SNS-ASSIGNMENT-2

BT18CSE063 - CHAUDHARI AMITSINH PRATAPSINH

Q1-a

Execution instructions :

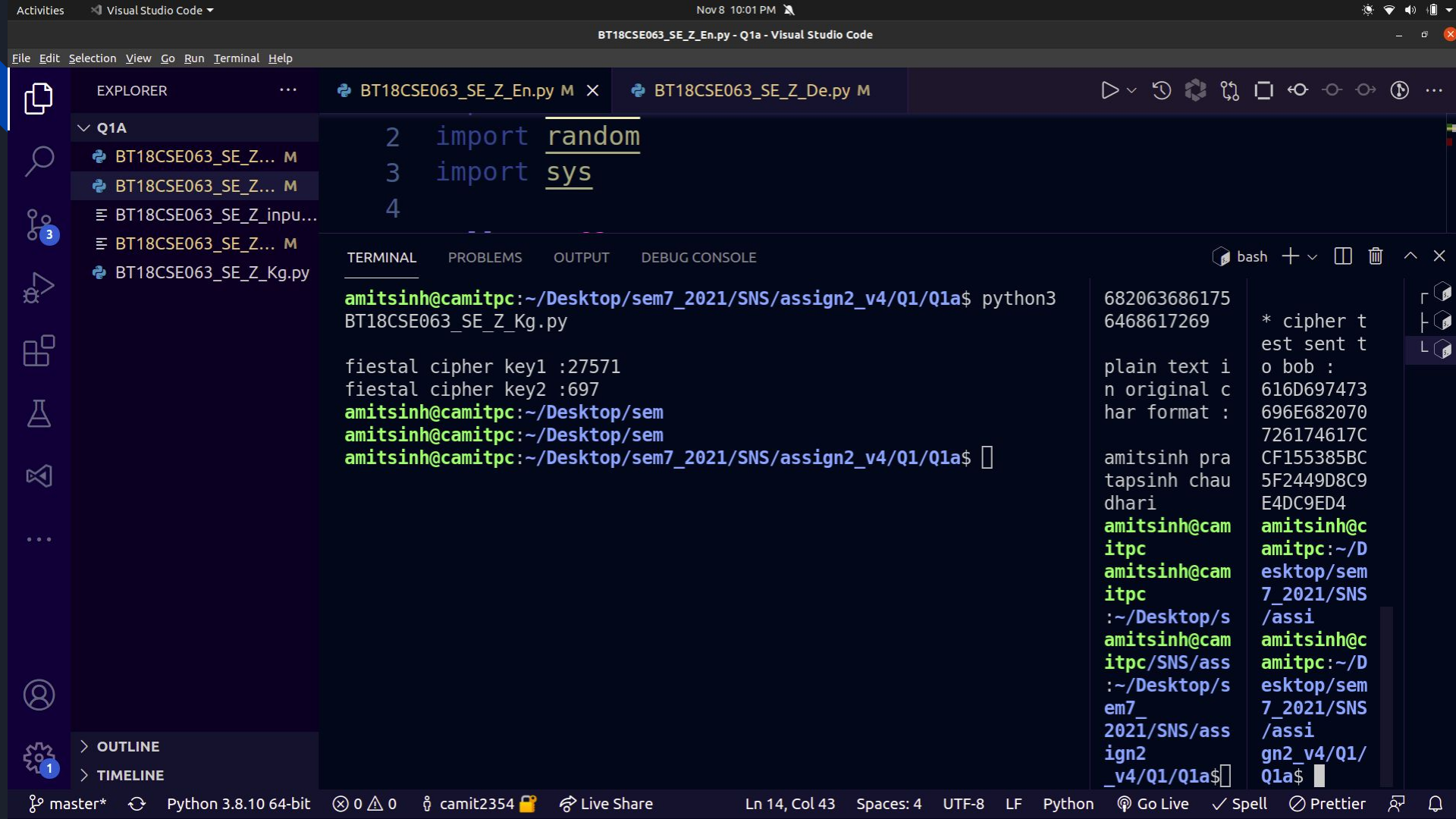
1) Terminal command For Key generation : python3 BT18CSE063_SE_Z_Kg.py
2) Terminal 1 -> First start server side / decryption side which

