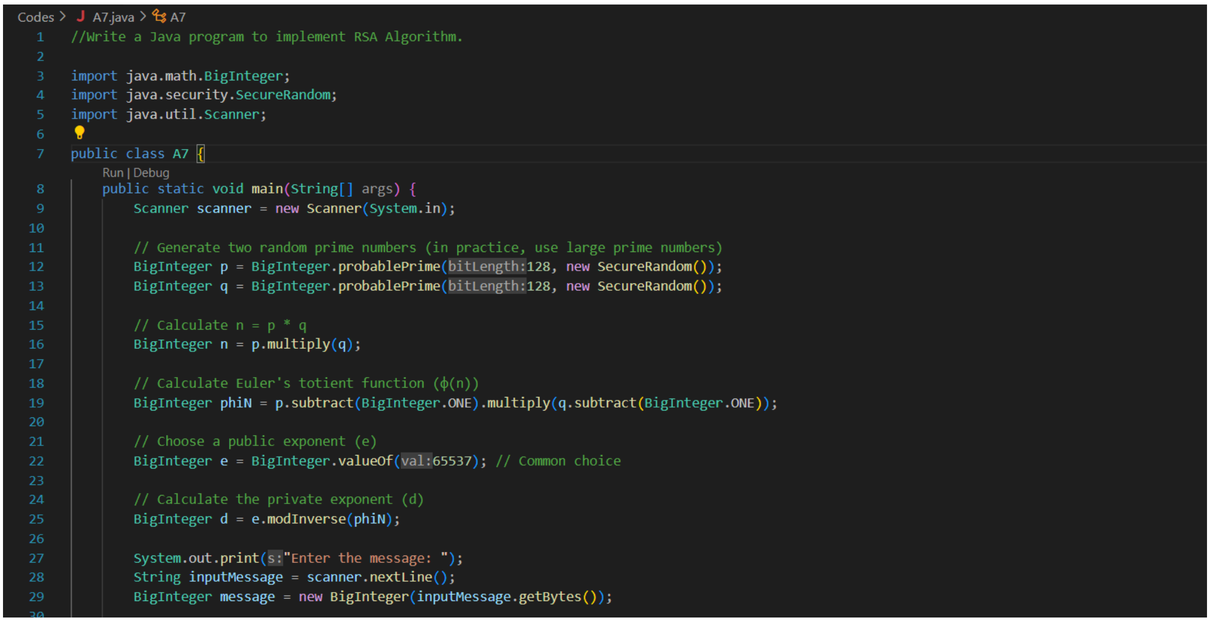
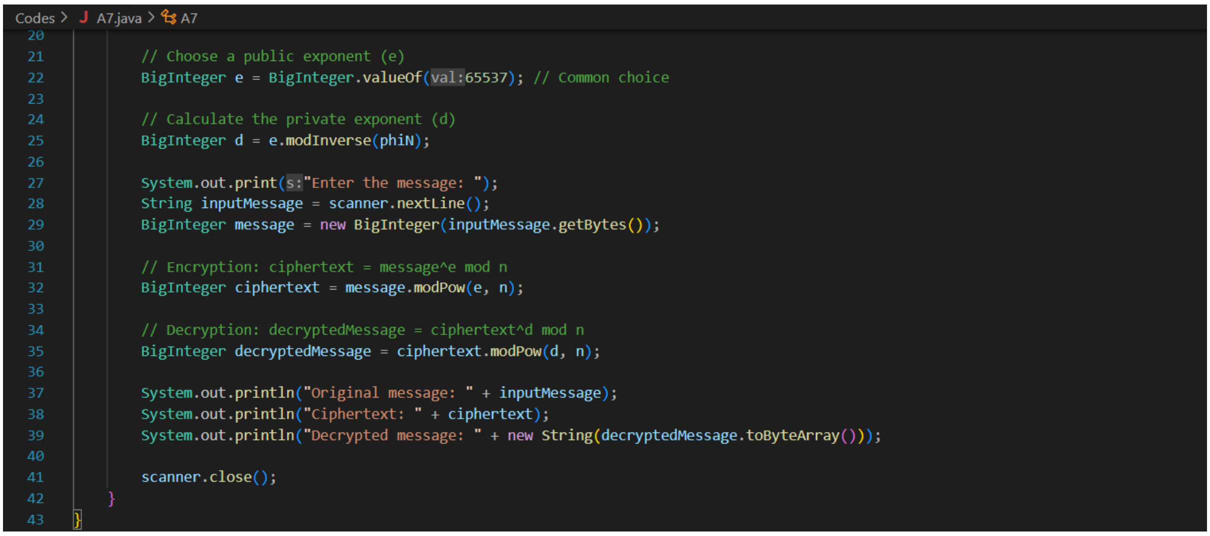
7. Write a Java program to implement the DES algorithm logic.

