




SNS-ASSIGNMENT-2

BT18CSE063 - CHAUDHARI AMITSINH
PRATAPSIH



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

BT18CSE063_SE_Z_En.py M BT18CSE063_SE_Z_De.py M

Q1A

BT18CSE063_SE_Z... M

BT18CSE063_SE_Z... M

BT18CSE063_SE_Z_inpu...

BT18CSE063_SE_Z... M

BT18CSE063_SE_Z_Kg.py

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

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\$

* cipher t

est sent t

o bob :

616D697473

696E682070

726174617C

CF155385BC

5F2449D8C9

E4DC9ED4

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

ActivitiesVisual Studio Code

Nov 8 10:01 PM

BT18CSE063_SE_Z_En.py - Q1a - Visual Studio Code

FileEditSelectionViewGoRunTerminalHelp

EXPLORER

BT18CSE063_SE_Z_En.py M ×BT18CSE063_SE_Z_De.py M

Q1A

BT18CSE063_SE_Z... M

BT18CSE063_SE_Z... M

BT18CSE063_SE_Z_inpu...

BT18CSE063_SE_Z... M

BT18CSE063_SE_Z_Kg.py

2import random

3import sys

4

TERMINALPROBLEMSOUTPUTDEBUG CONSOLE

bash

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 :

616D697473696E682070726174617073696E6820636861756468617269

**** Decryption ****

plain test in hex format :

616D697473696E682070726174617073696E6820636861756468617269

plain text in original char format :

amitsinh pratapsinh chaudhari

amitsinh@camitpc

amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a\$

* cipher text sent to bob :

616D697473

696E682070

726174617C

CF155385BC

5F2449D8C9

E4DC9ED4

amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1a\$

OUTLINE


TIMELINE

master*Python 3.8.10 64-bit0 0camit2354Live ShareLn 14, Col 43Spaces: 4UTF-8LFPythonGo Live✓ SpellPrettier

Timeline

```
* cipher test sent to bob :
616D6974736996E682070726174617CFC155385BC5F2449D8C9E4DC9ED4
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assi
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assi
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2 v4/Q1/Q1a
```

Ln 14, Col 43 Spaces: 4 UTF-8 LF Python Go Live Spell Prettier



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`

Activities

Visual Studio Code

Nov 8 10:07 PM

BT18CSE063_SE_C_Kg.py - Q1b - Visual Studio Code

File Edit Selection View Go Run Terminal Help

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\$

master*

Python 3.8.10 64-bit

0 0

camit2354

Live Share

Ln 43, Col 33

Spaces: 4

UTF-8

LF

Python

Go Live

Spell

Prettier

ActivitiesVisual Studio Code

Nov 8 10:08 PM

BT18CSE063_SE_C_En.py - Q1b - Visual Studio Code

FileEditSelectionViewGoRunTerminalHelp

BT18CSE063_SE_C_En.py ×BT18CSE063_SE_C_De.py

343ctl.append(ct)

TERMINALPROBLEMSOUTPUTDEBUG 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/s
em7_2021/SNSam
itsinh@camitpc
:~/Desktop/sem
7_2021/SNS/ass
ign
amitsinh@camit
pc:~/Desktop/s
em7_2021/SNS/a
ssign
amitsinh@camit
pc:~/Desktop/s
em7_2021/SNSam
itsinh@camitpc
:~/Desktop/sem
7_2021/SNS/ass
ign
amitsinh@camit
pc:~/Desktop/s
em7_2021/SNS/a
amitsinh@camit
pc:~/Desktop/s
em7_2021/SNS/a
ssign
2_v4/Q1/Q1b\$

master*Python 3.8.10 64-bit0 0camit2354Live ShareLn 351, Col 1Spaces: 4UTF-8LFPythonGo Live✓ SpellPrettier


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

 bash      

```

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/SNSamitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign2_v4/Q1/Q1b$ /Desktop/sem7_2021/SNS/assign

```



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`

Activities

Visual Studio Code

Nov 8 10:14 PM

BT18CSE063_AC_C_Kg.py - Q2 - Visual Studio Code

File Edit Selection View Go Run Terminal Help

BT18CSE063_AC_C_Vf.py

BT18CSE063_AC_C_input.txt

BT18CSE063_AC_C_Sg.py

BT18CSE063_AC_C_Kg.py M X

10 > def getFactors(n): ""

22

TERMINAL

PROBLEMS

OUTPUT

DEBUG CONSOLE

bash + - [] [X] ^ X

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\$

master*

Python 3.8.10 64-bit

0 0

camit2354

Live Share

Ln 40, Col 35

Spaces: 4

UTF-8

LF

Python

Go Live

✓ Spell

⊗ Prettier

ActivitiesVisual Studio Code

Nov 8 10:15 PM

BT18CSE063_AC_C_Sg.py - Q2 - Visual Studio Code

FileEditSelectionViewGoRunTerminalHelp

CSE063_AC_C_Vf.pyBT18CSE063_AC_C_input.txtBT18CSE063_AC_C_Sg.py ×BT18CSE063_AC_C_Kg.py

You, an hour ago | 1 author (You)

TERMINALPROBLEMSOUTPUTDEBUG CONSOLE

```
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$
```

bash

name : amitsinh
pratapsinh c
haudhari roll
no : 63

random r : 9

signature :
{ 's1': 4611686
018427387903,
's2': 11}

msg , sign se
nt for verific
ation !

amitsinh@camit
pc:~/Desktop/s
em7_2021/SNS/a
amitsinh@camit
pc:~/Desktop/s
em7_2021/SNS/a
ssign
2_v4/Q2\$

master*Python 3.8.10 64-bit0 0camit2354Live ShareLn 5, Col 1Spaces: 4UTF-8LFPythonGo Live✓ SpellPrettier

ActivitiesVisual Studio Code

Nov 8 10:15 PM

BT18CSE063_AC_C_Sg.py - Q2 - Visual Studio Code

FileEditSelectionViewGoRunTerminalHelp

CSE063_AC_C_Vf.pyBT18CSE063_AC_C_input.txtBT18CSE063_AC_C_Sg.pyXBT18CSE063_AC_C_Kg.py

You, an hour ago | 1 author (You)

TERMINALPROBLEMSOUTPUTDEBUG CONSOLE

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_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\$

bash

master*

Python 3.8.10 64-bit

0 0

camit2354

Live Share

Ln 5, Col 1

Spaces: 4

UTF-8

LF

Python

Go Live

Spell

Prettier



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$
```

[TERMINAL](#)
[PROBLEMS](#)
[OUTPUT](#)
[DEBUG CONSOLE](#)

```
***** Auth success ! *****
```

```
amitsinh@camitpc:~/Desktop/sem7_2021/SNS/assign3_v4/03$
```



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`

ActivitiesVisual Studio CodeNov 8 10:24 PMBT18CSE063_KM_C_A.py - Q4 - Visual Studio Code

FileEditSelectionViewGoRunTerminalHelp

BT18CSE063_KM_C_Kdc.pyBT18CSE063_KM_C_B.pyBT18CSE063_KM_C_A.py ×

You, 2 hours ago | 1 author (You)

TERMINALPROBLEMSOUTPUTDEBUG CONSOLE

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\$

bash

n : 20568D196293AA46


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

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

master*Python 3.8.10 64-bit0 0camit2354Live ShareYou, 8 hours agoLn 7, Col 1Spaces: 4UTF-8LFPython✓SpellPrettier



bash + [icon] [icon] [icon] [icon] [icon] [icon]



 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