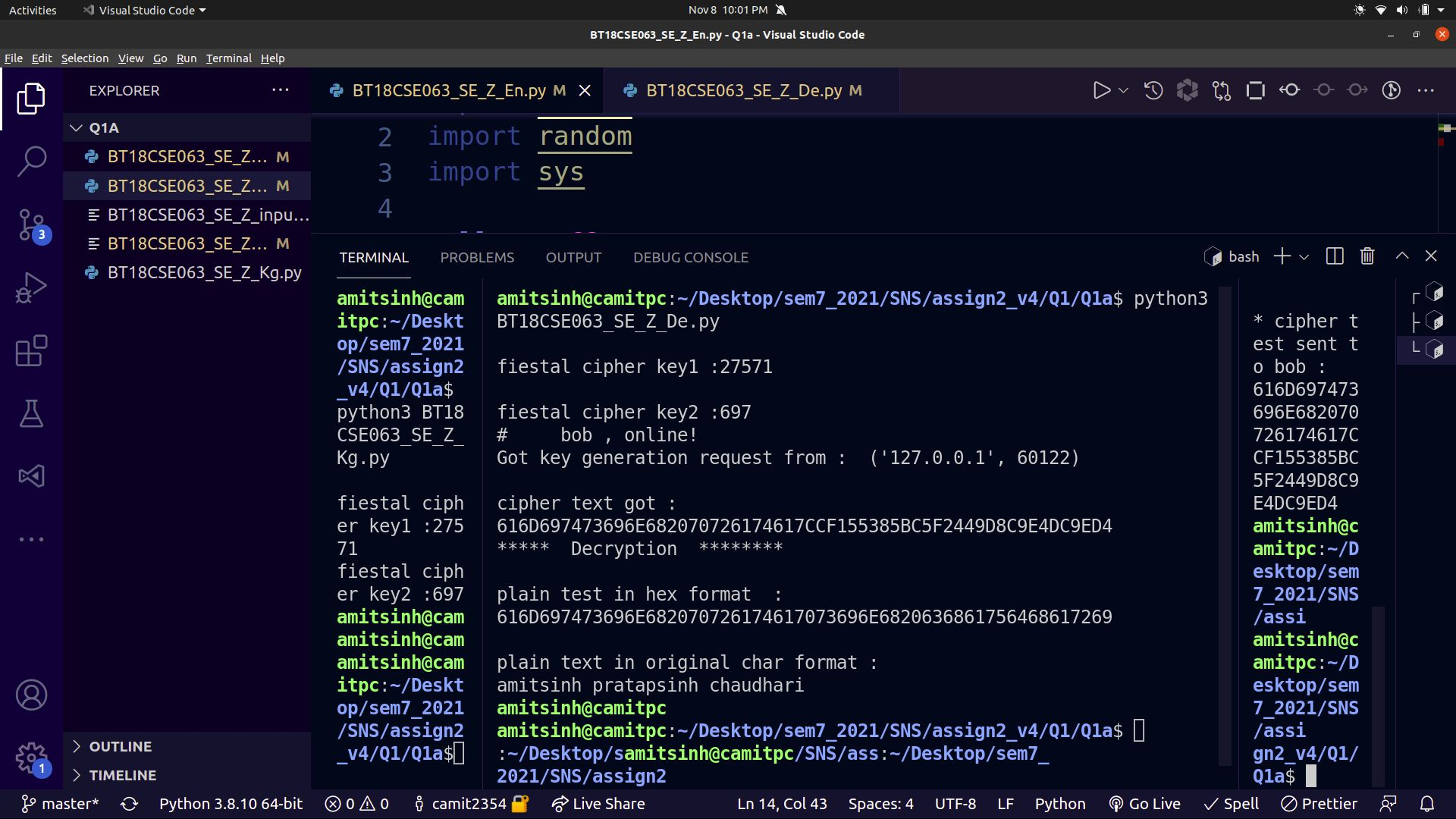
   Will accept cipher test from client node /encryption node

   Command : python3 BT18CSE063_SE_Z_De.py

3) Terminal 2 -> next start encryption process and send cipher test to decrypter :

