SF LAB - 07 REPORT

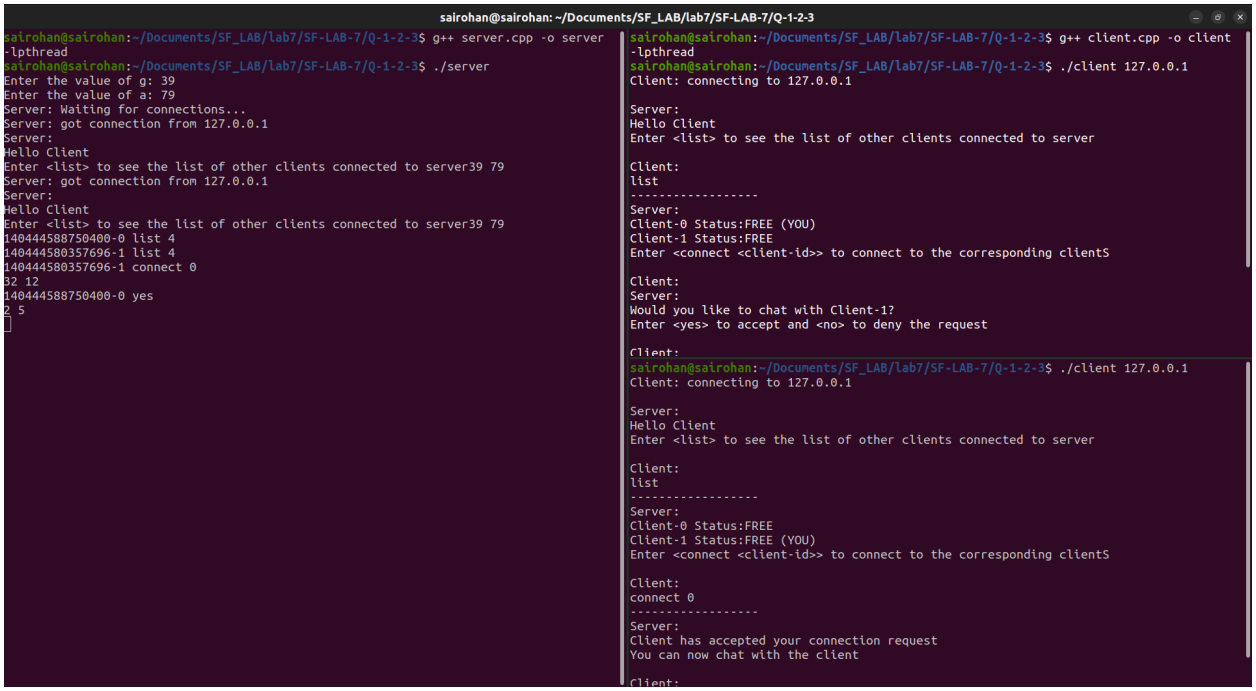
Sai Rohan Harshavardhan Vuppala (19CS02004)

Kamasali Koushik Kumar (19CS02006)