Code:



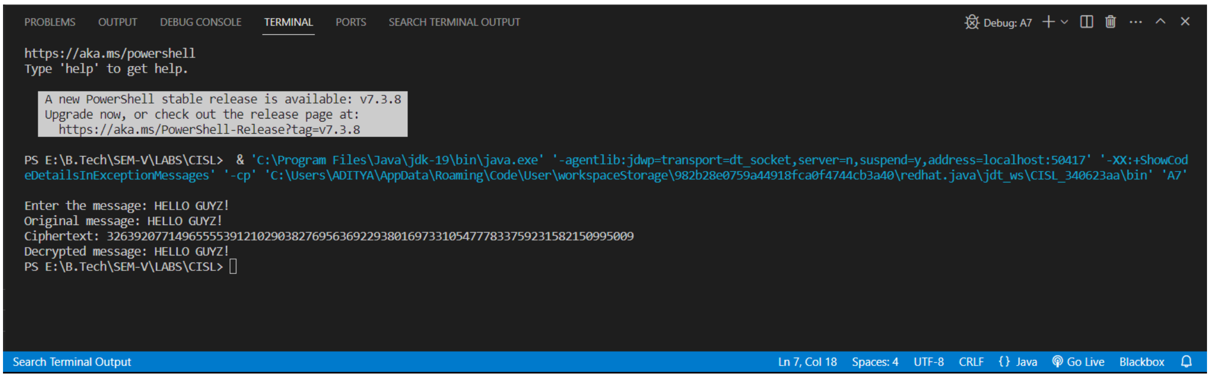
```java
//Write a Java program to implement RSA Algorithm.

import java.math.BigInteger;
import java.security.SecureRandom;
import java.util.Scanner;

public class A7 {
    Run | Debug
    public static void main(String[] args) {
        Scanner scanner = new Scanner(System.in);

        // Generate two random prime numbers (in practice, use large prime numbers)
        BigInteger p = BigInteger.probablePrime(bitLength:128, new SecureRandom());
        BigInteger q = BigInteger.probablePrime(bitLength:128, new SecureRandom());

        // Calculate n = p * q
        BigInteger n = p.multiply(q);

        // Calculate Euler's totient function (ϕ(n))
        BigInteger phiN = p.subtract(BigInteger.ONE).multiply(q.subtract(BigInteger.ONE));

        // Choose a public exponent (e)
        BigInteger e = BigInteger.valueOf(val:65537); // Common choice

        // Calculate the private exponent (d)
        BigInteger d = e.modInverse(phiN);

        System.out.print(s:"Enter the message: ");
        String inputMessage = scanner.nextLine();
        BigInteger message = new BigInteger(inputMessage.getBytes());
```



```java

        // Choose a public exponent (e)
        BigInteger e = BigInteger.valueOf(val:65537); // Common choice

        // Calculate the private exponent (d)
        BigInteger d = e.modInverse(phiN);

        System.out.print(s:"Enter the message: ");
        String inputMessage = scanner.nextLine();
        BigInteger message = new BigInteger(inputMessage.getBytes());
```

```java

        // Encryption: ciphertext = message^e mod n
        BigInteger ciphertext = message.modPow(e, n);

        // Decryption: decryptedMessage = ciphertext^d mod n
        BigInteger decryptedMessage = ciphertext.modPow(d, n);

        System.out.println("Original message: " + inputMessage);
        System.out.println("Ciphertext: " + ciphertext);
        System.out.println("Decrypted message: " + new String(decryptedMessage.toByteArray()));

        scanner.close();
    }
}
```

Output:



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

  A new PowerShell stable release is available: v7.3.8
  Upgrade now, or check out the release page at:
    https://aka.ms/PowerShell-Release?tag=v7.3.8

PS E:\B.Tech\SEM-V\LABS\CISL>  & 'C:\Program Files\Java\jdk-19\bin\java.exe' '-agentlib:jdwp=transport=dt_socket,server=n,suspend=y,address=localhost:50417' '-XX:+ShowCod
eDetailsInExceptionMessages' '-cp' 'C:\Users\ADITYA\AppData\Roaming\Code\User\workspaceStorage\982b28e0759a44918fca0f4744cb3a40\redhat.java\jdt_ws\CISL_340623aa\bin' 'A7'

Enter the message: HELLO GUYZ!
Original message: HELLO GUYZ!
Ciphertext: 32639207714965555391210290382769563692293801697331054777833759231582150995009
Decrypted message: HELLO GUYZ!
PS E:\B.Tech\SEM-V\LABS\CISL> 
```