   Terminal command : python3 BT18CSE063_SE_Z_En.py


Activities
Visual Studio Code
Nov 8 10:01 PM
BT18CSE063_SE_Z_En.py - Q1a - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
Q1A
BT18CSE063_SE_Z... M
BT18CSE063_SE_Z... M
BT18CSE063_SE_Z_inpu...
BT18CSE063_SE_Z... M
BT18CSE063_SE_Z_Kg.py
OUTLINE
TIMELINE
BT18CSE063_SE_Z_En.py M
BT18CSE063_SE_Z_De.py M
2 import random
3 import sys
4
TERMINAL
PROBLEMS
OUTPUT
DEBUG CONSOLE
bash
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$ python3 BT18CSE063_SE_Z_Kg.py
fiestal cipher key1 :27571
fiestal cipher key2 :697
amitsinh@camitpc:~/Desktop/sem
amitsinh@camitpc:~/Desktop/sem
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$
682063686175
6468617269
* cipher t
est sent t
o bob :
616D697473
696E682070
726174617C
CF155385BC
5F2449D8C9
E4DC9ED4
plain text i
n original c
har format :
amitsinh pra
tapsinh chau
dhari
amitsinh@cam
itpc
amitsinh@cam
itpc
:~/Desktop/s
amitsinh@cam
itpc/SNS/ass
:~/Desktop/s
em7_
2021/SNS/ass
ign2
_v4/Q1/Q1a$
amitsinh@c
amitpc:~/D
esktop/sem
7_2021/SNS
/assi
amitsinh@c
amitpc:~/D
esktop/sem
7_2021/SNS
/assi
gn2_v4/Q1/
Q1a$
master*
Python 3.8.10 64-bit
0 0
camit2354
Live Share
Ln 14, Col 43
Spaces: 4
UTF-8
LF
Python
Go Live
Spell
Prettier


Activities
Visual Studio Code
Nov 8 10:01 PM
BT18CSE063_SE_Z_En.py - Q1a - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
Q1A
BT18CSE063_SE_Z... M
BT18CSE063_SE_Z... M
BT18CSE063_SE_Z_inpu...
BT18CSE063_SE_Z... M
BT18CSE063_SE_Z_Kg.py
BT18CSE063_SE_Z_En.py M
BT18CSE063_SE_Z_De.py M
2 import random
3 import sys
4
TERMINAL
PROBLEMS
OUTPUT
DEBUG CONSOLE
bash
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$ python3 BT18CSE063_SE_Z_Kg.py
fiestal cipher key1 :27571
fiestal cipher key2 :697
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$ python3 BT18CSE063_SE_Z_De.py
fiestal cipher key1 :27571
fiestal cipher key2 :697
bob , online!
Got key generation request from : ('127.0.0.1', 60122)
cipher text got :
616D697473696E682070726174617CCF155385BC5F2449D8C9E4DC9ED4
***** Decryption ********
plain test in hex format :
616D697473696E68207072617461707369 6E6820636861756468617269
plain text in original char format :
amitsinh pratapsinh chaudhari
amitsinh@camitpc
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$
* cipher test sent to bob :
616D697473696E682070726174617CCF155385BC5F2449D8C9E4DC9ED4
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assi
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$
OUTLINE
TIMELINE
master*
Python 3.8.10 64-bit
0 0
camit2354
Live Share
Ln 14, Col 43
Spaces: 4
UTF-8
LF
Python
Go Live
Spell
Prettier

EXPLORER

Q1A
- BT18CSE063_SE_Z... M
- BT18CSE063_SE_Z... M
- BT18CSE063_SE_Z_inpu...
- BT18CSE063_SE_Z... M
- BT18CSE063_SE_Z_Kg.py

OUTLINE
TIMELINE

BT18CSE063_SE_Z_En.py M | BT18CSE063_SE_Z_De.py M

```
2  import random
3  import sys
4
```

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE bash

```
3 BT18CSE063_SE_Z_Kg.py

fiestal cipher key1 :27571
fiestal cipher key2 :697
amitsinh@ca
amitsinh@ca
amitsinh@caitpc:~/Desktop/sem7_202/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$
```

