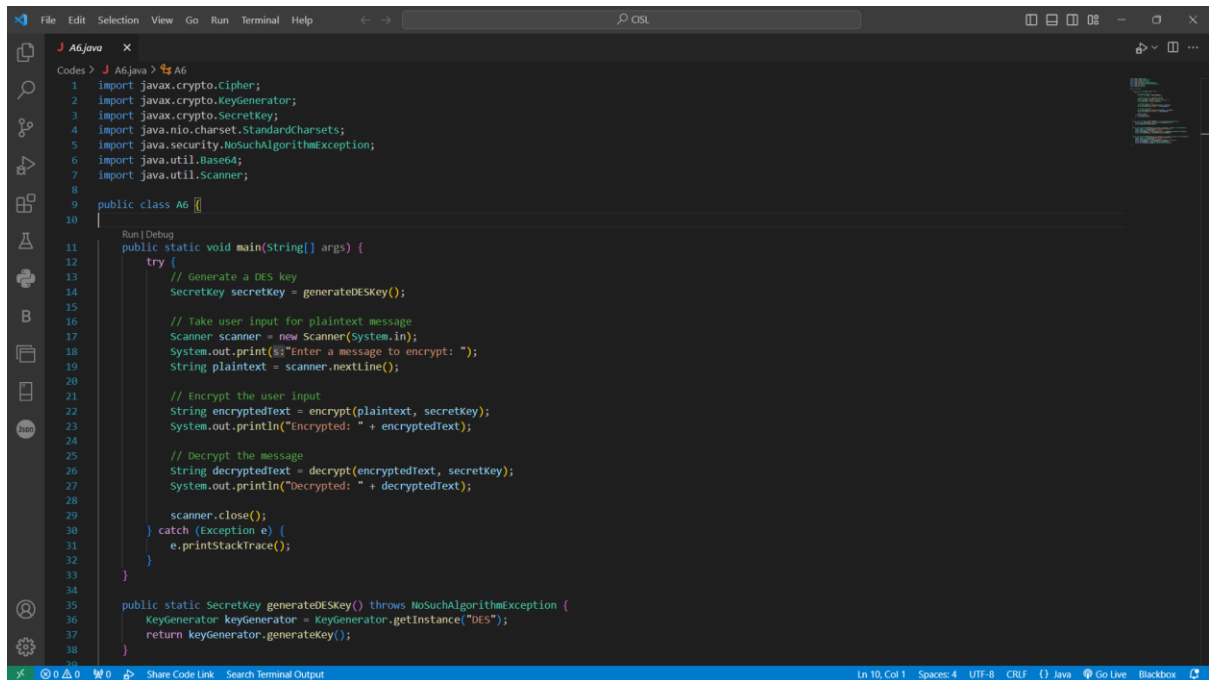
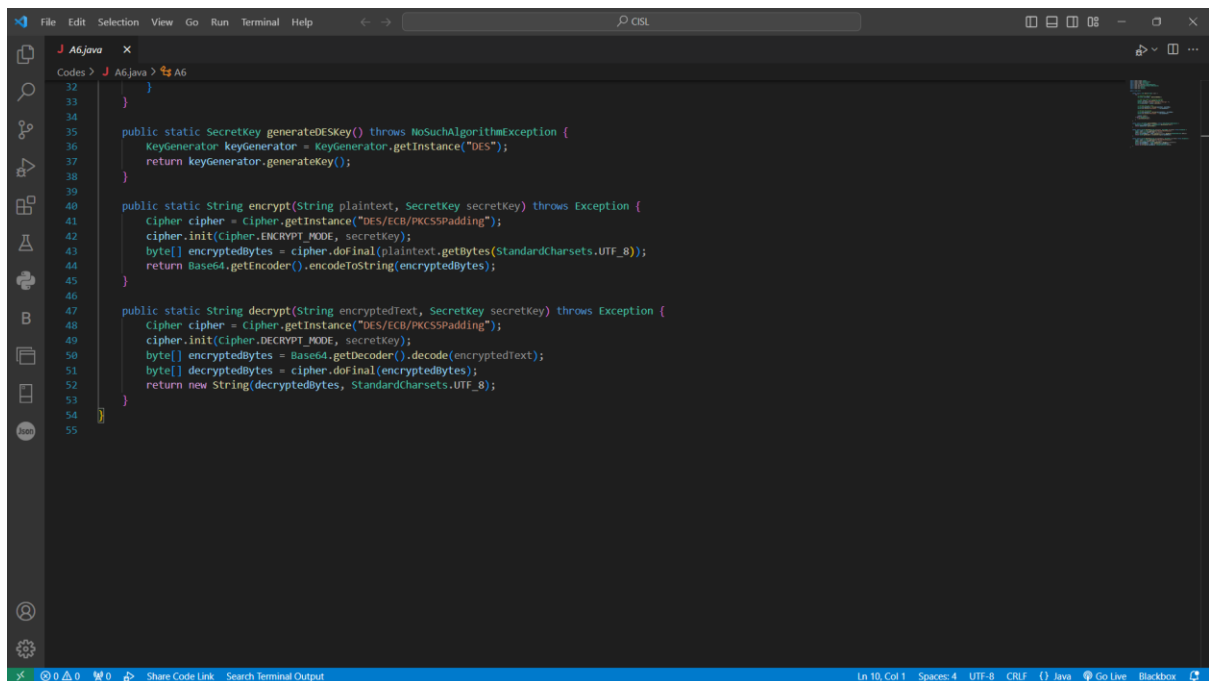


