

# SNS Execution instructions

BT18CSE060 Rishu Kumar

D set code

Link to this pdf on notion website: <https://vast-turnip-20a.notion.site/SNS-Execution-instructions-08b4071ebef24b6688ba6b93b43eceb8>

- 💡 Pre-requisites installation commands:

1. pip install des
2. pip install pycryptodome

## Q1. Symmetric Encryption - 2 Round fiestal Cipher

▼ Files :: BT18CSE060\_SE\_Z\_En (Alice), BT18CSE060\_SE\_Z\_De (Bob), BT18CSE060\_SE\_Z\_util (Helper)

- Run Bob file first to start the server
- Run Alice file and send the message using **cmd args**
- Get the decrypted message using Bob file

Double click on image to see it on full screen

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS D:\College\Sem7\SNS\Assignment2> python BT18CSE060_SE_Z_En.py "HelloWorld"
-----
Thank you for connecting
The Entered Plain Text is: HelloWorld
Message encrypted, sending it to Bob
Bob replied: Got your Message, Thank you!
connection closed
-----
PS D:\College\Sem7\SNS\Assignment2> 
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS D:\College\Sem7\SNS\Assignment2> python BT18CSE060_SE_Z_De.py
#####
socket binded to 8001
Bob is listening
-----
Got connection from ('127.0.0.1', 62225)
-----
getting message....
Alice sent message :: HelloWorld
#####
[]
```

## Commands ::

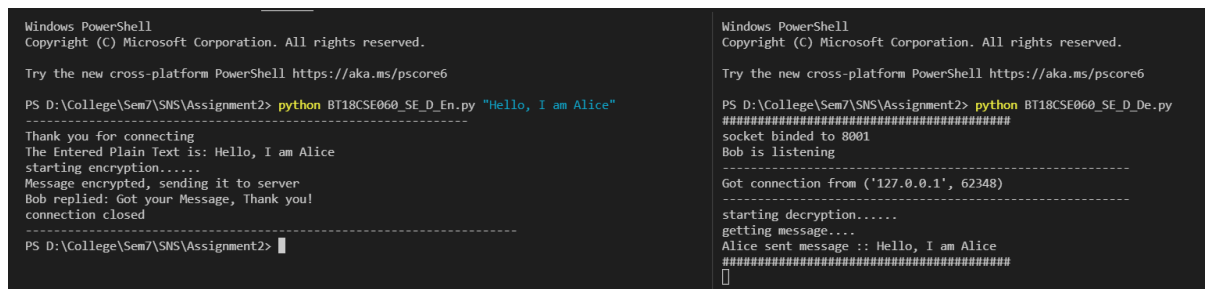
```
#Decryption
1) python BT18CSE060_SE_Z_De.py
#Encryption
2) python BT18CSE060_SE_Z_En.py "HelloWorld"
```

## Q2. Symmetric Encryption - CTR

▼ Files :: BT18CSE060\_SE\_D\_En (Alice), BT18CSE060\_SE\_D\_De (Bob)

- Run Bob file first to start the server
- Run Alice file and send the message using **cmd args**
- Get the decrypted message using Bob file

Double click on image to see it on full screen



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS D:\College\Sem7\SNS\Assignment2> python BT18CSE060_SE_D_En.py "Hello, I am Alice"
-----
Thank you for connecting
The Entered Plain Text is: Hello, I am Alice
starting encryption.....
Message encrypted, sending it to server
Bob replied: Got your Message, Thank you!
connection closed
-----
PS D:\College\Sem7\SNS\Assignment2>

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS D:\College\Sem7\SNS\Assignment2> python BT18CSE060_SE_D_De.py
#####
socket binded to 8001
Bob is listening
-----
Got connection from ('127.0.0.1', 62348)
-----
starting decryption.....
getting message....
Alice sent message :: Hello, I am Alice
#####
```

## Commands ::

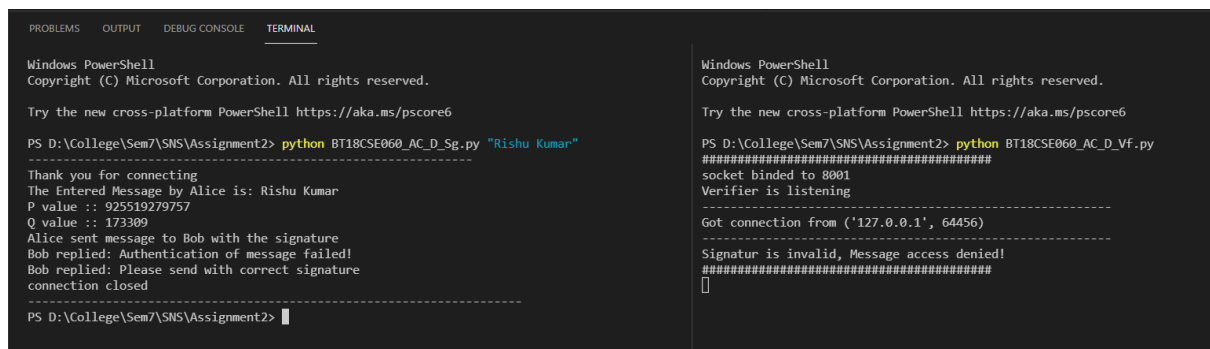
```
#Decryption
1) python BT18CSE060_SE_D_De.py
#Encryption
2) python BT18CSE060_SE_D_En.py "Hello, I am Alice"
```