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$ python3 BT18CSE063_SE_Z_De.py

fiestal cipher key1 :27571

fiestal cipher key2 :697
#     bob , online!
Got key generation request from :  ( '127.0.0.1', 60122)
```

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assi7_2021/SNS/assign2_v4/Q1/Q1a$ python3 BT18CSE063_SE_Z_En.py

fiestal cipher key1 :27571

fiestal cipher key2 :697
#     alice, online!
bob : connection created !

* Plain text for encryption in hex format :
616D697473696E6820707261746170736965682063686175646861726 9
*****  Encryption  ********

* cipher test sent to bob :
616D697473696E682070726174617CCF155385BC5F2449D8C9E4DC9ED4
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assi
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assi
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a$
```

Q1-b

Execution instructions :

1) Terminal command For Key generation : python3 BT18CSE063_SE_C_Kg.py
2) Terminal 1 -> First start server side / decryption side which

   Will accept cipher test from client node /encryption node

   Command : python3 BT18CSE063_SE_C_De.py

3) Terminal 2 -> next start encryption process and send cipher test to decrypter :

   python3 BT18CSE063_SE_C_En.py

EXPLORER

Q1B

- BT18CSE063_SE_C_De.py
- BT18CSE063_SE_C_En.py
- BT18CSE063_SE_C_inp...
- BT18CSE063_SE_C... M
- BT18CSE063_SE_C_Kg.py

OUTLINE

TIMELINE

BT18CSE063_SE_C_En.py | BT18CSE063_SE_C_Kg.py

You, 8 hours ago | 1 author (You)

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE bash

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1b$ python3 BT18CSE063_SE_C_Kg.py

 key generated : 8F1DE11E9EF4B83A
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1b$
```

BT18CSE063_SE_C_En.py | BT18CSE063_SE_C_De.py

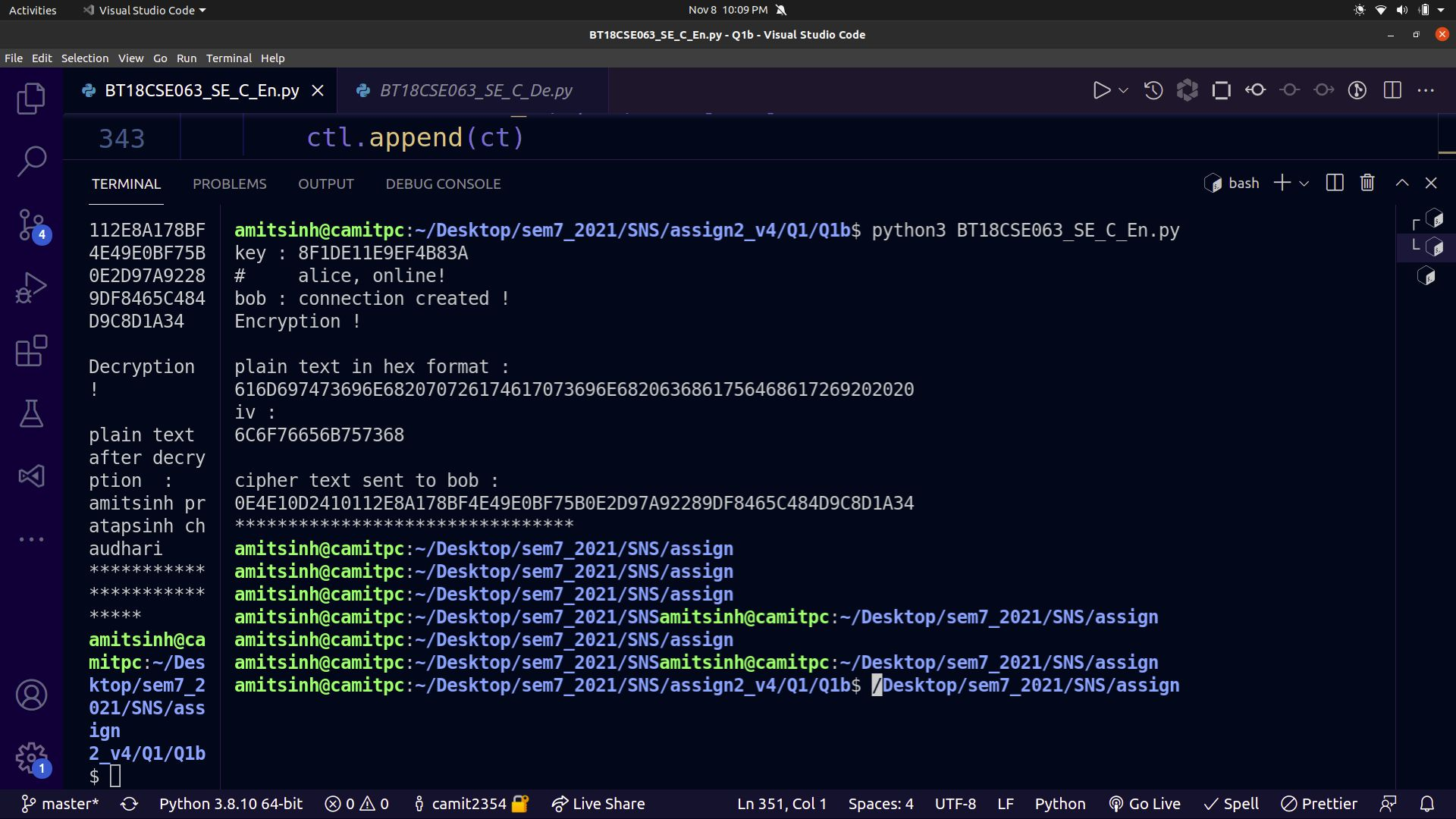
```
343         ctl.append(ct)
```

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1b$ python3 BT18CSE063_SE_C_Kg.py

 key generated : 8F1DE11E9EF4B83A
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1b$ python3 BT18CSE063_SE_C_De.py
key : 8F1DE11E9EF4B83A
#     bob , online!
Got key generation request from :  ('127.0.0.1', 60306)

cipher text got :
0E4E10D2410112E8A178BF4E49E0BF75B0E2D97A92289DF8465C484D9C8D1A34

Decryption !

plain text after decryption  :
amitsinh pratapsinh chaudhari
**************************
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1b$
```