6. Write a Java program to implement the DES algorithm logic.

Program:

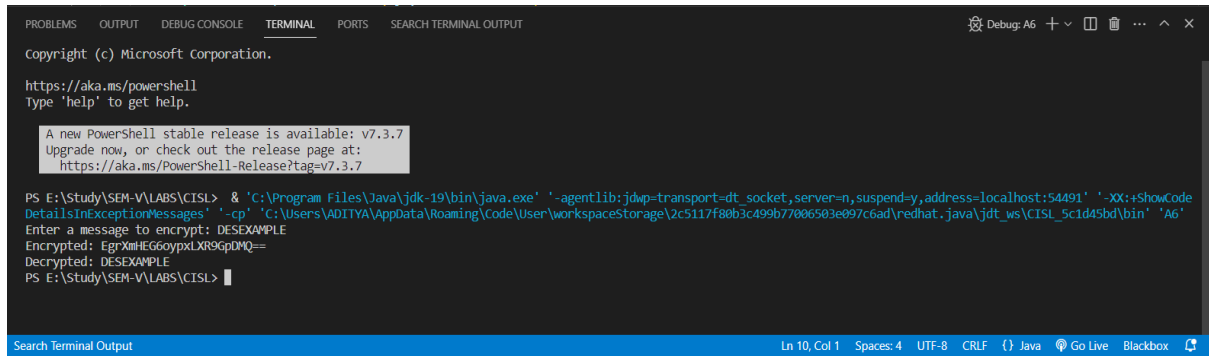


```
1 import javax.crypto.Cipher;
2 import javax.crypto.KeyGenerator;
3 import javax.crypto.SecretKey;
4 import java.nio.charset.StandardCharsets;
5 import java.security.NoSuchAlgorithmException;
6 import java.util.Base64;
7 import java.util.Scanner;
8
9 public class A6 {
10
11     Run | Debug
12     public static void main(String[] args) {
13         try {
14             // Generate a DES key
15             SecretKey secretKey = generateDESKey();
16
17             // Take user input for plaintext message
18             Scanner scanner = new Scanner(System.in);
19             System.out.print("Enter a message to encrypt: ");
20             String plaintext = scanner.nextLine();
21
22             // Encrypt the user input
23             String encryptedText = encrypt(plaintext, secretKey);
24             System.out.println("Encrypted: " + encryptedText);
25
26             // Decrypt the message
27             String decryptedText = decrypt(encryptedText, secretKey);
28             System.out.println("Decrypted: " + decryptedText);
29
30             scanner.close();
31         } catch (Exception e) {
32             e.printStackTrace();
33         }
34     }
35
36     public static SecretKey generateDESKey() throws NoSuchAlgorithmException {
37         KeyGenerator keyGenerator = KeyGenerator.getInstance("DES");
38         return keyGenerator.generateKey();
39     }
40 }
```



```
32 }
33
34
35 public static SecretKey generateDESKey() throws NoSuchAlgorithmException {
36     KeyGenerator keyGenerator = KeyGenerator.getInstance("DES");
37     return keyGenerator.generateKey();
38 }
39
40 public static String encrypt(String plaintext, SecretKey secretKey) throws Exception {
41     Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
42     cipher.init(Cipher.ENCRYPT_MODE, secretKey);
43     byte[] encryptedBytes = cipher.doFinal(plaintext.getBytes(StandardCharsets.UTF_8));
44     return Base64.getEncoder().encodeToString(encryptedBytes);
45 }
46
47 public static String decrypt(String encryptedText, SecretKey secretKey) throws Exception {
48     Cipher cipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
49     cipher.init(Cipher.DECRYPT_MODE, secretKey);
50     byte[] encryptedBytes = Base64.getDecoder().decode(encryptedText);
51     byte[] decryptedBytes = cipher.doFinal(encryptedBytes);
52     return new String(decryptedBytes, StandardCharsets.UTF_8);
53 }
54
55 }
```

Output:



The screenshot shows a Visual Studio Code terminal window with the following content:

```
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:+ShowCodeDetailsInExceptionMessages' '-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: EgrXmmHEG6oypxLXR9GpDMQ==
Decrypted: DESEXAMPLE
PS E:\Study\SEM-V\LABS\CISL> |
```

The terminal window has a blue status bar at the bottom with the text "Search Terminal Output" on the left and "Ln 10, Col 1 Spaces: 4 UTF-8 CRLF {} Java Go Live Blackbox" on the right.