Needham Schroeder Protocol

Under the guidance of :
Dr. Soumyadev Maity

Presented By :

Anshul Anand - ICM2014501
Kritika Sharma - ICM2014502
Jatin Goel - ICM2014503
Rishabh Verma - ICM2014004
Varun Kumar - ICM2014008

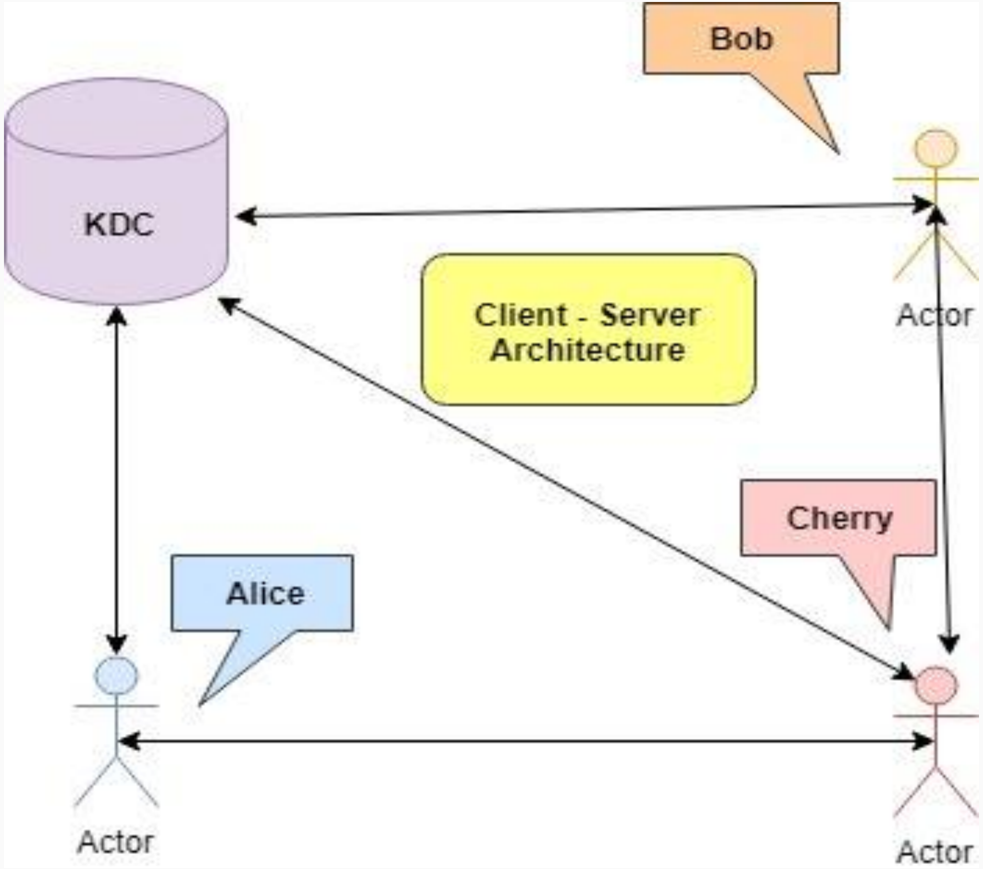
Introduction

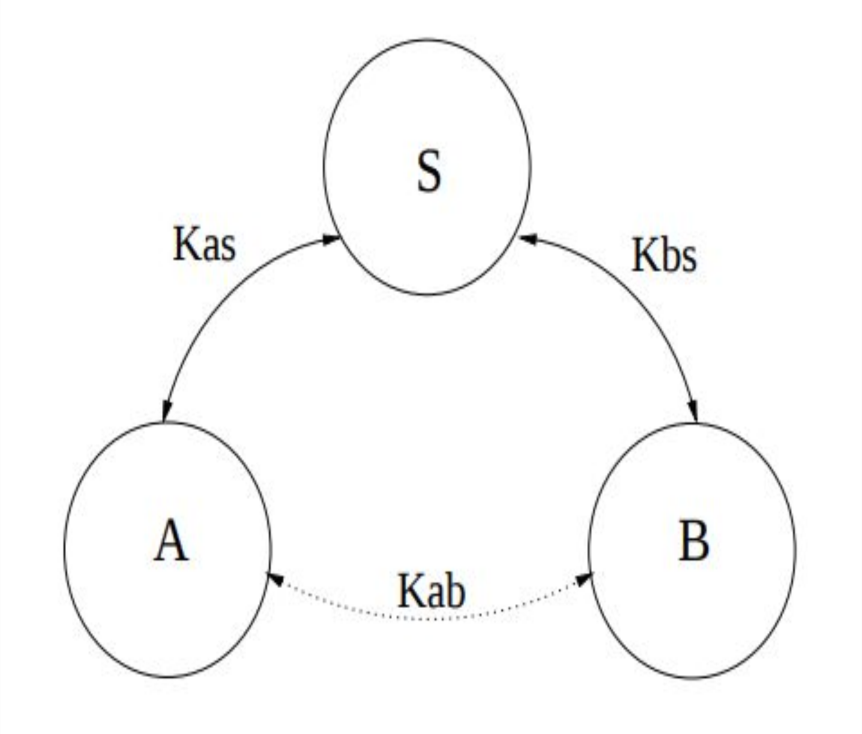
- Network authentication is a major concern these days to secure the communication from impersonation, eavesdropping, etc.
- To ensure the same, many protocols have been developed like Needham Schroeder protocol.

Needham Schroeder Protocol

- Proposed by Needham and Schroeder in 1978.
- This is a shared key authentication protocol.
- Designed to generate and propagate a session key.
- Forms a basis for Kerberos authentication protocol.

Basic Architecture





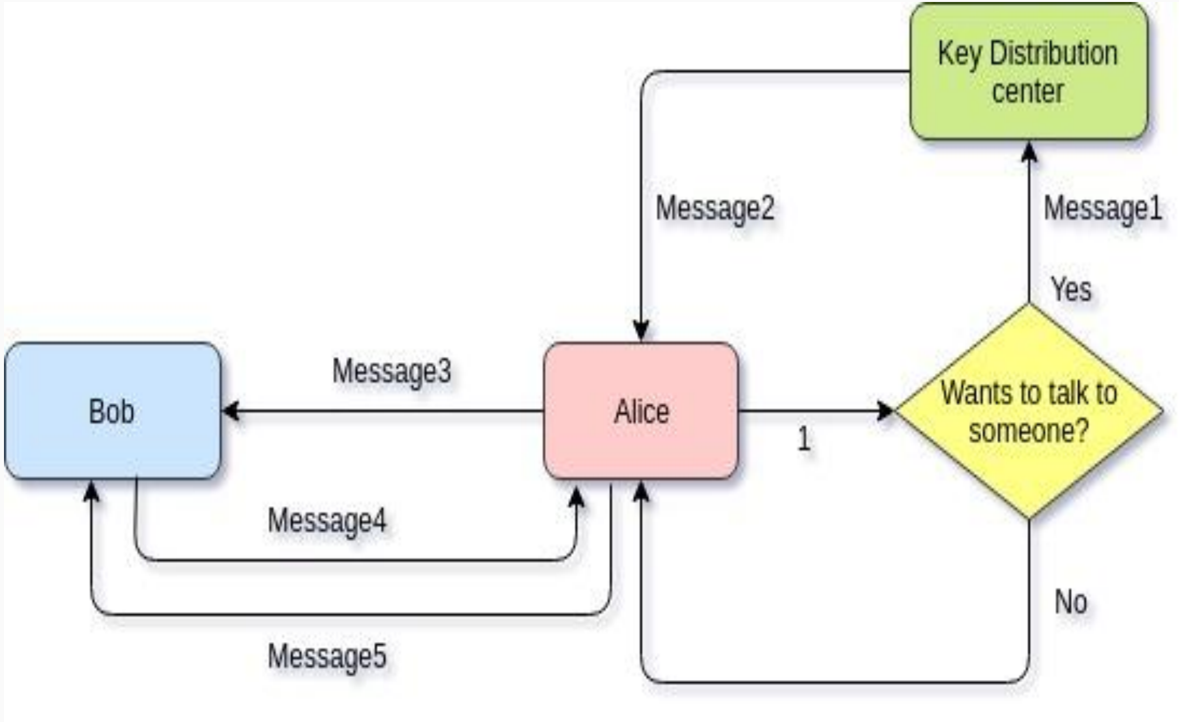
Components :

1. Initiator
2. Responder
3. Key Distribution Center

Messages Exchange

1. Alice -> KDC : Alice, Bob, R_A
2. KDC -> Alice : $E_{KA}[R_A, \text{Bob}, K_{AB}, E_{KB}[\text{Alice}, K_{AB}]]$
3. Alice -> Bob : $E_{KB}[\text{Alice}, K_{AB}]$
4. Bob -> Alice : $E_{KAB}[R_B]$
5. Alice -> Bob : $E_{KAB}[R_B - 1]$

Flow chart



Key Distribution center
Message2
Message1
Yes
Message3
Bob
Alice
1
Wants to talk to someone?
Message4
Message5
No

