SNS ASSIGNMENT-2 Program instructions

## Srujan R, BT18CSE041

# Z – 2-round Feistel Cipher:

1. First run Alice program with port number as command line input.

Ex: python BT18CSE041\_Z\_A.py 12345

1. Next run Bob program with the same port number as Alice as command line input.

Ex: python BT18CSE041\_Z\_B.py 12345

Text

Description automatically generated

# SE – A Cipher Block Chaining (CBC):

1. First run Alice program with port number as command line input.

Ex: python BT18CSE041\_SE\_A\_A.py 12345

1. Next run Bob program with the same port number as Alice as command line input.

Ex: python BT18CSE041\_SE\_A\_B.py 12345

Text

Description automatically generated with medium confidence

## AC – A OAEP construction of RSA:

1. First run Alice program with port number as command line input.

Ex: python BT18CSE041\_AC\_A\_A.py 12345

1. Next run Bob program with the same port number as Alice as command line input.

Ex: python BT18CSE041\_AC\_A\_B.py 12345

Text

Description automatically generated

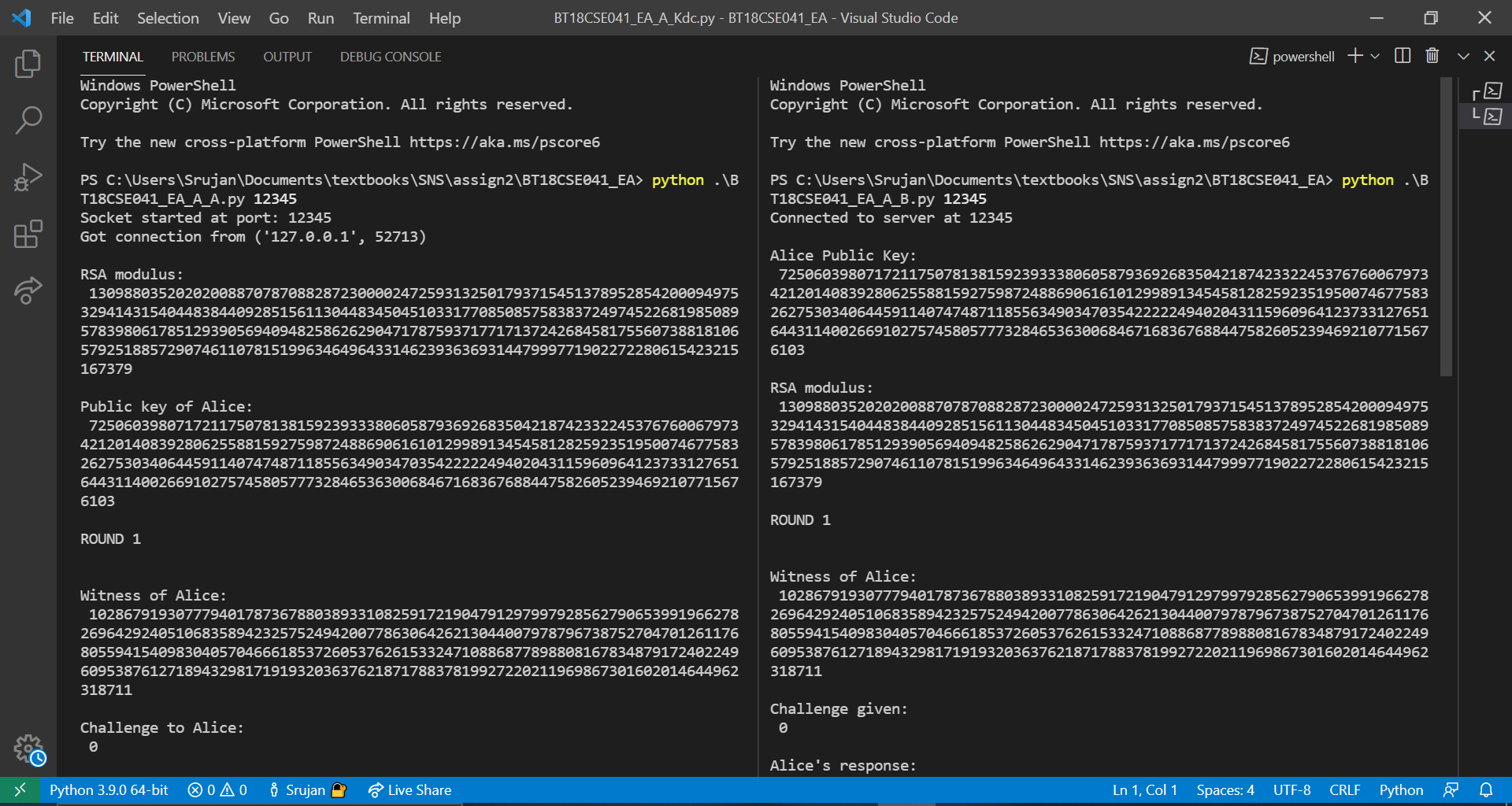
## EA – A Fiat-Shamir Protocol:

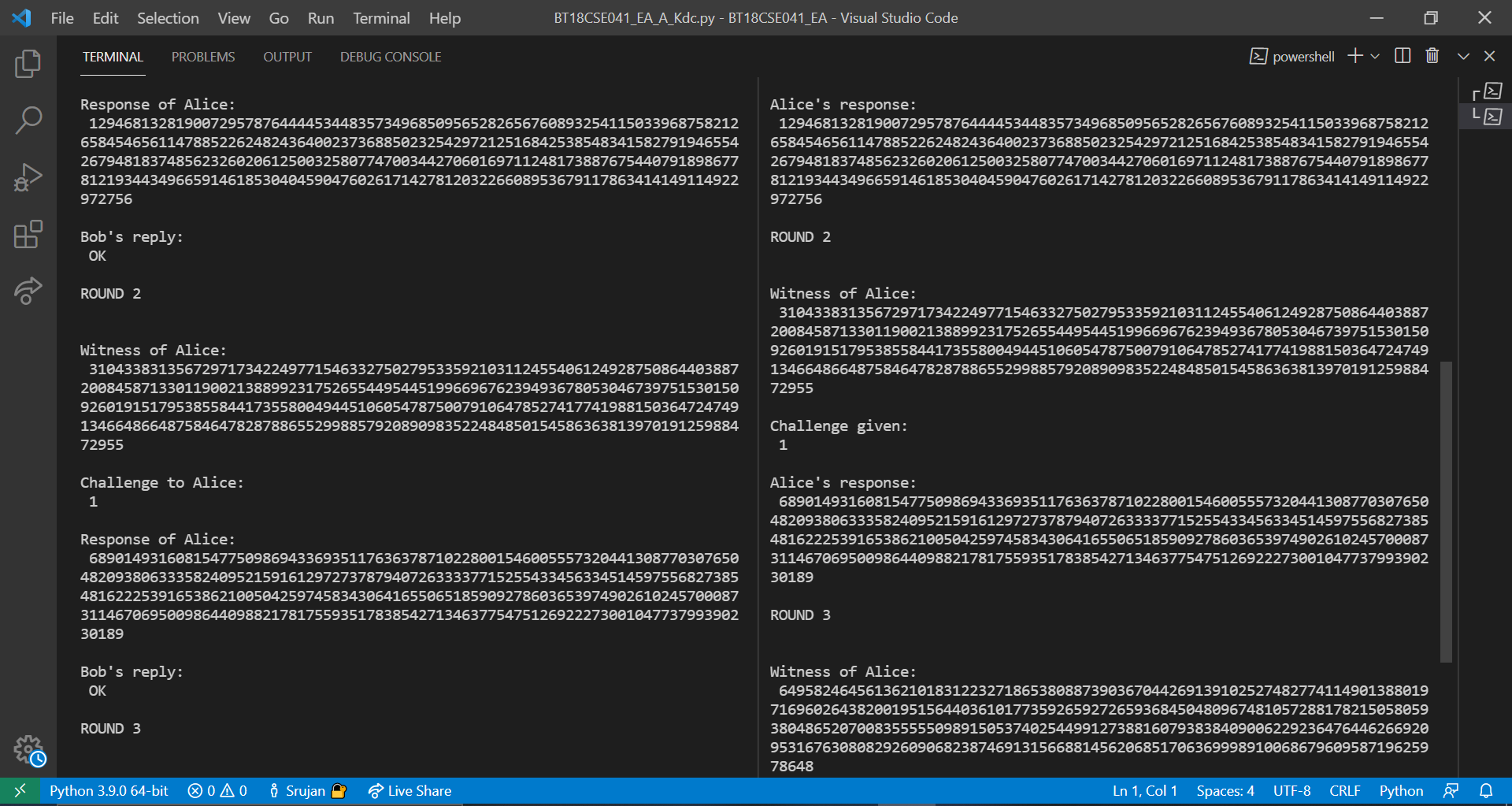
1. First run Alice program with port number as command line input.

Ex: python BT18CSE041\_EA\_A\_A.py 12345

1. Next run Bob program with the same port number as Alice as command line input.

Ex: python BT18CSE041\_EA\_A\_B.py 12345





Graphical user interface, text

Description automatically generated

## KM – A Needham - Schroeder Protocol:

1. First check whether the port numbers 12345 (KDC program), 12346 (Alice program) and 12347 (Bob program) are free or not.

Ex: netstat -ano|findstr 12345 , if any process with pid present can stop it using – kill pid

1. Run the KDC program.

Ex: python BT18CSE041\_KM\_A\_Kdc.py

1. Run the Bob program.

Ex: python BT18CSE041\_KM\_A\_B.py

1. Run the Alice program.

Ex: python BT18CSE041\_KM\_A\_A.py

Graphical user interface, text

Description automatically generated