bash

```
pc:~/Desktop/sem7_2021/SNSamitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNSamitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/a
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
2_v4/Q1/Q1b$
```


Activities
Visual Studio Code
Nov 8 10:09 PM
BT18CSE063_SE_C_En.py - Q1b - Visual Studio Code
File Edit Selection View Go Run Terminal Help
BT18CSE063_SE_C_En.py
BT18CSE063_SE_C_De.py
343 ctl.append(ct)
TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE
bash
112E8A178BF
4E49E0BF75B
0E2D97A9228
9DF8465C484
D9C8D1A34
Decryption
!
plain text
after decry
ption :
amitsinh pr
atapsinh ch
audhari
****
****
*****
amitsinh@ca
mitpc:~/Des
ktop/sem7_2
021/SNS/ass
ign
2_v4/Q1/Q1b
$
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1b$ python3 BT18CSE063_SE_C_En.py
key : 8F1DE11E9EF4B83A
alice, online!
bob : connection created !
Encryption !
plain text in hex format :
616D697473696E6820707261746170736696E6820636861756468617269202020
iv :
6C6F76656B757368
cipher text sent to bob :
0E4E10D2410112E8A178BF4E49E0BF75B0E2D97A92289DF8465C484D9C8D1A34
****
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNSamitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNSamitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1b$ /Desktop/sem7_2021/SNS/assign
master*
Python 3.8.10 64-bit
0 0
camit2354
Live Share
Ln 351, Col 1
Spaces: 4
UTF-8
LF
Python
Go Live
Spell
Prettier

Q2

Execution instructions :

1) Key generation : python BT18CSE063_AC_C_Kg.py
2) Terminal 1 -> Start verifier in listening mode : python3 BT18CSE063_AC_C_Vf.py
3) Terminal 2 - > Start signer & send sign , msg to verifier in new terminal : python3 BT18CSE063_AC_C_Sg.py

3_AC_C_Vf.py | BT18CSE063_AC_C_input.txt | BT18CSE063_AC_C_Sg.py | BT18CSE063_AC_C_Kg.py M

```
16 > def getFactors(n): ...
22
```