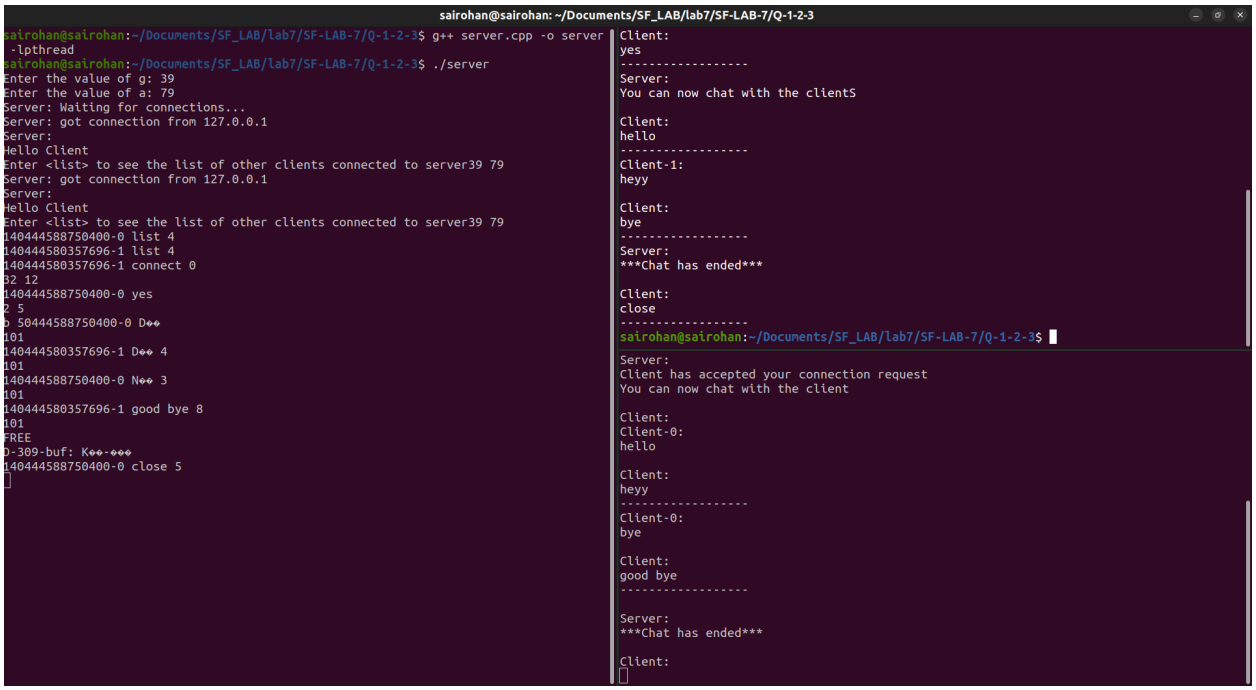
Question 1, 2, 3

Chat application by sending messages via server. Encryption is done using RC4 Cipher and the key is decided using Diffie Hellman Key exchange.

- Two Clients chatting with each other with help of server.



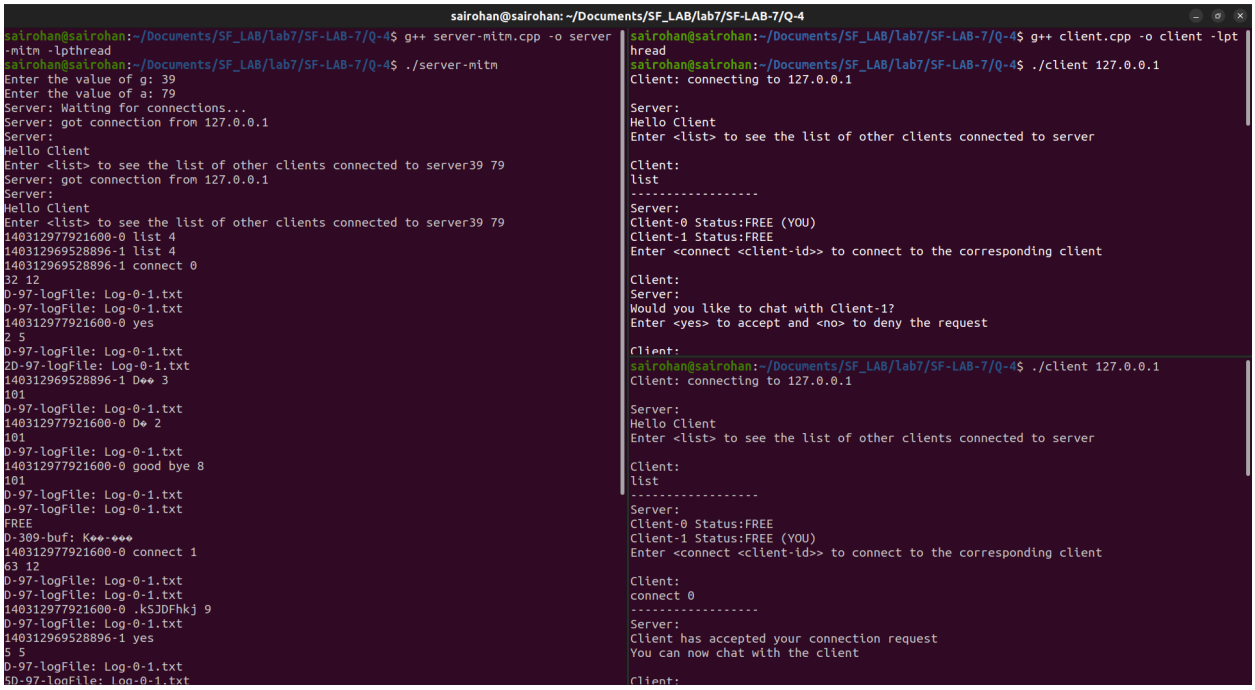
- Encrypted messages printed in the server's terminal where as decryted messages can be seen at client's end.