K_A 🔒 Encrypted with Alice-KDC secret key

K_B 🔒 Encrypted with Bob-KDC secret key

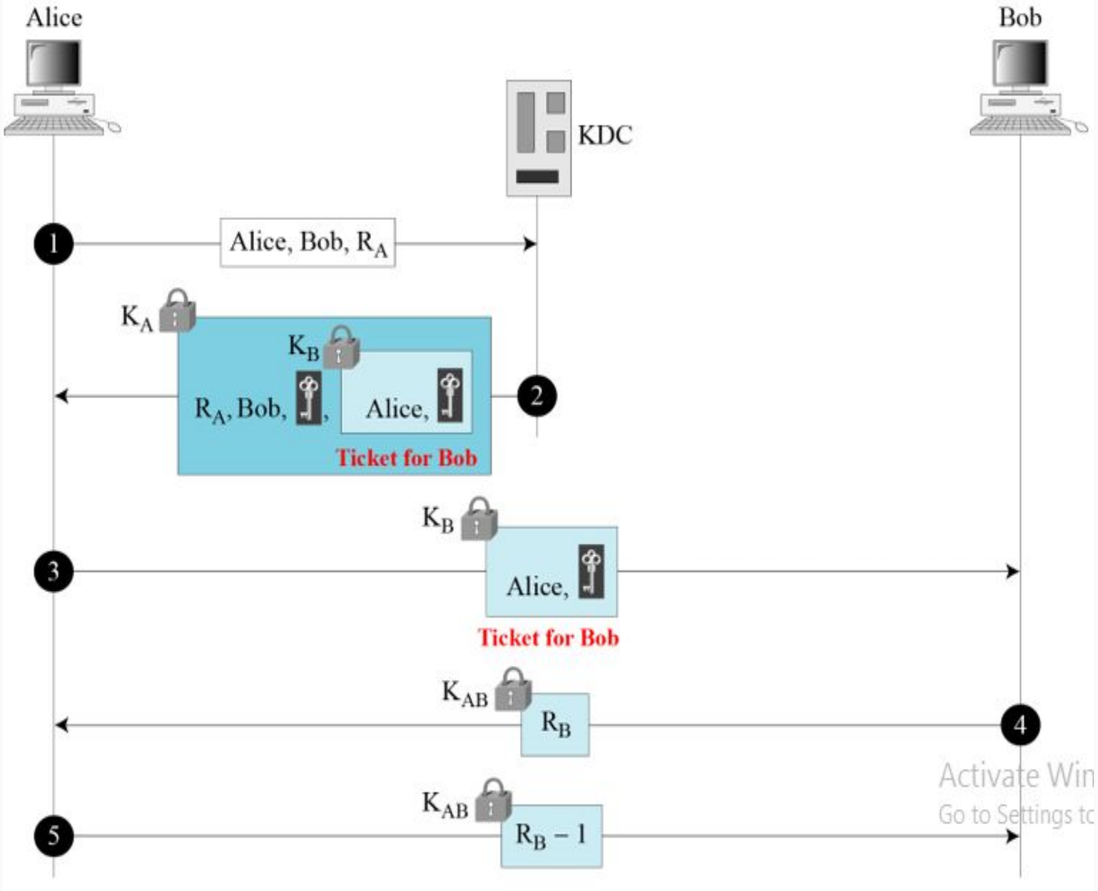
K_{AB} 🔒 Encrypted with Alice-Bob session key

🔑 Session key between Alice and Bob

KDC: Key-distribution center

R_A: Alice's nonce

R_B: Bob's nonce



Protocol Message Exchange Diagram

Experimental setup

- Implemented in python3 with following libraries :
    - Pycrypto
    - Netifaces
    - IP
    - Socket
    - Threading

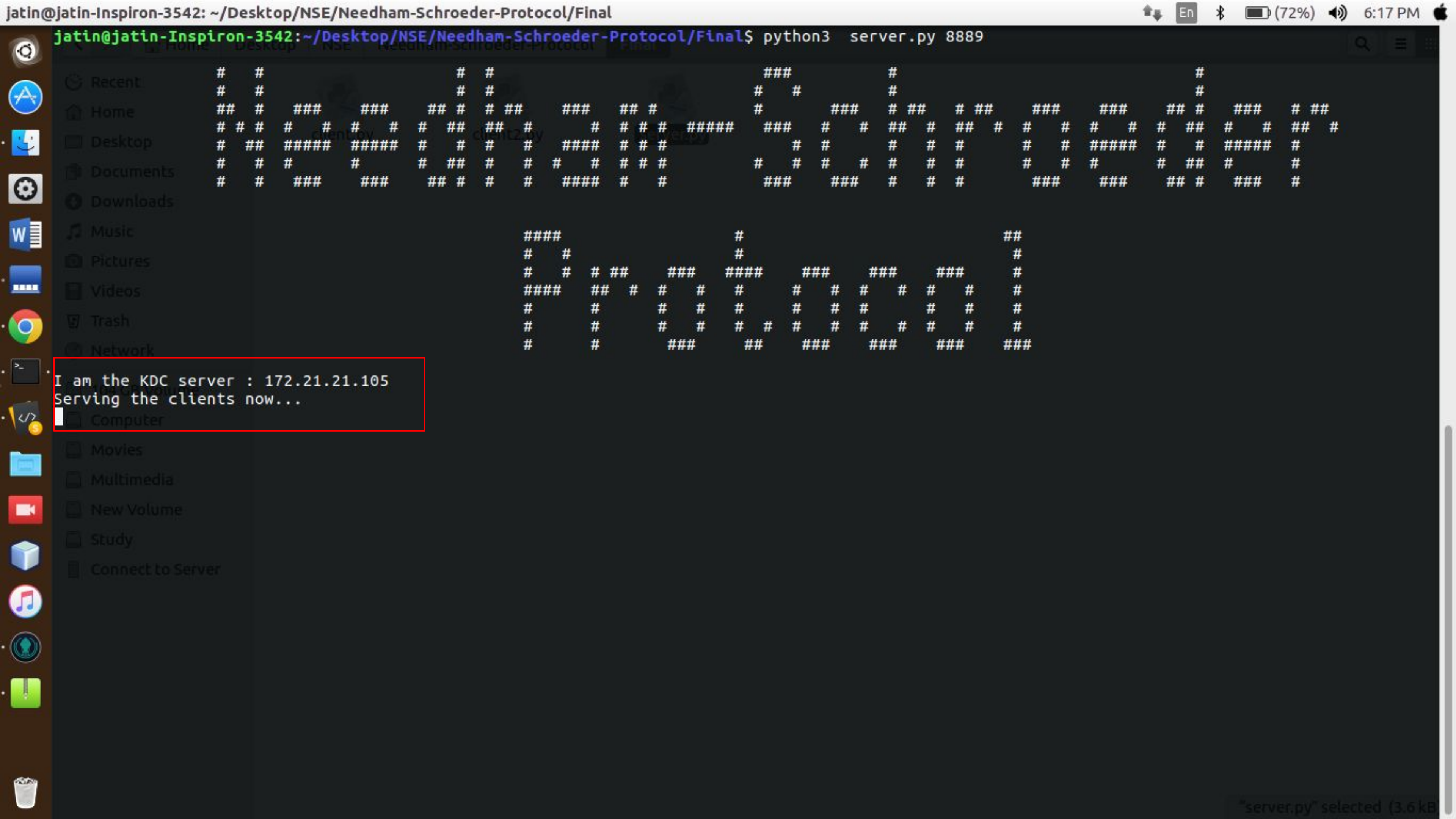
Protocol Instances - Actual Messages

- **Server[KDC]** Running at IP Address : 172.21.21.105

- **Alice** IP Address : 172.21.21.103
- **Bob** IP Address : 172.21.21.206
- **Cherry** IP Address : 172.21.21.106

Protocol Instances - Actual Messages

- **Server** is Running Persistently ………..
-

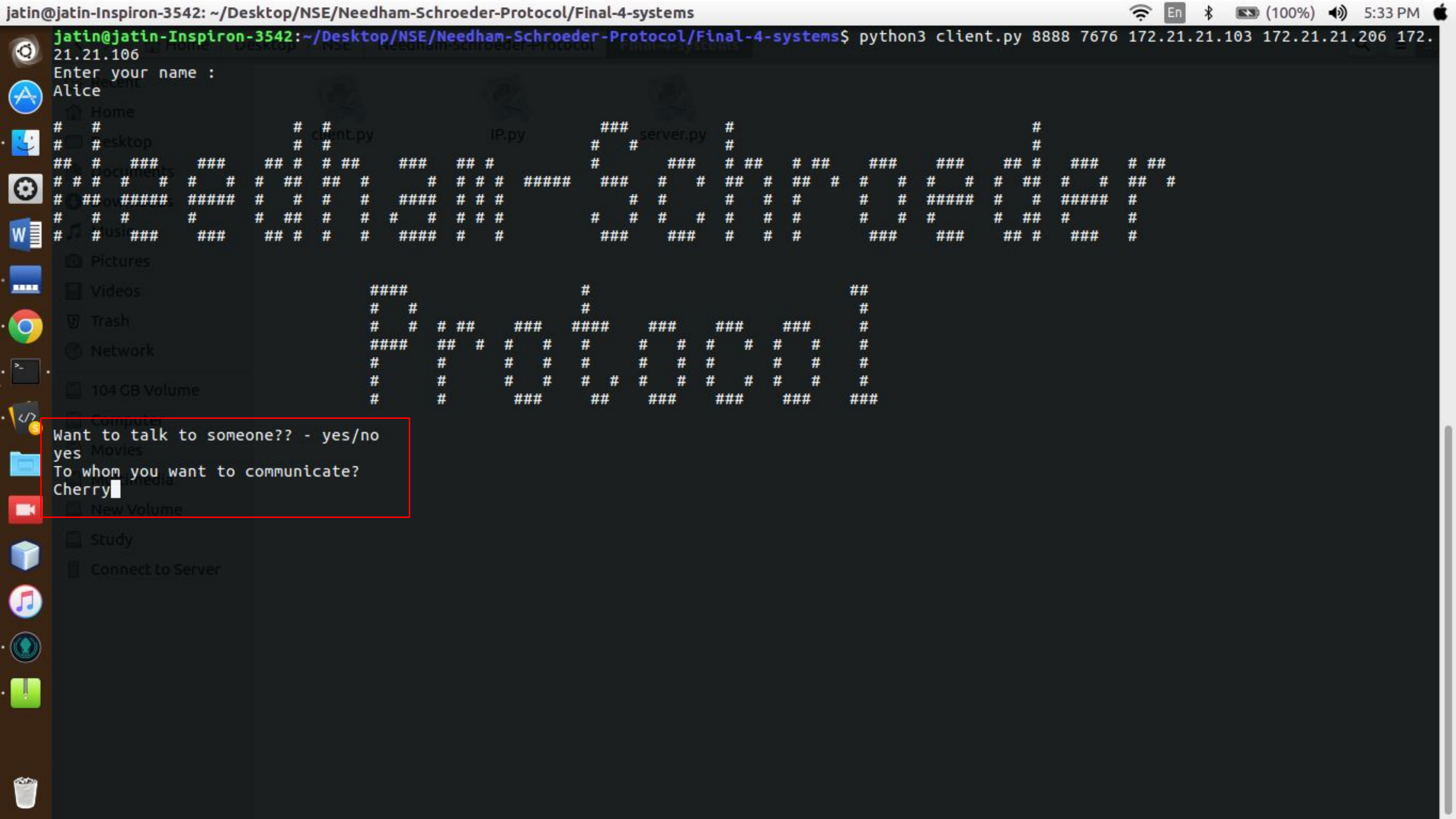


jatin@jatin-Inspiron-3542: ~/Desktop/NSE/Needham-Schroeder-Protocol/Final

```
jatin@jatin-Inspiron-3542:~/Desktop/NSE/Needham-Schroeder-Protocol/Final$ python3  server.py 8889
                 #   #                    #  #                            ###          #                               #
                 #   #                    #  #                           #   #         #                               #
                 ##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##   # ##    ###    ###    ## #   ###   # ##
                 # # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
                 #  ##  #####  #####  #   #  #   #   ####  # # #              #  #      #   #  #      #   #  #####  #   #  #####  #
                 #   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
                 #   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                                 ####                  #                          ##
                                                 #   #                 #                           #
                                                 #   #  # ##    ###   ####    ###    ###    ###    #
                                                 ####   ##  #  #   #   #     #   #  #   #  #   #   #
                                                 #      #      #   #   #     #   #  #      #   #   #
                                                 #      #      #   #   #  #  #   #  #   #  #   #   #
                                                 #      #       ###     ##    ###    ###    ###   ###

I am the KDC server : 172.21.21.105
Serving the clients now...
```