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE bash

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q2$ python BT18CSE063_AC_C_Kg.py
public key : {'q': 7, 'p': 2311, 'e1': 2, 'e2': 936}
secret key : {'d': 605}
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q2$
```

CSE063_AC_C_Vf.py | BT18CSE063_AC_C_input.txt | BT18CSE063_AC_C_Sg.py | BT18CSE063_AC_C_Kg.py

You, an hour ago | 1 author (You)

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE bash

```
secret key : {'d': 605}
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q2$ python3 BT18CSE063_AC_C_Vf.py
************   Verification!   ****************
#     bob , online!

public key : {'q': 7, 'p': 2311, 'e1': 2, 'e2': 936}

Got key generation request from :
 ('127.0.0.1', 60464)

#verify req :

doc for verify :
name : amitsinh pratapsinh chaudhari roll no : 63


signature on given doc  :
{'s1': 4611686018427387903, 's2': 11}

v :4611686018427387903
 s1 : 4611686018427387903

verification result :
True
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q2$
```

```
name : amitsinh pratapsinh chaudhari roll no : 63

random r : 9

signature :
{'s1': 4611686018427387903, 's2': 11}

 msg , sign sent for verification !

amitsinh@camitpc:~/Desktop/sem7_2021/SNS/a
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
2_v4/Q2$
```

CSE063_AC_C_Vf.py | BT18CSE063_AC_C_input.txt | BT18CSE063_AC_C_Sg.py | BT18CSE063_AC_C_Kg.py

You, an hour ago | 1 author (You)

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE bash

```
ktop/sem7_2021/SNS/assign2_v4/Q2$ python BT18CSE063_AC_C_Kg.py
public key : {'q': 7, 'p': 2311, 'e1': 2, 'e2': 936}
secret key : {'d': 605}
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q2$ python3 BT18CSE063_AC_C_Vf.py
***********
*   Verification!  ***
```

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q2$ python3 BT18CSE063_AC_C_Sg.py
***********   Signature !  ***************
#     alice, online!

secret key : {'d': 605}
bob : connection created !

Doc for sign :
name : amitsinh pratapsinh chaudhari roll no : 63

random r : 9

signature :
{'s1': 4611686018427387903, 's2': 11}

 msg , sign sent for verification !

amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q2$
```

Q3

Execution instructions :

1) Key generation : python3 BT18CSE063_EA_C_Kg.py
2) Terminal 1 : Start the authenticator node (bob) in listening mode : python3 BT18CSE063_EA_C_B.py
3) Terminal 2 : Start the connection req creating node & create a connection req : python3 BT18CSE063_EA_C_A.py

BT18CSE063_EA_C_Kg.py

```
39  p1 = primes[random.randint(1, len(primes)-1)]
40  p2 = primes[random.randint(1, len(primes)-1)]
41
```

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE bash

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q3$ python3 BT18CSE063_EA_C_Kg.py
public key : {'n': 26711, 'v': 14745, 'e': 5}
secret key : {'s': 74933}
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q3$
```

BT18CSE063_EA_C_A.py

```
17
18  # public key
19
20
21  def select_random_r():
22      r = random.randint(1, 77)
23      print("randomly selected r : "+str(r))
24      return r      You, 4 days ago • "assign-2 version 4"
```

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE

```
public key : {'n': 26711, 'v': 14745, 'e': 5}
secret key : {'s': 74933}
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q3$ python3 BT18CSE063_EA_C_B.py