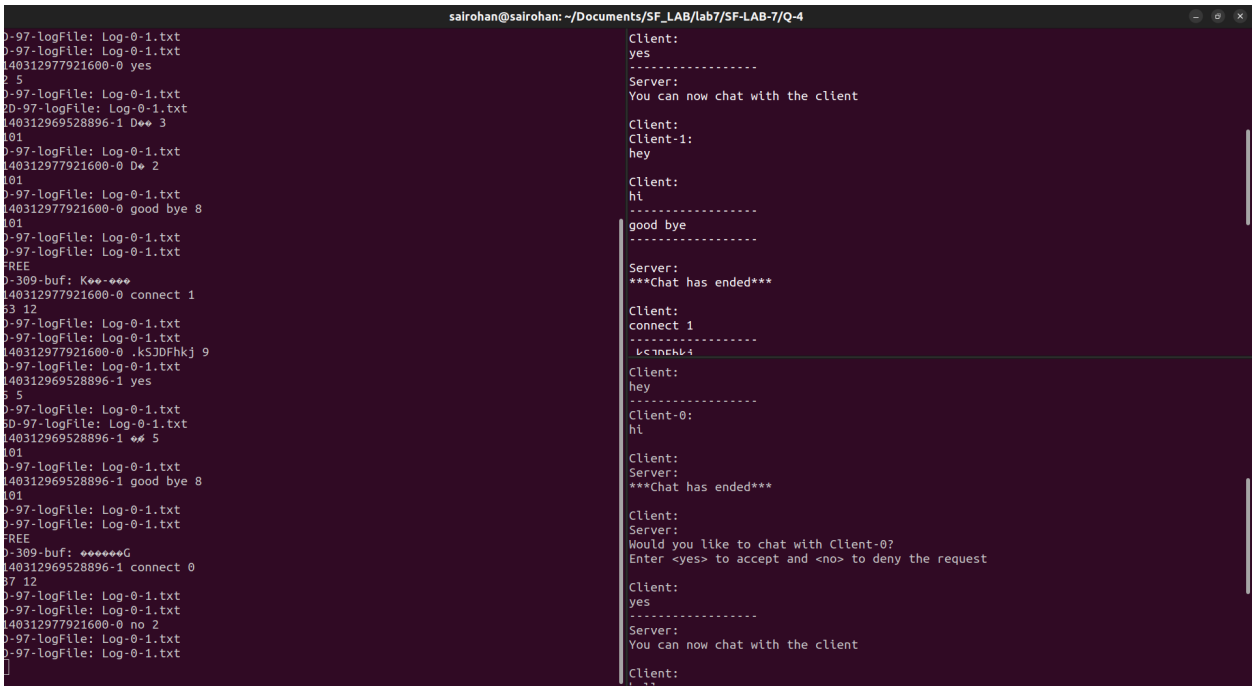


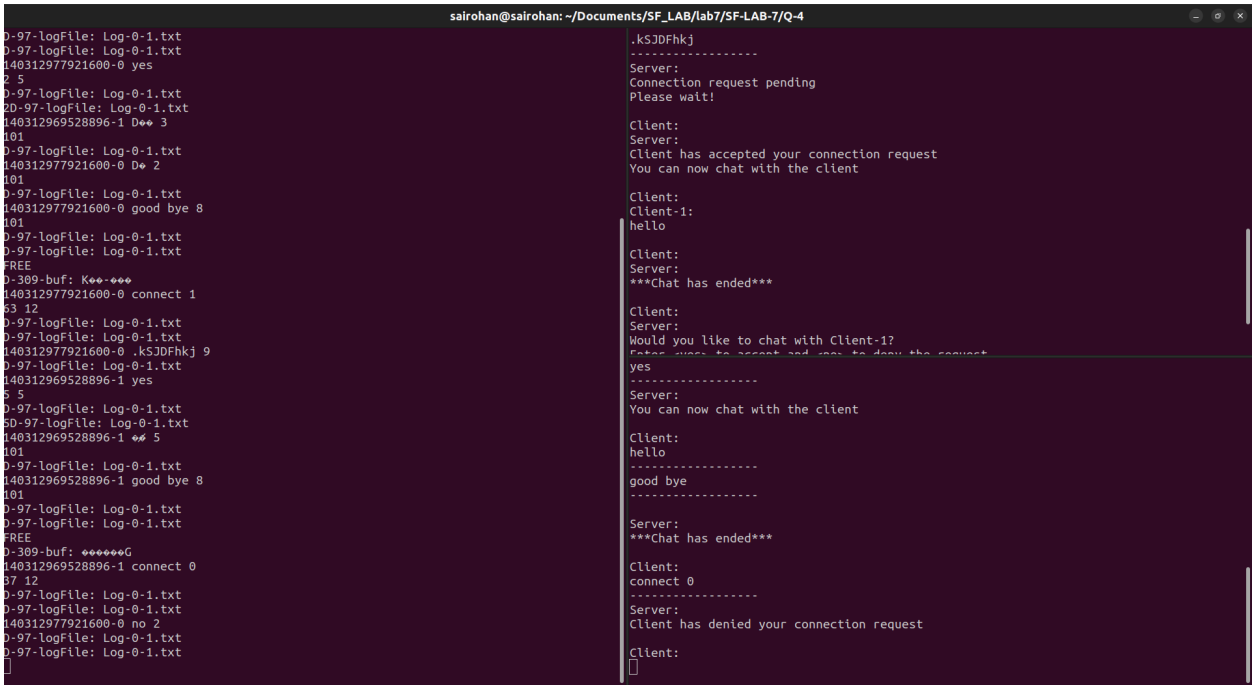
Question 4

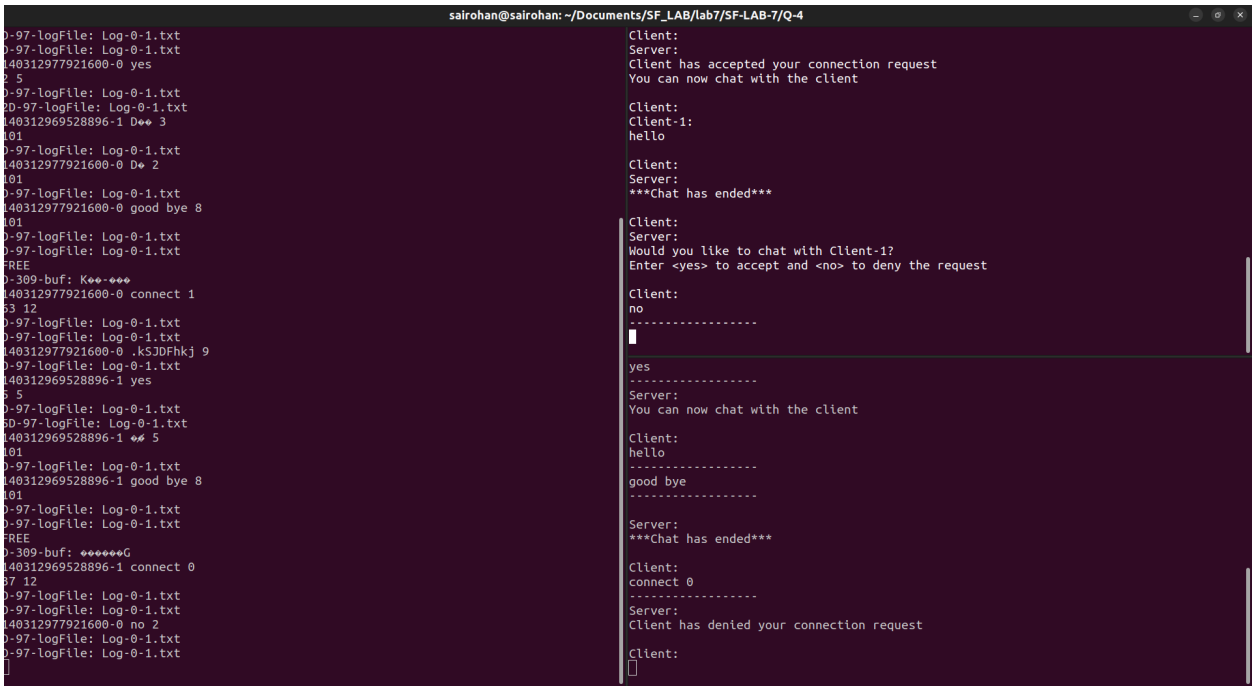
- While clients chat with each other, MITM intercepts the messages and these messages are saved in log files.
- We Used Discrete Logarithm method which helps MITM to find the value of key and decryt the messages present in log file to decrypted file.
- MITM(man in the middle) is implemented in the chat Application as follows :-

- Log files are being genereated for two clients chatting with each other.