Protocol Instances - Actual Messages

- **Server[KDC]** is Running Persistently ………….
- Now **Alice** Want to Communicate with **Cherry**
-

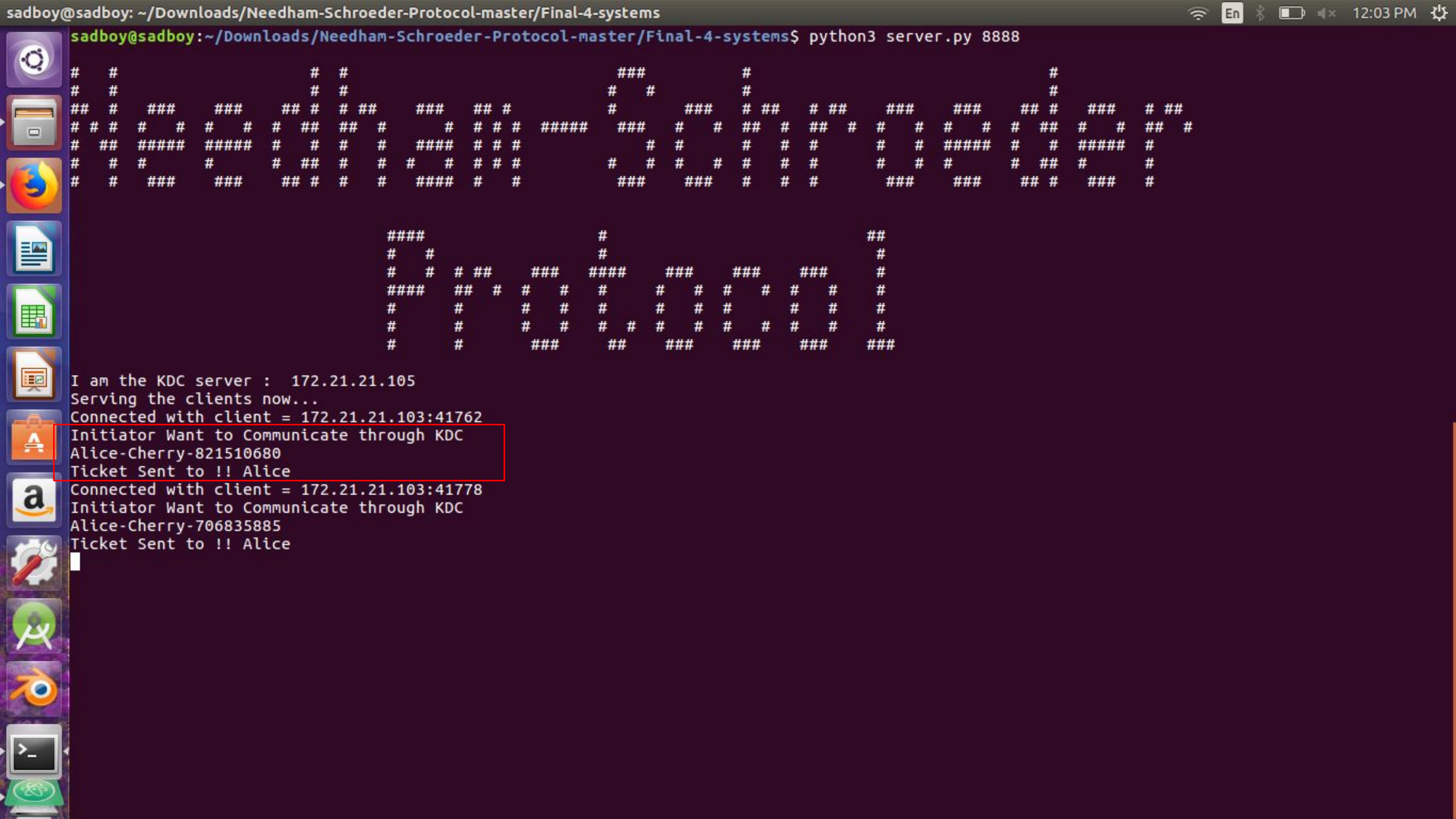


jatin@jatin-Inspiron-3542: ~/Desktop/NSE/Needham-Schroeder-Protocol/Final-4-systems
En
(100%)
5:33 PM

```
jatin@jatin-Inspiron-3542:~/Desktop/NSE/Needham-Schroeder-Protocol/Final-4-systems$ python3 client.py 8888 7676 172.21.21.103 172.21.21.206 172.
21.21.106
Enter your name :
Alice

#   #                    #  #                            ###          #                               #
#   #                    #  #                           #   #         #                               #
##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##   # ##    ###    ###    ## #   ###   # ##
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   #####   ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
yes
To whom you want to communicate?
Cherry
```

Protocol Instances - Actual Messages

- **Server** is Running Persistently ………….
- Now **Alice** Want to Communicate with **Cherry**
- **Alice-Cherry-NonceA** received at **KDC**
- Now **KDC** generates the Ticket for **Alice** which includes the TIcket of **Cherry.**
-

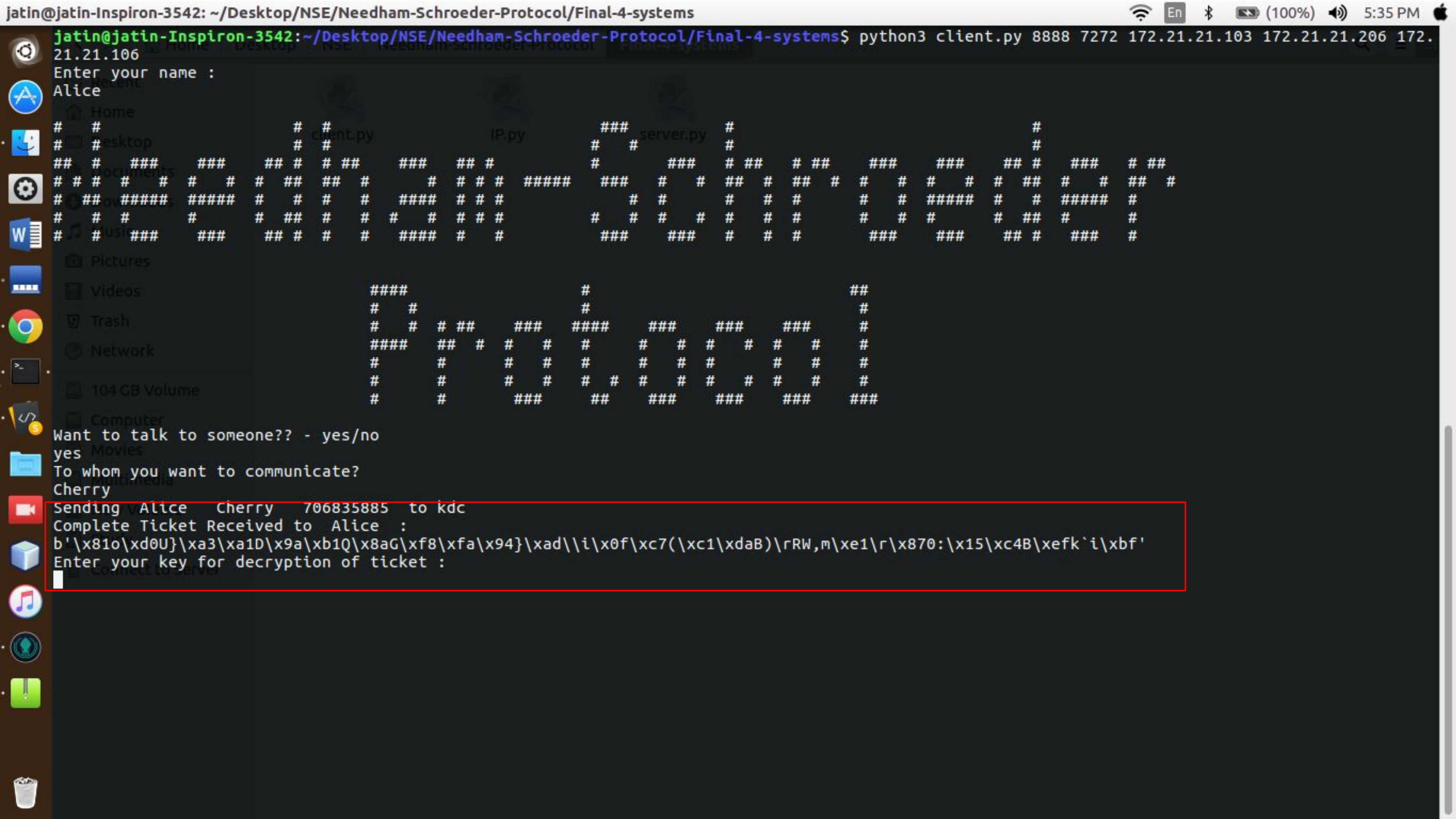


sadboy@sadboy: ~/Downloads/Needham-Schroeder-Protocol-master/Final-4-systems
En
12:03 PM

```
sadboy@sadboy:~/Downloads/Needham-Schroeder-Protocol-master/Final-4-systems$ python3 server.py 8888

#   #                    #  #                            ###          #                               #
#   #                    #  #                           #   #         #                               #
##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##   # ##    ###    ###    ## #   ###   # ##
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   #####   ###    ###    ###     #
                                 ####   ##  #  #   #    #     #   #  #   #  #   #    #
                                 #      #      #   #    #     #   #  #      #   #    #
                                 #      #      #   #    #  #  #   #  #   #  #   #    #
                                 #      #       ###      ##    ###    ###    ###    ###

I am the KDC server :  172.21.21.105
Serving the clients now...
Connected with client = 172.21.21.103:41762
Initiator Want to Communicate through KDC
Alice-Cherry-821510680
Ticket Sent to !! Alice
Connected with client = 172.21.21.103:41778
Initiator Want to Communicate through KDC
Alice-Cherry-706835885
Ticket Sent to !! Alice
```