 public key : {'n': 26711, 'v': 14745, 'e': 5}
#     bob, online!
Got connection from ('127.0.0.1', 60574)
**********  round 0  ************
Witness got : 17612
randomly selected c : 2
y got : 6425
y2 : 17612 x : 17612
valid y !
**********  round 1  ************
Witness got : 8484
randomly selected c : 2
y got : 23416
y2 : 8484 x : 8484
valid y !
**********  round 2  ************
Witness got : 32
randomly selected c : 4
y got : 2689
y2 : 32 x : 32
valid y !
**********  round 3  ************
Witness got : 1
randomly selected c : 4
y got : 14700
y2 : 1 x : 1
valid y !
**********  round 4  ************
Witness got : 10342
randomly selected c : 1
y got : 16088
y2 : 10342 x : 10342
valid y !
************    Auth success !      ***************
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q3$
```

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q3$ python3 BT18CSE063_EA_C_A.py

 secret key : {'s': 74933}
#     Alice , online!
Auth required !
**********  round 0  ************
randomly selected r : 67
witness sent : 17612
c got : 2
y sent : 6425
status got  : 1
**********  round 1  ************
randomly selected r : 28
witness sent : 8484
c got : 2
y sent : 23416
status got  : 1
**********  round 2  ************
randomly selected r : 2
witness sent : 32
c got : 4
y sent : 2689
status got  : 1
**********  round 3  ************
randomly selected r : 1
witness sent : 1
c got : 4
y sent : 14700
status got  : 1
**********  round 4  ************
randomly selected r : 38
witness sent : 10342
c got : 1
y sent : 16088
status got  : 1
******  Authentication succesful ! *************
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/aamitsinh@camitpc:~/Desktop/sem7_2021/SNS/aamitsinh@camitpc:~/Desktop/sem7_202amitsinh@camitpc:~/Desktop/sem7_202amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assamitsinh@camitpc:~/Desktamitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q3$
```

Q4

Execution instructions :

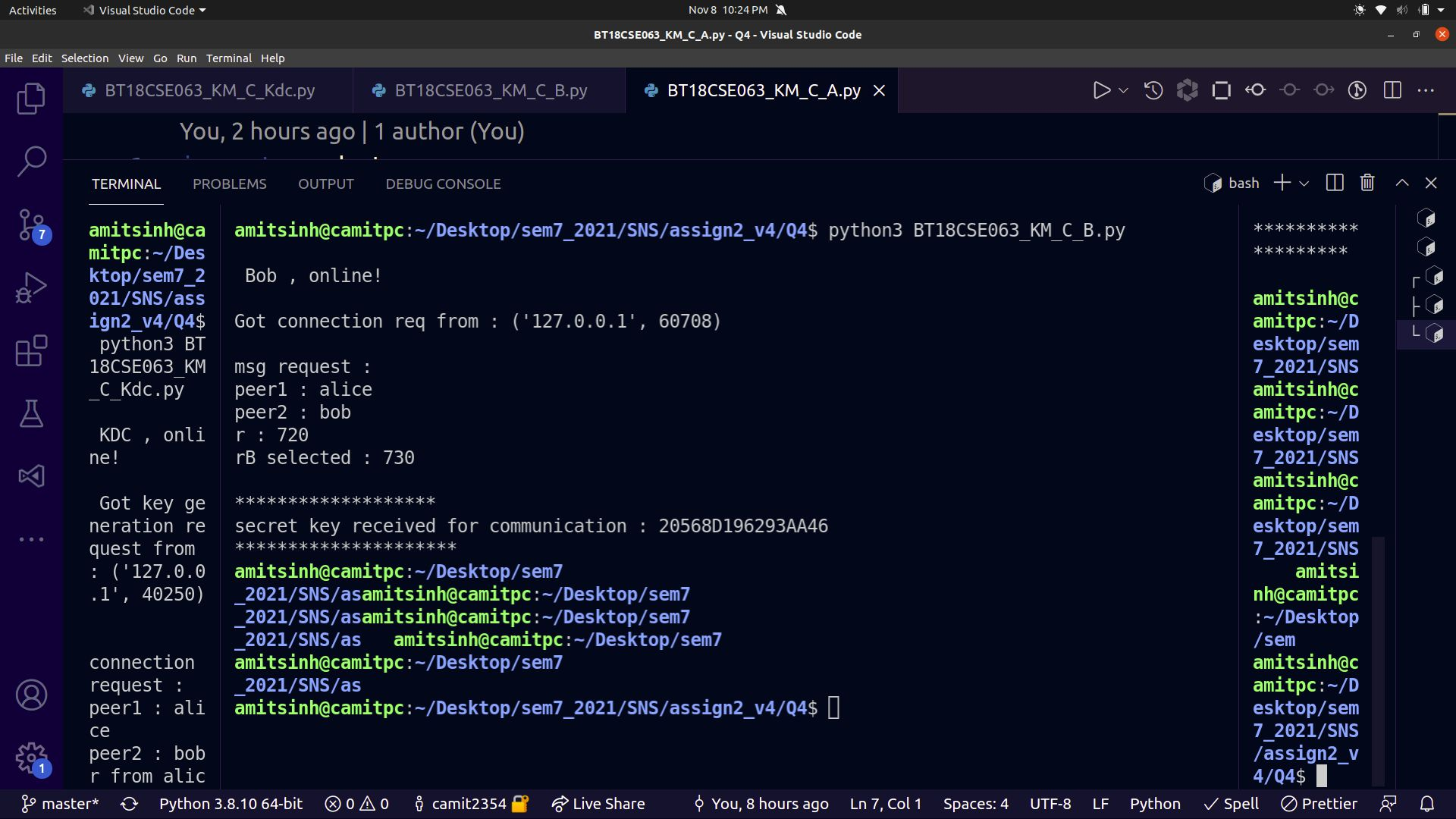
1) Terminal 1 -> Start KDC in listening mode : python3 BT18CSE063_KM_C_Kdc.py
2) Terminal 2 -> Start Bob in listening mode : python3 BT18CSE063_KM_C_B.py
3) Terminal 3 -> Alice Create connection req to Bob & acquire secret key for further communication from KDC: python3 BT18CSE063_KM_C_A.py