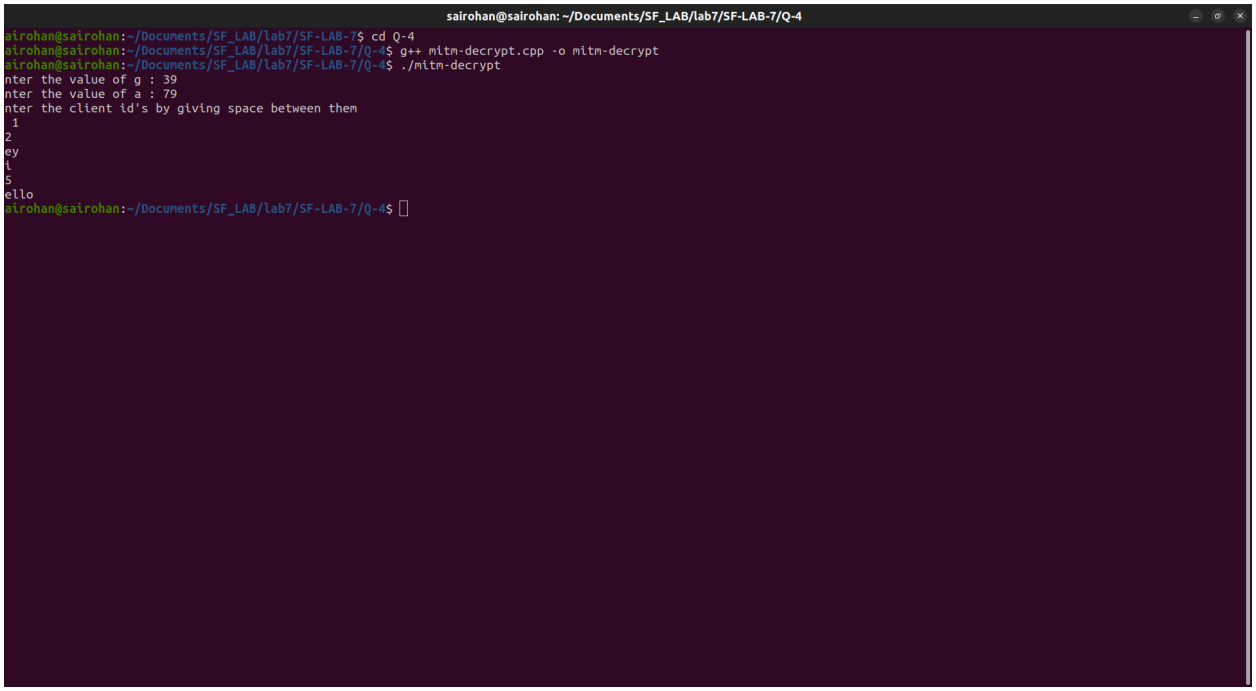




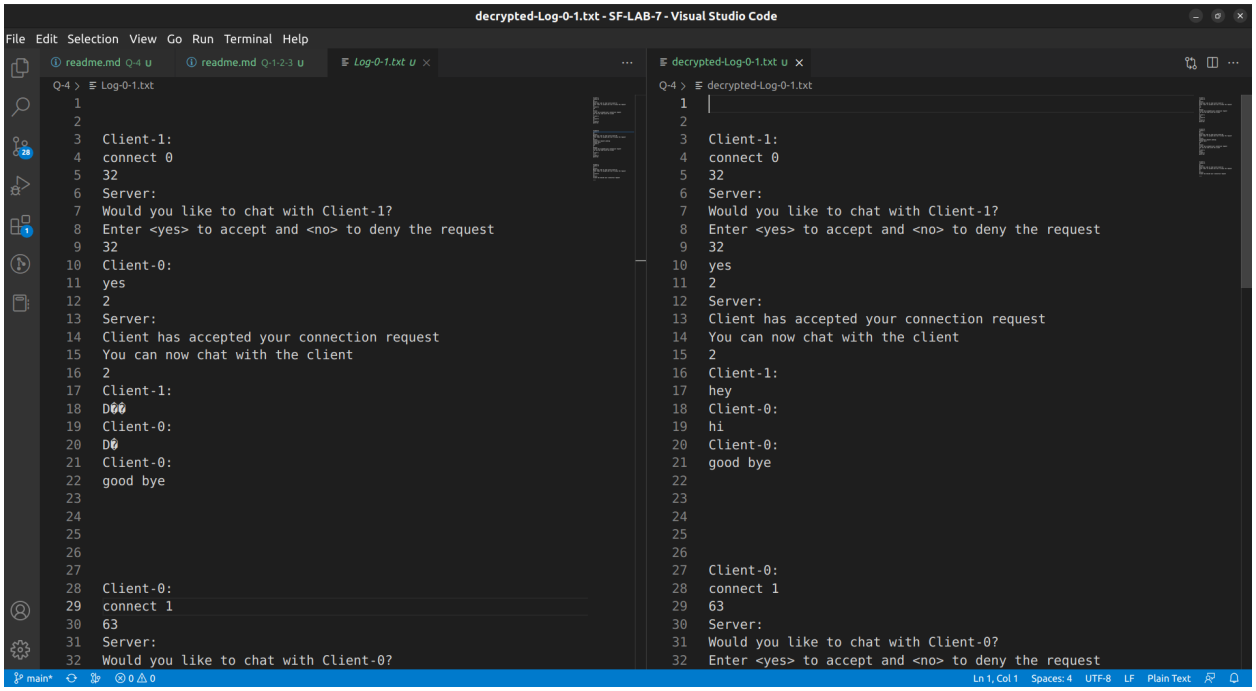

sairohan@sairohan: ~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4
.kSJDFhkj
Server:
Connection request pending
Please wait!
Client:
Server:
Client has accepted your connection request
You can now chat with the client
Client:
Client-1:
hello
Client:
Server:
Chat has ended
Client:
Server:
Would you like to chat with Client-1?
yes
Server:
You can now chat with the client
Client:
hello
good bye
Server:
Chat has ended
Client:
connect 0
Server:
Client has denied your connection request
Client:

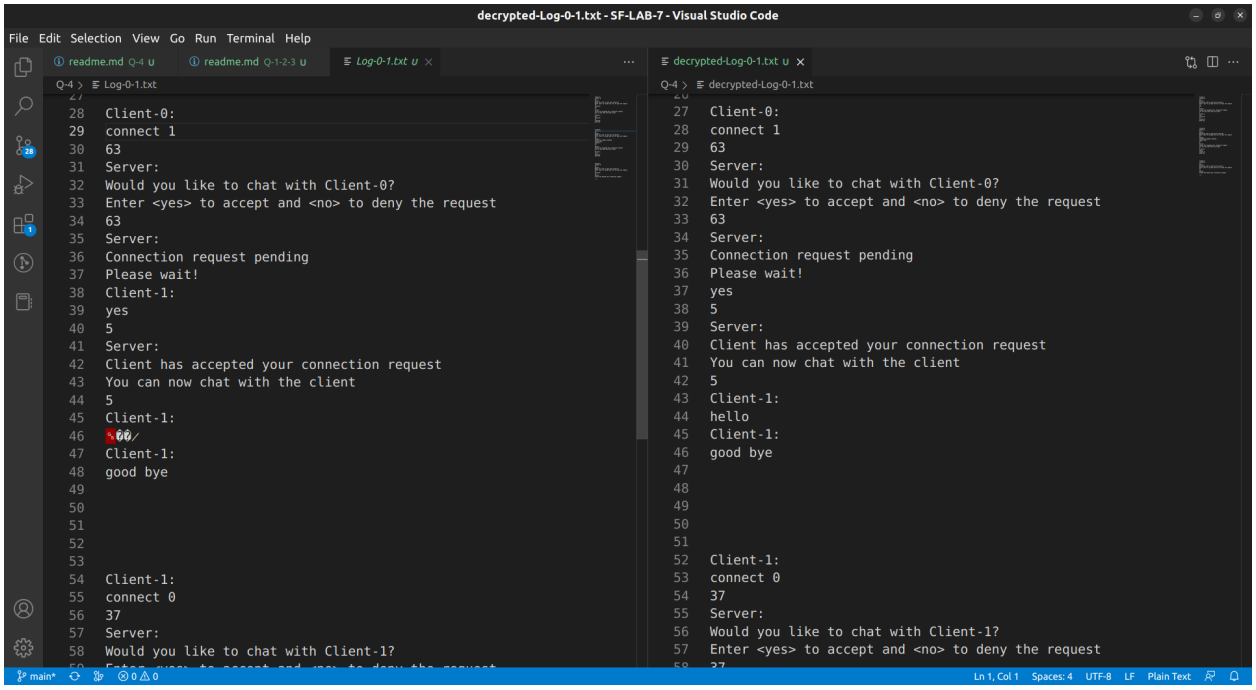

sairohan@sairohan: ~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4
Client:
Server:
Client has accepted your connection request
You can now chat with the client
Client:
Client-1:
hello
Client:
Server:
Chat has ended
Client:
Server:
Would you like to chat with Client-1?
Enter <yes> to accept and <no> to deny the request
Client:
no
yes
Server:
You can now chat with the client
Client:
hello
good bye
Server:
Chat has ended
Client:
connect 0
Server:
Client has denied your connection request
Client:

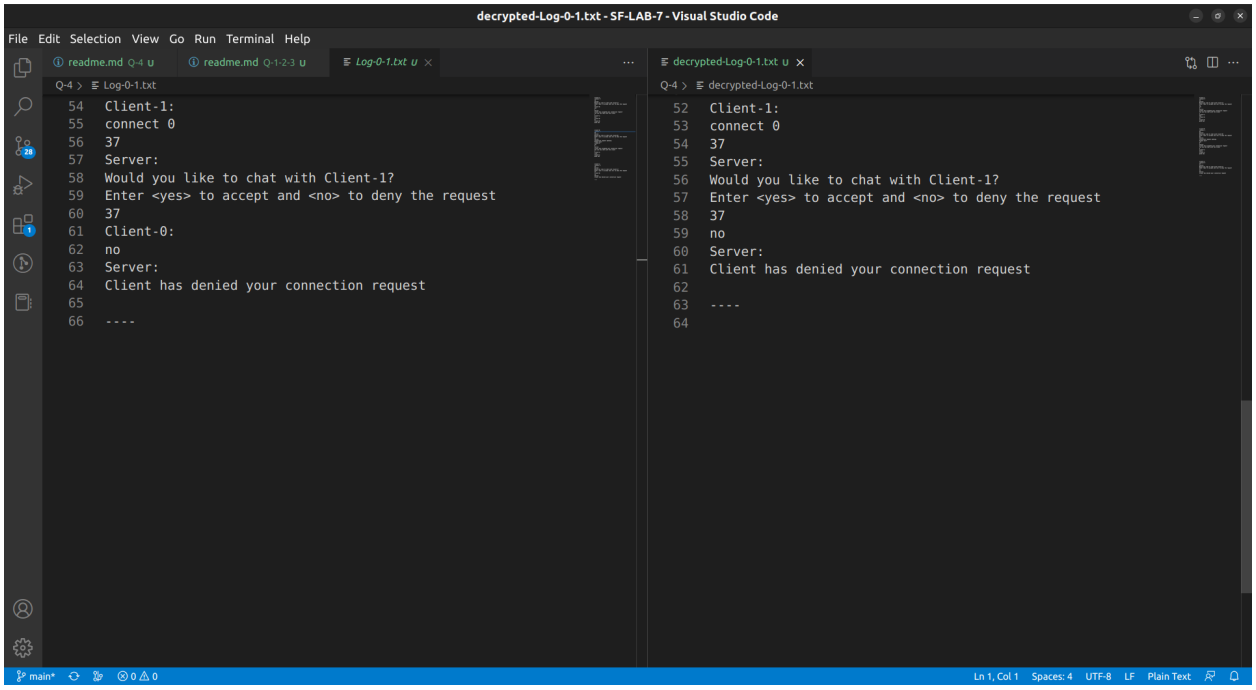
- Decrypting the messages



- Decrypted messages using log file are stored in decrpted-Log file which is generated by MITM.




decrypted-Log-0-1.txt - SF-LAB-7 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
readme.md Q-4 u
readme.md Q-1-2-3 u
Log-0-1.txt u
decrypted-Log-0-1.txt u
Q-4 > Log-0-1.txt
Q-4 > decrypted-Log-0-1.txt
Client-0:
connect 1
63
Server:
Would you like to chat with Client-0?
Enter <yes> to accept and <no> to deny the request
63
Server:
Connection request pending
Please wait!
Client-1:
yes
5
Server:
Client has accepted your connection request
You can now chat with the client
5
Client-1:
hello
Client-1:
good bye
Client-1:
connect 0
37
Server:
Would you like to chat with Client-1?
Enter <yes> to accept and <no> to deny the request
main*
Ln 1, Col 1
Spaces: 4
UTF-8
LF
Plain Text


decrypted-Log-0-1.txt - SF-LAB-7 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
readme.md Q-4 u
readme.md Q-1-2-3 u
Log-0-1.txt u
decrypted-Log-0-1.txt u
Q-4 > Log-0-1.txt
Q-4 > decrypted-Log-0-1.txt
Client-1:
connect 0
37
Server:
Would you like to chat with Client-1?
Enter <yes> to accept and <no> to deny the request
37
Client-0:
no
Server:
Client has denied your connection request
----
main*
Ln 1, Col 1
Spaces: 4
UTF-8
LF
Plain Text