Protocol Instances - Actual Messages

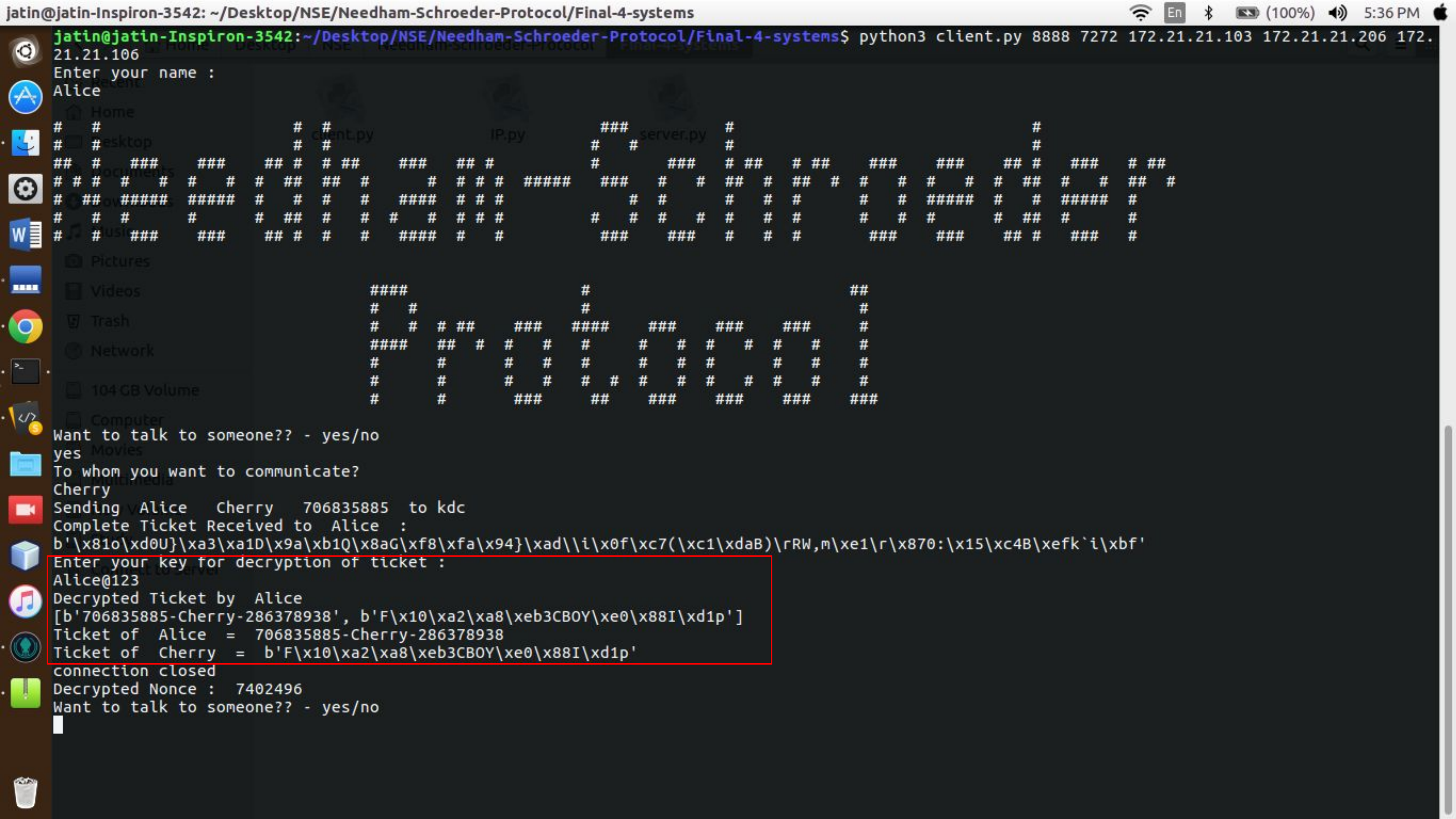
- **Server** is Running Persistently ………….
- Now **Alice** Want to Communicate with **Cherry**
- **Alice-Cherry-NonceA** received at **KDC**
- Now **KDC** generates the Ticket for **Alice** which includes the TIcket of **Cherry.**
-


jatin@jatin-Inspiron-3542: ~/Desktop/NSE/Needham-Schroeder-Protocol/Final-4-systems
En
(100%)
5:35 PM

```
jatin@jatin-Inspiron-3542:~/Desktop/NSE/Needham-Schroeder-Protocol/Final-4-systems$ python3 client.py 8888 7272 172.21.21.103 172.21.21.206 172.
21.21.106
Enter your name :
Alice

#   #                    #  #                            ###          #                               #
#   #                    #  #                           #   #         #                               #
##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##    # ##    ###    ###    ## #   ###   # ##
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   #####   ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
yes
To whom you want to communicate?
Cherry
Sending  Alice   Cherry   706835885  to kdc
Complete Ticket Received to  Alice  :
b'\x81o\xd0U}\xa3\xa1D\x9a\xb1Q\x8aG\xf8\xfa\x94}\xad\\i\x0f\xc7(\xc1\xdaB)\rRW,m\xe1\r\x870:\x15\xc4B\xefk`i\xbf'
Enter your key for decryption of ticket :
```

Protocol Instances - Actual Messages

- **Server** is Running Persistently ………….
- Now **Alice** Want to Communicate with **Cherry**
- **Alice-Cherry-NonceA** received at **KDC**
- Now **KDC** generates the Ticket for **Alice** which includes the TIcket of **Cherry.**
- Now **Alice** will Enter the **Private Key [Alice@123]** for decryption of ticket and **Alice** will send the Ticket for **Cherry**.

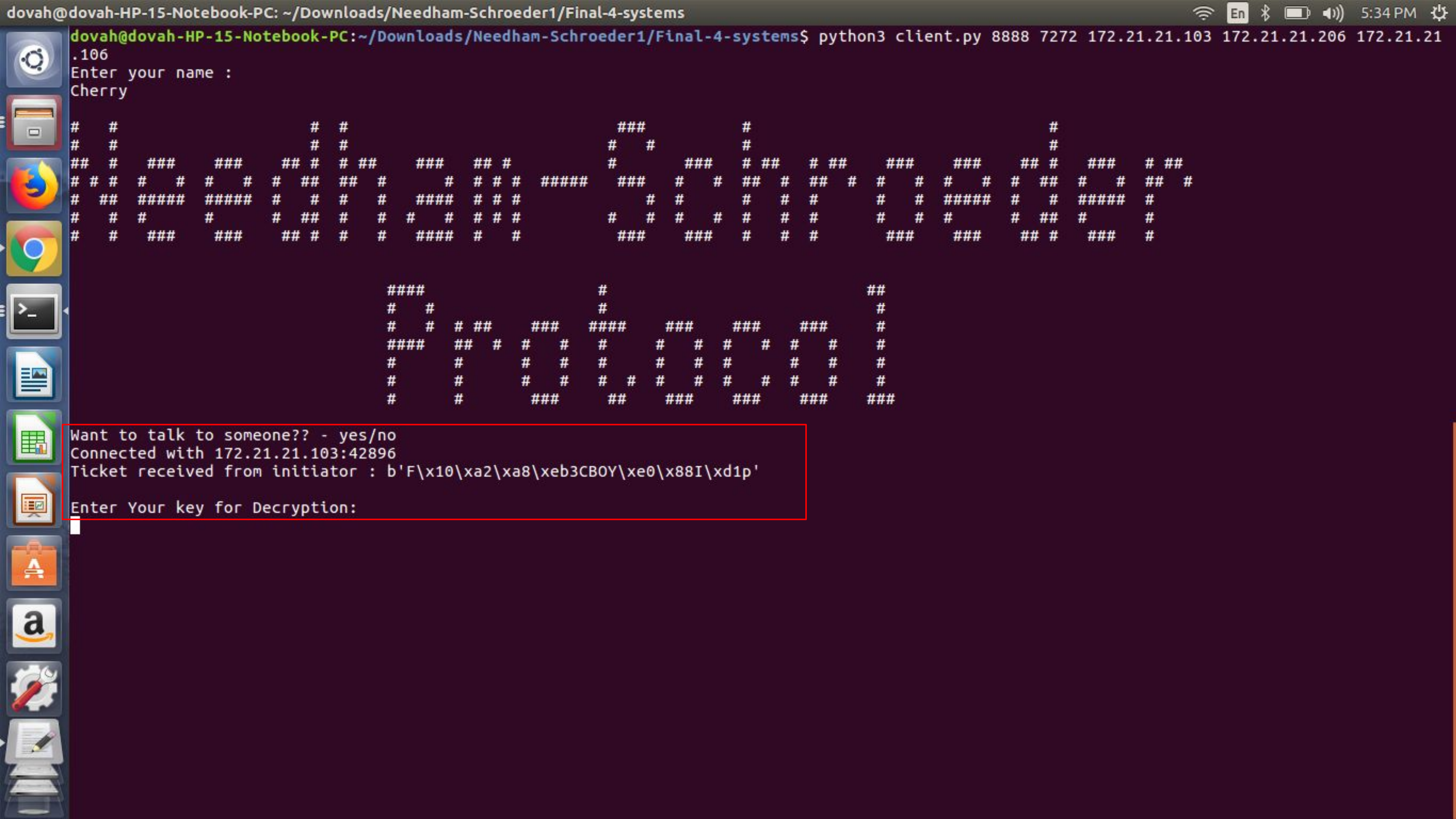


jatin@jatin-Inspiron-3542: ~/Desktop/NSE/Needham-Schroeder-Protocol/Final-4-systems
En
(100%)
5:36 PM

```
jatin@jatin-Inspiron-3542:~/Desktop/NSE/Needham-Schroeder-Protocol/Final-4-systems$ python3 client.py 8888 7272 172.21.21.103 172.21.21.206 172.
21.21.106
Enter your name :
Alice

#   #                    #  #                            ###          #                               #
#   #                    #  #                           #   #         #                               #
##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##   # ##    ###    ###    ## #   ###   # ##
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   ####    ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
yes
To whom you want to communicate?
Cherry
Sending  Alice   Cherry   706835885  to kdc
Complete Ticket Received to  Alice  :
b'\x81o\xd0U}\xa3\xa1D\x9a\xb1Q\x8aG\xf8\xfa\x94}\xad\\i\x0f\xc7(\xc1\xdaB)\rRW,m\xe1\r\x870:\x15\xc4B\xefk`i\xbf'
Enter your key for decryption of ticket :
Alice@123
Decrypted Ticket by  Alice
[b'706835885-Cherry-286378938', b'F\x10\xa2\xa8\xeb3CBOY\xe0\x88I\xd1p']
Ticket of  Alice  =  706835885-Cherry-286378938
Ticket of  Cherry  =  b'F\x10\xa2\xa8\xeb3CBOY\xe0\x88I\xd1p'
connection closed
Decrypted Nonce :  7402496
Want to talk to someone?? - yes/no
```