## Q3. Asymmetric Cryptography - DSS

▼ Files :: BT18CSE060\_AC\_D\_Sg (Signer), BT18CSE060\_AC\_D\_Vf (Verifier), BT18CSE060\_AC\_D\_Kg (Key Generation), BT18CSE060\_AC\_D\_helper (Helper)

- Run verifier file first to start the server
- Run Signer file to generate keys and send the message using **cmd args**
- Get the sign verified and decrypted message using Verifier file

Double click on image to see it on full screen



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS D:\College\Sem7\SNS\Assignment2> python BT18CSE060_AC_D_Sg.py "Rishu Kumar"
-----
Thank you for connecting
The Entered Message by Alice is: Rishu Kumar
P value :: 925519279757
Q value :: 173309
Alice sent message to Bob with the signature
Bob replied: Authentication of message failed!
Bob replied: Please send with correct signature
connection closed
-----
PS D:\College\Sem7\SNS\Assignment2>

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS D:\College\Sem7\SNS\Assignment2> python BT18CSE060_AC_D_Vf.py
#####
socket binded to 8001
Verifier is listening
-----
Got connection from ('127.0.0.1', 64456)
-----
Signature is invalid, Message access denied!
#####
[]
```

## Commands ::

```
#Verifier
1) python BT18CSE060_AC_D_Vf.py
#Signer
2) python BT18CSE060_AC_D_Sg.py "Rishu Kumar"
```

## Q4. Entity Authentication - Guillou – Quisquater protocol

▼ Files :: BT18CSE060\_EA\_D\_A (Alice), BT18CSE060\_EA\_D\_B (Bob), BT18CSE060\_EA\_D\_Kg (Key Generation), BT18CSE060\_EA\_D\_util (Helper)

- Run Bob file first to start the server
- Run Alice file to generate keys and start Authentication

Double click on image to see it on full screen

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS D:\College\Sem7\SNS\Assignment2> python BT18CSE060_EA_D_A.py
-----
Thank you for connecting
Verification starting.....
Passed the test 1 successfully
Passed the test 2 successfully
Passed the test 3 successfully
Verification of Alice done successfully
connection closed
-----
PS D:\College\Sem7\SNS\Assignment2>

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS D:\College\Sem7\SNS\Assignment2> python BT18CSE060_EA_D_B.py
#####
socket binded to 8001
Bob is listening
-----
Got connection from ('127.0.0.1', 62402)
-----
File created to access Public values
Authenticating and verifying the Alice for 3 rounds
Pass the test 1 of verification
Pass the test 2 of verification
Pass the test 3 of verification
Alice can now send the messages freely
#####
█
```

## Commands ::

```
#Bob
1) python BT18CSE060_EA_D_B.py
#Alice
2) python BT18CSE060_EA_D_A.py
```

## Q5. Key Management - Otway-Rees Protocol

▼ Files :: BT18CSE060\_KM\_D\_A (Alice), BT18CSE060\_KM\_D\_B (Bob), BT18CSE060\_KM\_D\_Kdc (KDC)

- Run KDC file - KDC server to allocate session key
- Run Bob file - Receive session key from KDC
- Run Alice file - Receive session key from KDC via Alice and send the message using cmd args
- Get the decrypted message using Bob file

Double click on image to see it on full screen

<pre>PS D:\College\Sem7\SNS\Assignment2&gt; python BT18CSE060_KM_D_A.py "I am Alice, let's talk" ----- Alice is in running status... Thank you Alice for connecting Connection details sent to Bob.... Received Session Key from KDC Session Key decrypted by Alice Connection established successfully between Alice and Bob... Message sent to Bob..... Bob replied: Got your Message, Thank you! connection closed PS D:\College\Sem7\SNS\Assignment2&gt; []</pre>	<pre>Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved.  Try the new cross-platform PowerShell https://aka.ms/pscore6  PS D:\College\Sem7\SNS\Assignment2&gt; python BT18CSE060_KM_D_B.py ##### socket binded to 8002 Bob is listening ----- Got connection from ('127.0.0.1', 62411) ----- Established Connection with KDC Alice details recieved successfully by KDC Bob details recieved successfully by KDC Received Session Keys for Both Alice and Bob Forwarded the session key details to alic Shared Key Established..... Decrypting message..... Message sent by Alice: I am Alice, let's talk ##### █</pre>	<pre>Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved.  Try the new cross-platform PowerShell https://aka.ms/pscore6  PS D:\College\Sem7\SNS\Assignment2&gt; python BT18CSE060_KM_D_Kdc.py ##### socket binded to 8003 KDC is in listening mode ----- Got connection from ('127.0.0.1', 62412) ----- Alice details recieved Decrypted the value of Ra from alic details Bob details recieved Decrypted the value of Rb from bob details session key generated is: 49reumev Generated Session key for Alice and Bob Session key details of Alice sent Session key details of Bob sent Connection established between Bob and Alice! ----- []</pre>
---	--	--

## Commands ::

```
#KDC
1) python BT18CSE060_KM_D_Kdc.py
#Bob
2) python BT18CSE060_KM_D_B.py
#Alice
3) python BT18CSE060_KM_D_A.py "I am Alice, let's talk"
```