BT18CSE063_KM_C_Kdc.py | BT18CSE063_KM_C_B.py | BT18CSE063_KM_C_A.py

You, 2 hours ago | 1 author (You)

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE bash

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q4$ python3 BT18CSE063_KM_C_Kdc.py

 KDC , online!

 Got key generation request from : ('127.0.0.1', 40250)


connection request :
peer1 : alice
peer2 : bob
r from alice : 720
rA from alice : 162
r from bob : 720
rB from bob : 730

**********
secret key generated : 20568D196293AA46

 secret key sent ...
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q4$
```


Activities
Visual Studio Code
Nov 8 10:24 PM
BT18CSE063_KM_C_A.py - Q4 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
BT18CSE063_KM_C_Kdc.py
BT18CSE063_KM_C_B.py
BT18CSE063_KM_C_A.py
You, 2 hours ago | 1 author (You)
TERMINAL
PROBLEMS
OUTPUT
DEBUG CONSOLE
bash
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q4$ python3 BT18CSE063_KM_C_B.py
Bob , online!
Got connection req from : ('127.0.0.1', 60708)
msg request :
peer1 : alice
peer2 : bob
r : 720
rB selected : 730
****
secret key received for communication : 20568D196293AA46
****
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q4$
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q4$ python3 BT18CSE063_KM_C_Kdc.py
KDC , online!
Got key generation request from : ('127.0.0.1', 40250)
connection request :
peer1 : alice
peer2 : bob
r from alic
master*
Python 3.8.10 64-bit
0 0
camit2354
Live Share
You, 8 hours ago
Ln 7, Col 1
Spaces: 4
UTF-8
LF
Python
Spell
Prettier

BT18CSE063_KM_C_Kdc.py | BT18CSE063_KM_C_B.py | BT18CSE063_KM_C_A.py

You, 2 hours ago | 1 author (You)

TERMINAL PROBLEMS OUTPUT DEBUG CONSOLE bash

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q4$ python3 BT18CSE063_KM_C_Kdc.py

 KDC , online!

 Got key generation request from : ('127.0.0.1', 40250)


connection request : peer1 : alice
peer2 : bobr from alic
```

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q4$
```

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q4$ python3 BT18CSE063_KM_C_A.py

 Alice , online!

connection request sent to Bob

msg request :
r selected :720
rA selected : 162

********************
secret key received for communication : 20568D196293AA46
********************
```

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNSamitsinh@camitpc:~/Desktop/sem7_2021/SNSamitsinh@camitpc:~/Desktop/sem7_2021/SNS    amitsinh@camitpc:~/Desktop/sem7_2021/SNS amitsinh@camitpc:~/Desktop/sem7_2021/SNS/
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q4$
```

master* Python 3.8.10 64-bit 0 0 camit2354 Live Share You, 8 hours ago Ln 7, Col 1 Spaces: 4 UTF-8 LF Python Spell Prettier