Protocol Instances - Actual Messages

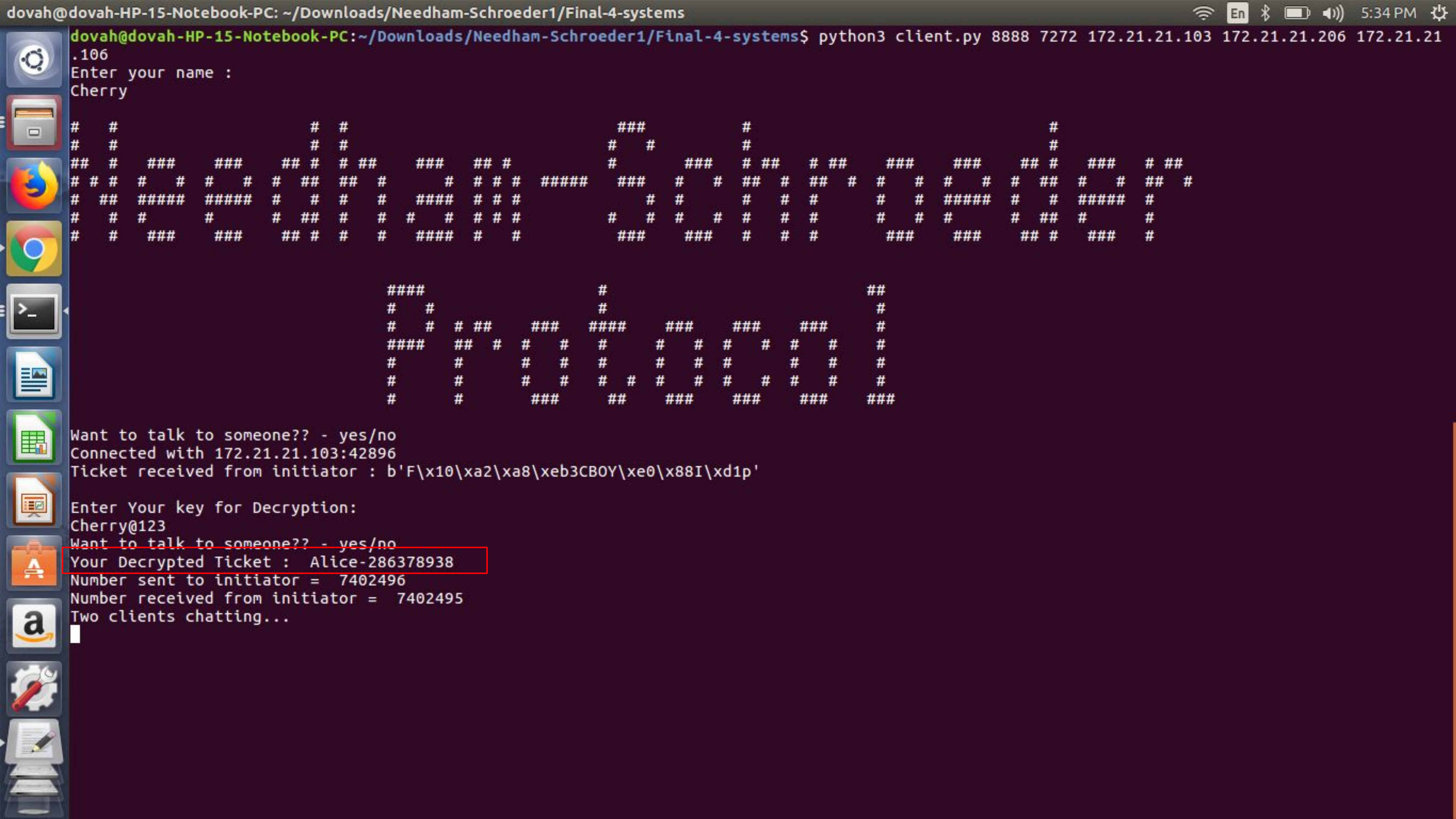
- **Server** is Running Persistently ………….
- Now **Alice** Want to Communicate with **Cherry**
- **Alice-Cherry-NonceA** received at **KDC**
- Now **KDC** generates the Ticket for **Alice** which includes the TIcket of **Cherry.**
- Now **Alice** will Enter the **Private Key [Alice@123]** for decryption of ticket and **Alice** will send the Ticket for **Cherry**.


dovah@dovah-HP-15-Notebook-PC: ~/Downloads/Needham-Schroeder1/Final-4-systems
En
5:34 PM

```
dovah@dovah-HP-15-Notebook-PC:~/Downloads/Needham-Schroeder1/Final-4-systems$ python3 client.py 8888 7272 172.21.21.103 172.21.21.206 172.21.21
.106
Enter your name :
Cherry

#   #                    #  #                            ###          #                               #
#   #                    #  #                           #   #         #                               #
##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##   # ##    ###    ###    ## #   ###   # ##
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   ####    ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
Connected with 172.21.21.103:42896
Ticket received from initiator : b'F\x10\xa2\xa8\xeb3CBOY\xe0\x88I\xd1p'

Enter Your key for Decryption:
```

Protocol Instances - Actual Messages

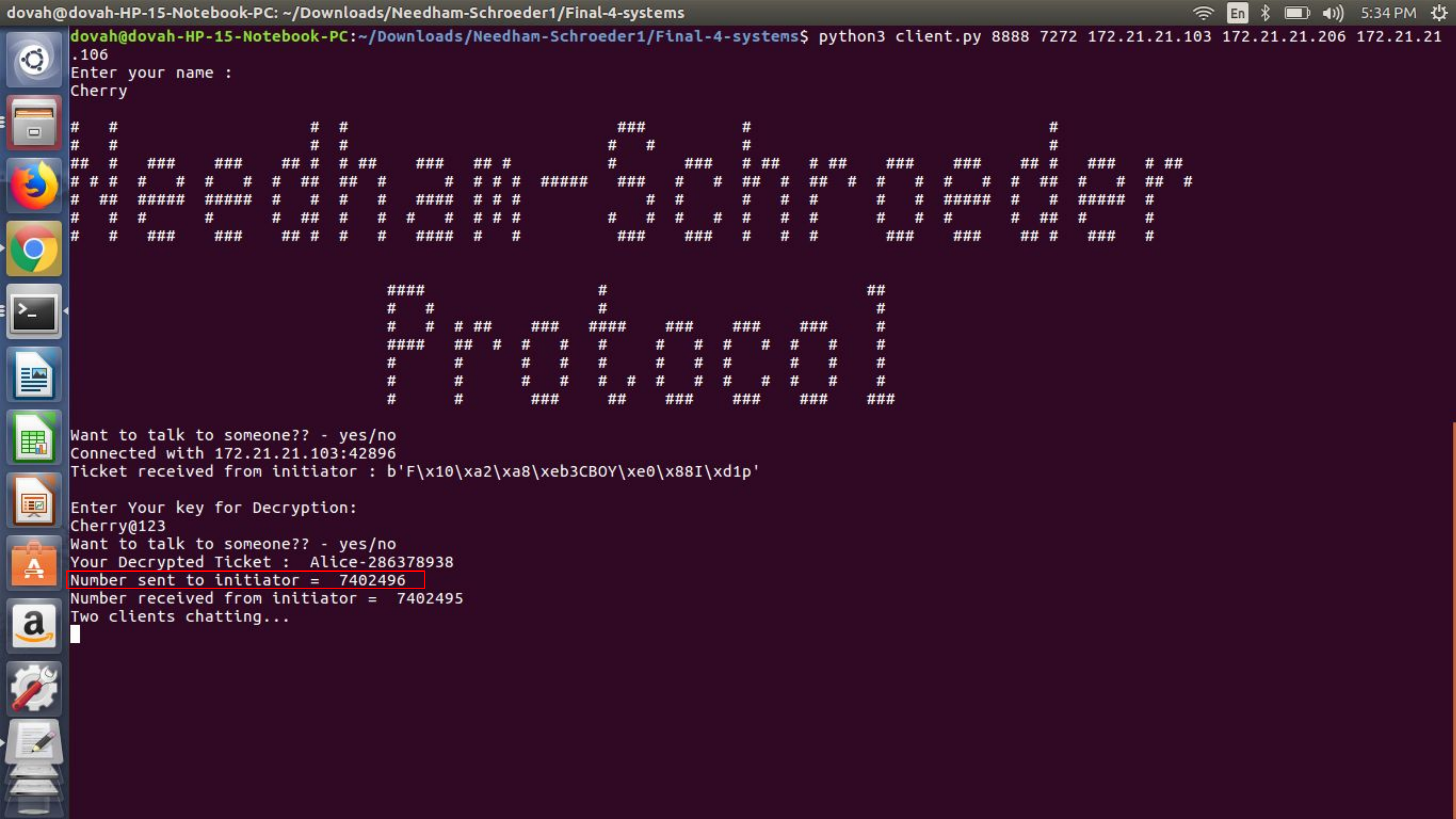
- **Server** is Running Persistently …………
- Now **Alice** Want to Communicate with **Cherry**
- **Alice-Cherry-NonceA** received at **KDC**
- Now **KDC** generates the Ticket for **Alice** which includes the TIcket of **Cherry.**
- Now **Alice** will Enter the **Private Key [Alice@123]** for decryption of ticket and **Alice** will send the Ticket for **Cherry**.
- Now **Cherry** will enter the **Private Key[Cherry@123]** for decryption of ticket
-


dovah@dovah-HP-15-Notebook-PC: ~/Downloads/Needham-Schroeder1/Final-4-systems
En
5:34 PM

```
dovah@dovah-HP-15-Notebook-PC:~/Downloads/Needham-Schroeder1/Final-4-systems$ python3 client.py 8888 7272 172.21.21.103 172.21.21.206 172.21.21
.106
Enter your name :
Cherry

#   #                    #  #                            ###          #                               #
#   #                    #  #                           #   #         #                               #
##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##   # ##    ###    ###    ## #   ###   # ##
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   ####    ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
Connected with 172.21.21.103:42896
Ticket received from initiator : b'F\x10\xa2\xa8\xeb3CBOY\xe0\x88I\xd1p'

Enter Your key for Decryption:
Cherry@123
Want to talk to someone?? - yes/no
Your Decrypted Ticket :  Alice-286378938
Number sent to initiator =  7402496
Number received from initiator =  7402495
Two clients chatting...
```

Protocol Instances - Actual Messages

- Now **KDC** generates the Ticket for **Alice** which includes the TIcket of **Cherry.**
- Now **Alice** will Enter the **Private Key [Alice@123]** for decryption of ticket and **Alice** will send the Ticket for **Cherry**.
- Now **Cherry** will enter the **Private Key[Cherry@123]** for decryption of ticket
- Now **Cherry** will Random **NonceC** to **Alice.**

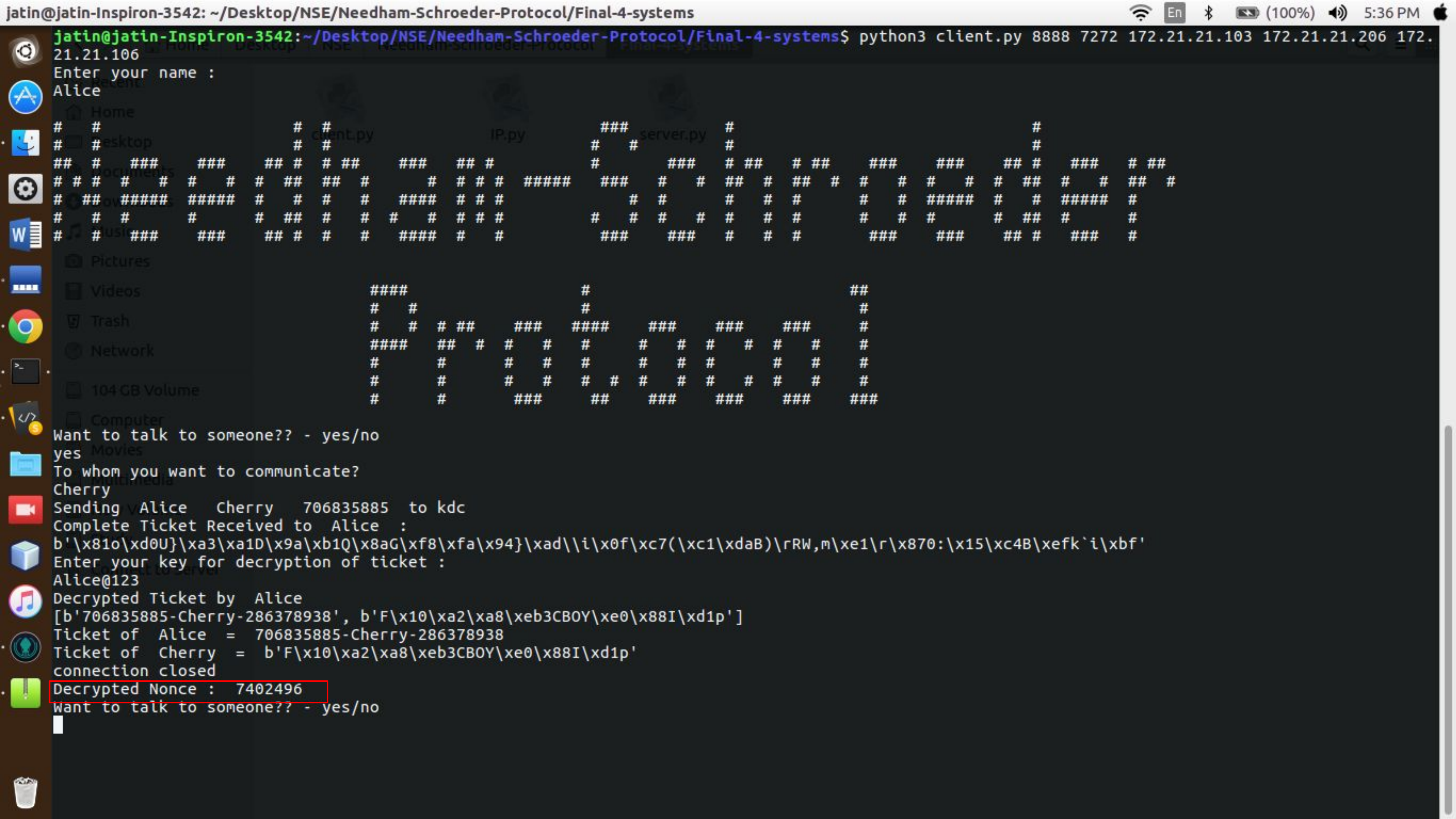


dovah@dovah-HP-15-Notebook-PC: ~/Downloads/Needham-Schroeder1/Final-4-systems
En
5:34 PM

```
dovah@dovah-HP-15-Notebook-PC:~/Downloads/Needham-Schroeder1/Final-4-systems$ python3 client.py 8888 7272 172.21.21.103 172.21.21.206 172.21.21
.106
Enter your name :
Cherry

#   #                    #  #                            ###          #                               #
#   #                    #  #                           #   #         #                               #
##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##   # ##    ###    ###    ## #   ###   # ##
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   ####    ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
Connected with 172.21.21.103:42896
Ticket received from initiator : b'F\x10\xa2\xa8\xeb3CBOY\xe0\x88I\xd1p'

Enter Your key for Decryption:
Cherry@123
Want to talk to someone?? - yes/no
Your Decrypted Ticket :  Alice-286378938
Number sent to initiator =  7402496
Number received from initiator =  7402495
Two clients chatting...
```

Protocol Instances - Actual Messages

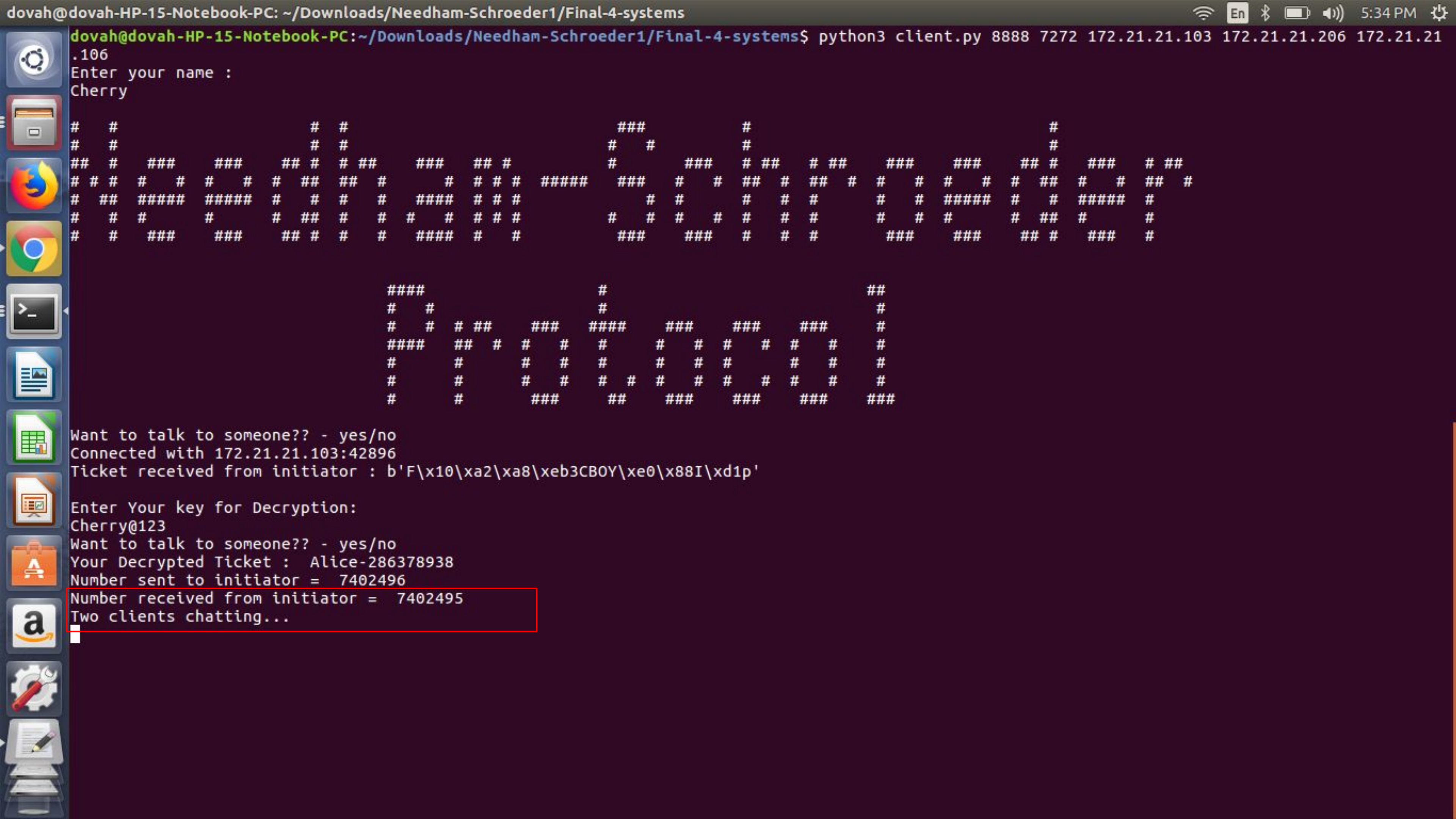
- Now **KDC** generates the Ticket for **Alice** which includes the TIcket of **Cherry.**
- Now **Alice** will Enter the **Private Key [Alice@123]** for decryption of ticket and **Alice** will send the Ticket for **Cherry**.
- Now **Cherry** will enter the **Private Key[Cherry@123]** for decryption of ticket
- Now **Cherry** will Random **NonceC** encrypted by **Session key** to **Alice.**
- **Alice** received **NonceC** , send back **NonceC - 1** to Cherry.


jatin@jatin-Inspiron-3542: ~/Desktop/NSE/Needham-Schroeder-Protocol/Final-4-systems
En
(100%)
5:36 PM

```
jatin@jatin-Inspiron-3542:~/Desktop/NSE/Needham-Schroeder-Protocol/Final-4-systems$ python3 client.py 8888 7272 172.21.21.103 172.21.21.206 172.
21.21.106
Enter your name :
Alice

#   #                    #  #                            ###          #                               #
#   #                    #  #                           #   #         #                               #
##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##   # ##    ###    ###    ## #   ###   # ##
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   ####    ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
yes
To whom you want to communicate?
Cherry
Sending  Alice   Cherry   706835885  to kdc
Complete Ticket Received to  Alice  :
b'\x81o\xd0U}\xa3\xa1D\x9a\xb1Q\x8aG\xf8\xfa\x94}\xad\\i\x0f\xc7(\xc1\xdaB)\rRW,m\xe1\r\x870:\x15\xc4B\xefk`i\xbf'
Enter your key for decryption of ticket :
Alice@123
Decrypted Ticket by  Alice
[b'706835885-Cherry-286378938', b'F\x10\xa2\xa8\xeb3CBOY\xe0\x88I\xd1p']
Ticket of  Alice  =  706835885-Cherry-286378938
Ticket of  Cherry  =  b'F\x10\xa2\xa8\xeb3CBOY\xe0\x88I\xd1p'
connection closed
Decrypted Nonce :  7402496
Want to talk to someone?? - yes/no
```

Protocol Instances - Actual Messages

- Now **Alice** will Enter the **Private Key [Alice@123]** for decryption of ticket and **Alice** will send the Ticket for **Cherry**.
- Now **Cherry** will enter the **Private Key[Cherry@123]** for decryption of ticket
- Now **Cherry** will Random **NonceC** encrypted by **Session key** to **Alice.**
- **Alice** received **NonceC** , send back **NonceC - 1** to Cherry.
- **Cherry** received the **NonceC - 1** from Alice.

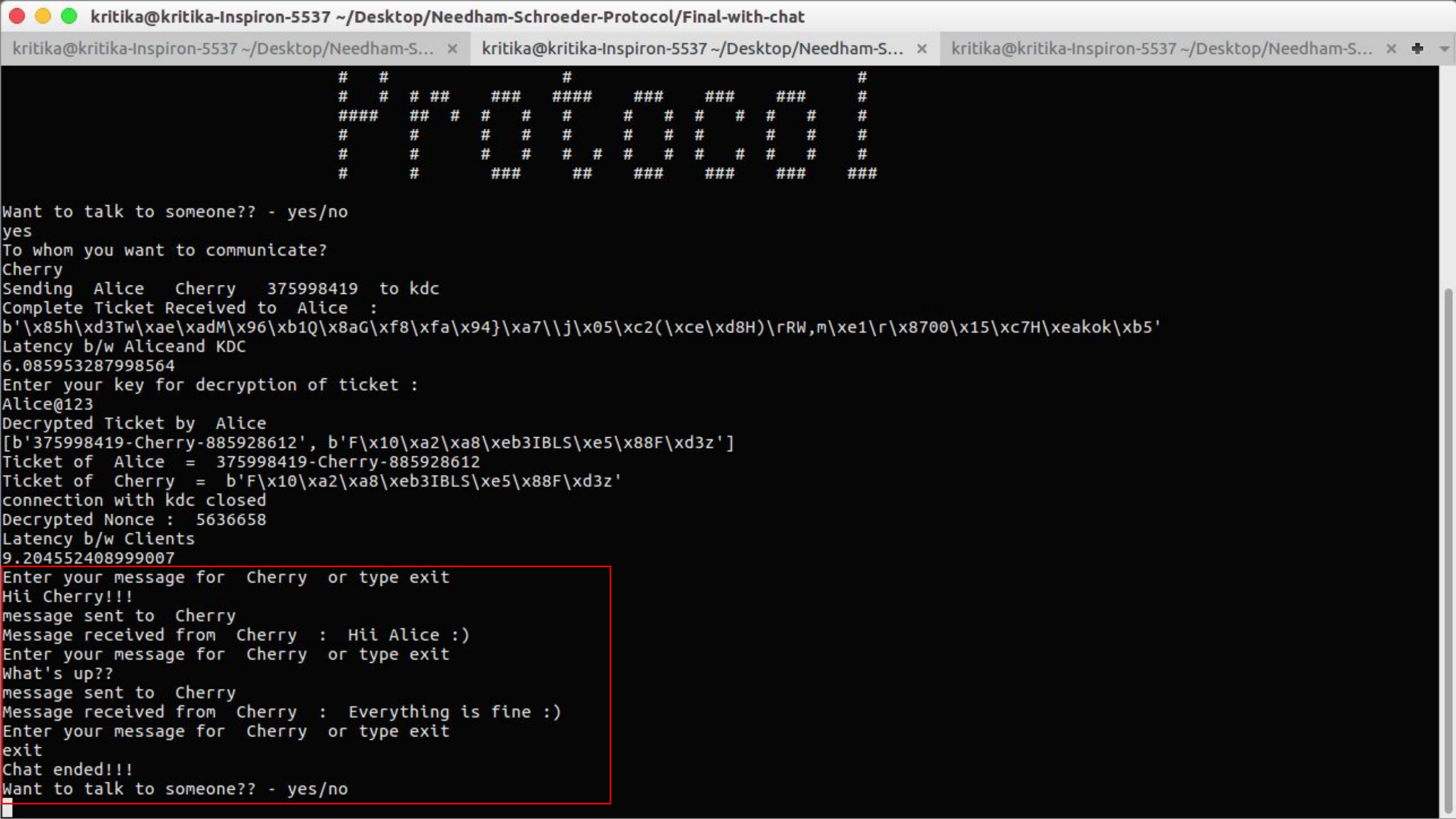


dovah@dovah-HP-15-Notebook-PC: ~/Downloads/Needham-Schroeder1/Final-4-systems
En
5:34 PM

```
dovah@dovah-HP-15-Notebook-PC:~/Downloads/Needham-Schroeder1/Final-4-systems$ python3 client.py 8888 7272 172.21.21.103 172.21.21.206 172.21.21
.106
Enter your name :
Cherry

#   #                    #  #                            ###          #                               #
#   #                    #  #                           #   #         #                               #
##  #   ###    ###    ## #  # ##    ###   ## #          #       ###   # ##   # ##    ###    ###    ## #   ###   # ##
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   ####    ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
Connected with 172.21.21.103:42896
Ticket received from initiator : b'F\x10\xa2\xa8\xeb3CBOY\xe0\x88I\xd1p'

Enter Your key for Decryption:
Cherry@123
Want to talk to someone?? - yes/no
Your Decrypted Ticket :  Alice-286378938
Number sent to initiator =  7402496
Number received from initiator =  7402495
Two clients chatting...
```

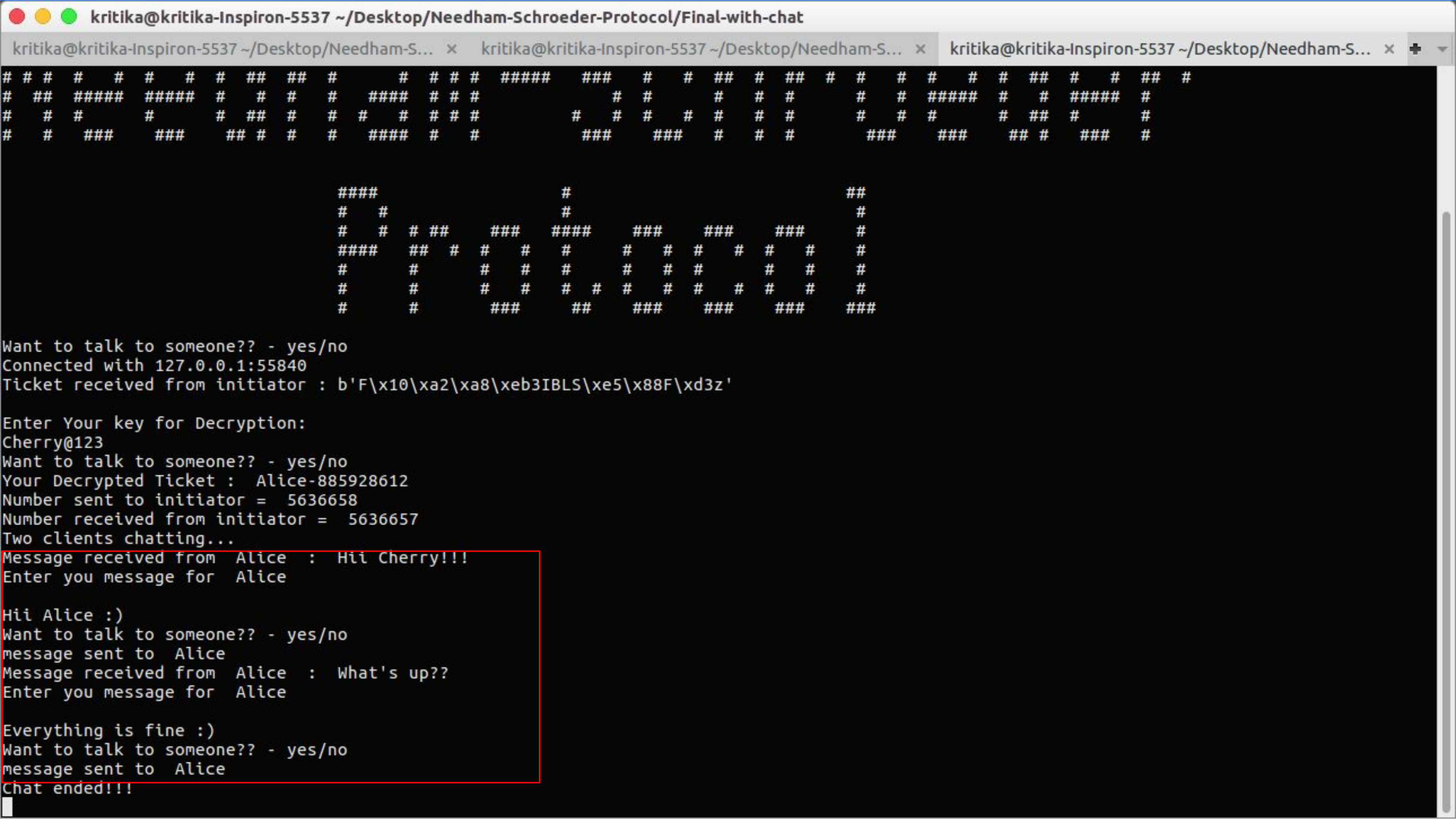
Protocol Instances - Actual Messages

- Now **Cherry** will Random **NonceC** encrypted by **Session key** to **Alice.**
- **Alice** received **NonceC** , send back **NonceC - 1** to Cherry.
- **Cherry** received the **NonceC - 1** from Alice.
- Now **Session Key** is established b/w **Alice and Cherry** . So they can now do chatting with each other.



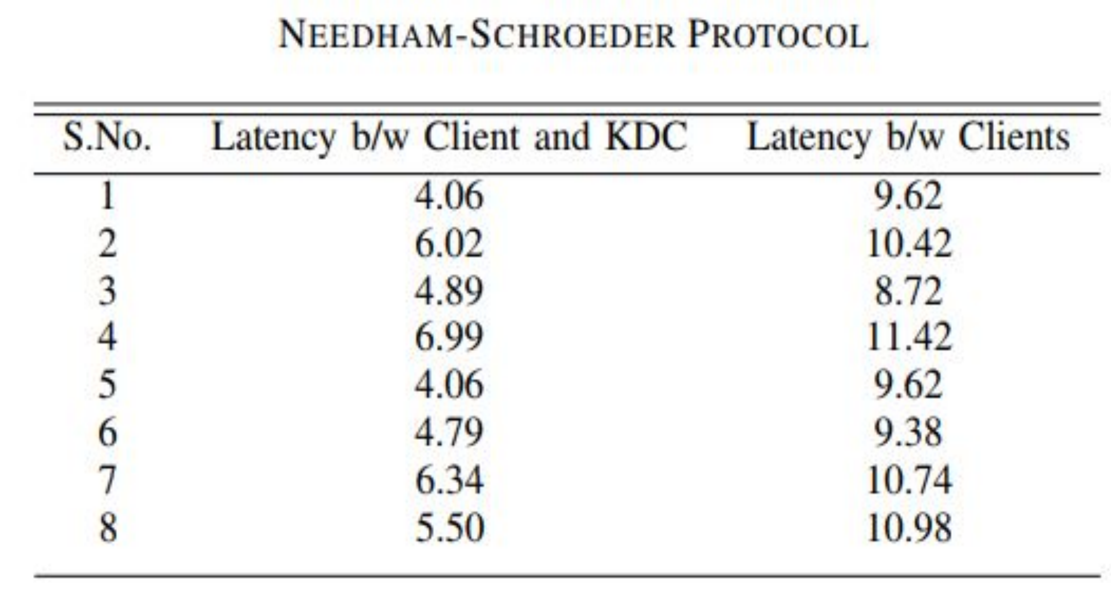
kritika@kritika-Inspiron-5537 ~/Desktop/Needham-Schroeder-Protocol/Final-with-chat
kritika@kritika-Inspiron-5537 ~/Desktop/Needham-S...
kritika@kritika-Inspiron-5537 ~/Desktop/Needham-S...
kritika@kritika-Inspiron-5537 ~/Desktop/Needham-S...

```
                                 #   #                 #                            #
                                 #   #  # ##    ###   ####    ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
yes
To whom you want to communicate?
Cherry
Sending  Alice   Cherry   375998419  to kdc
Complete Ticket Received to  Alice  :
b'\x85h\xd3Tw\xae\xadM\x96\xb1Q\x8aG\xf8\xfa\x94}\xa7\\j\x05\xc2(\xce\xd8H)\rRW,m\xe1\r\x8700\x15\xc7H\xeakok\xb5'
Latency b/w Aliceand KDC
6.085953287998564
Enter your key for decryption of ticket :
Alice@123
Decrypted Ticket by  Alice
[b'375998419-Cherry-885928612', b'F\x10\xa2\xa8\xeb3IBLS\xe5\x88F\xd3z']
Ticket of  Alice  =  375998419-Cherry-885928612
Ticket of  Cherry  =  b'F\x10\xa2\xa8\xeb3IBLS\xe5\x88F\xd3z'
connection with kdc closed
Decrypted Nonce :  5636658
Latency b/w Clients
9.204552408999007
Enter your message for  Cherry  or type exit
Hii Cherry!!!
message sent to  Cherry
Message received from  Cherry  :  Hii Alice :)
Enter your message for  Cherry  or type exit
What's up??
message sent to  Cherry
Message received from  Cherry  :  Everything is fine :)
Enter your message for  Cherry  or type exit
exit
Chat ended!!!
Want to talk to someone?? - yes/no
```


kritika@kritika-Inspiron-5537 ~/Desktop/Needham-Schroeder-Protocol/Final-with-chat
kritika@kritika-Inspiron-5537 ~/Desktop/Needham-S...
kritika@kritika-Inspiron-5537 ~/Desktop/Needham-S...
kritika@kritika-Inspiron-5537 ~/Desktop/Needham-S...

```
# # #  #   #  #   #  #  ##  ##  #      #  # # #  #####   ###   #   #  ##  #  ##  #  #   #  #   #  #  ##  #   #  ##  #
#  ##  #####  #####  #   #  #   #   ####  # # #             #  #      #   #  #      #   #  #####  #   #  #####  #
#   #  #      #      #  ##  #   #  #   #  # # #         #   #  #   #  #   #  #      #   #  #      #  ##  #      #
#   #   ###    ###    ## #  #   #   ####  #   #          ###    ###   #   #  #       ###    ###    ## #   ###   #


                                 ####                  #                           ##
                                 #   #                 #                            #
                                 #   #  # ##    ###   ####    ###    ###    ###     #
                                 ####   ##  #  #   #   #     #   #  #   #  #   #    #
                                 #      #      #   #   #     #   #  #      #   #    #
                                 #      #      #   #   #  #  #   #  #   #  #   #    #
                                 #      #       ###     ##    ###    ###    ###    ###

Want to talk to someone?? - yes/no
Connected with 127.0.0.1:55840
Ticket received from initiator : b'F\x10\xa2\xa8\xeb3IBLS\xe5\x88F\xd3z'

Enter Your key for Decryption:
Cherry@123
Want to talk to someone?? - yes/no
Your Decrypted Ticket :  Alice-885928612
Number sent to initiator =  5636658
Number received from initiator =  5636657
Two clients chatting...
Message received from  Alice  :  Hii Cherry!!!
Enter you message for  Alice

Hii Alice :)
Want to talk to someone?? - yes/no
message sent to  Alice
Message received from  Alice  :  What's up??
Enter you message for  Alice

Everything is fine :)
Want to talk to someone?? - yes/no
message sent to  Alice
Chat ended!!!
```

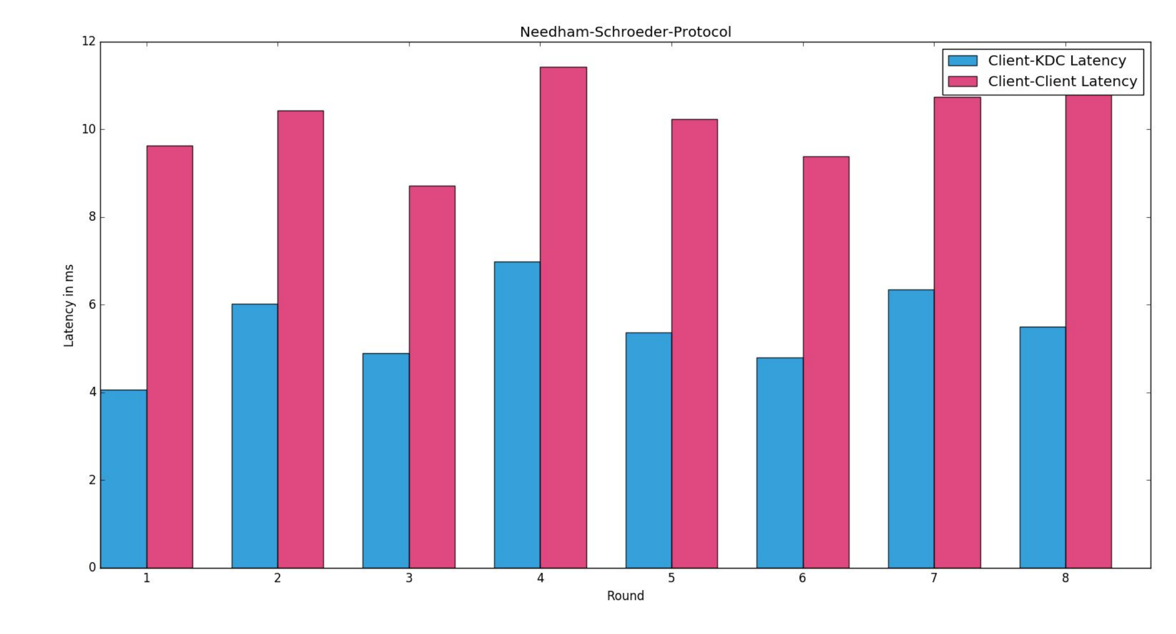
Latency Analysis



Needham-Schroeder Protocol

S.No.	Latency b/w Client and KDC	Latency b/w Clients
1	4.06	9.62
2	6.02	10.42
3	4.89	8.72
4	6.99	11.42
5	4.06	9.62
6	4.79	9.38
7	6.34	10.74
8	5.50	10.98

Latency Plot



Disadvantages

- If session key is compromised and ticket to Bob is recorded, then intruder can impersonate initiator by carrying out last 3 steps.

- This is a replay attack mechanism , as there is no nonce in message 3 , the attacker can replay the message Alice -> Bob : E_{KB}[Alice, K_{AB}] and Bob would accept it as legitimate as it doesn't know the freshness.

- Single point of failure.

Conclusion

- This was indeed a great learning Experience for all of us.
- Needham schroeder protocol has been successfully implemented.
- Authentication for further communication has been done.

Thank You!