

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.

```
sairohan@sairohan: ~/Documents/SF_LAB/lab7/SF-LAB-7/Q-1-2-3$ g++ server.cpp -o server
-lpthread
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-1-2-3$ ./server
Enter the value of g: 39
Enter the value of a: 79
Server: Waiting for connections...
Server: got connection from 127.0.0.1
Server:
Hello Client
Enter <list> to see the list of other clients connected to server39 79
Server: got connection from 127.0.0.1
Server:
Hello Client
Enter <list> to see the list of other clients connected to server39 79
140444588750400-0 list 4
140444588357696-1 list 4
140444588357696-1 connect 0
32 12
140444588750400-0 yes
2 5

```

```
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-1-2-3$ g++ client.cpp -o client
-lpthread
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-1-2-3$ ./client 127.0.0.1
Client: connecting to 127.0.0.1

Server:
Hello Client
Enter <list> to see the list of other clients connected to server

Client:
list
-----
Server:
Client-0 Status:FREE (YOU)
Client-1 Status:FREE
Enter <connect <client-id>> to connect to the corresponding clients

Client:
Server:
Would you like to chat with Client-1?
Enter <yes> to accept and <no> to deny the request

Client:
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-1-2-3$ ./client 127.0.0.1
Client: connecting to 127.0.0.1

Server:
Hello Client
Enter <list> to see the list of other clients connected to server

Client:
list
-----
Server:
Client-0 Status:FREE
Client-1 Status:FREE (YOU)
Enter <connect <client-id>> to connect to the corresponding clients

Client:
connect 0
-----
Server:
Client has accepted your connection request
You can now chat with the client

Client:

```

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

```

sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-1-2-3$ g++ server.cpp -o server
-lpthread
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-1-2-3$ ./server
Enter the value of g: 39
Enter the value of a: 79
Server: Waiting for connections...
Server: got connection from 127.0.0.1
Server:
Hello Client
Enter <list> to see the list of other clients connected to server39 79
Server: got connection from 127.0.0.1
Server:
Hello Client
Enter <list> to see the list of other clients connected to server39 79
140444588750400-0 list 4
140444580357696-1 list 4
140444580357696-1 connect 0
32 12
140444588750400-0 yes
2 5
b 50444588750400-0 D++ 4
101
140444580357696-1 D++ 4
101
140444588750400-0 N++ 3
101
140444580357696-1 good bye 8
101
FREE
0-309-buf: K++-+++
140444588750400-0 close 5

```

```

Client:
yes
-----
Server:
You can now chat with the clients
Client:
hello
-----
Client-1:
hey
-----
Client:
bye
-----
Server:
***Chat has ended***
Client:
close
-----
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-1-2-3$
Server:
Client has accepted your connection request
You can now chat with the client
Client:
Client-0:
hello
-----
Client:
hey
-----
Client-0:
bye
-----
Client:
good bye
-----
Server:
***Chat has ended***
Client:

```

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 decrypt 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 generated for two clients chatting with each other.

```

saïrohan@saïrohan: ~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4
saïrohan@saïrohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4$ g++ server-mitm.cpp -o server -lthread
saïrohan@saïrohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4$ ./server-mitm
Enter the value of g: 39
Enter the value of a: 79
Server: Waiting for connections....
Server: got connection from 127.0.0.1
Server:
Hello Client
Enter <list> to see the list of other clients connected to server39 79
Server: got connection from 127.0.0.1
Server:
Hello Client
Enter <list> to see the list of other clients connected to server39 79
140312977921600-0 list 4
140312969528896-1 list 4
140312969528896-1 connect 0
32 12
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 yes
2 5
0-97-logFile: Log-0-1.txt
20-97-logFile: Log-0-1.txt
140312969528896-1 D= 3
101
0-97-logFile: Log-0-1.txt
140312977921600-0 D= 2
101
0-97-logFile: Log-0-1.txt
140312977921600-0 good bye 8
101
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
FREE
0-309-buf: K==***
140312977921600-0 connect 1
63 12
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 .KSJDFhkj 9
0-97-logFile: Log-0-1.txt
140312969528896-1 yes
5 5
0-97-logFile: Log-0-1.txt
50-97-logFile: Log-0-1.txt

saïrohan@saïrohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4$ g++ client.cpp -o client -lpt
saïrohan@saïrohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4$ ./client 127.0.0.1
Client: connecting to 127.0.0.1
Server:
Hello Client
Enter <list> to see the list of other clients connected to server
Client:
list
-----
Server:
Client-0 Status:FREE (YOU)
Client-1 Status:FREE
Enter <connect <client-id>> to connect to the corresponding client
Client:
Server:
Would you like to chat with Client-1?
Enter <yes> to accept and <no> to deny the request
Client:
saïrohan@saïrohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4$ ./client 127.0.0.1
Client: connecting to 127.0.0.1
Server:
Hello Client
Enter <list> to see the list of other clients connected to server
Client:
list
-----
Server:
Client-0 Status:FREE
Client-1 Status:FREE (YOU)
Enter <connect <client-id>> to connect to the corresponding client
Client:
connect 0
-----
Server:
Client has accepted your connection request
You can now chat with the client
Client:

```

```

saïrohan@saïrohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 yes
2 5
0-97-logFile: Log-0-1.txt
20-97-logFile: Log-0-1.txt
140312969528896-1 D= 3
101
0-97-logFile: Log-0-1.txt
140312977921600-0 D= 2
101
0-97-logFile: Log-0-1.txt
140312977921600-0 good bye 8
101
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
FREE
0-309-buf: K==***
140312977921600-0 connect 1
63 12
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 .KSJDFhkj 9
0-97-logFile: Log-0-1.txt
140312969528896-1 yes
5 5
0-97-logFile: Log-0-1.txt
20-97-logFile: Log-0-1.txt
140312969528896-1 D= 5
101
0-97-logFile: Log-0-1.txt
140312969528896-1 good bye 8
101
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
FREE
0-309-buf: *****G
140312969528896-1 connect 0
67 12
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 no 2
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt

Client:
yes
-----
Server:
You can now chat with the client
Client:
Client-1:
hey
-----
Client:
hi
-----
good bye
-----
Server:
***Chat has ended***
Client:
connect 1
-----
Client:
hey
-----
Client-0:
hi
-----
Client:
Server:
***Chat has ended***
Client:
Server:
Would you like to chat with Client-0?
Enter <yes> to accept and <no> to deny the request
Client:
yes
-----
Server:
You can now chat with the client
Client:

```

```
sairohan@sairohan: ~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4

0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 yes
2 5
0-97-logFile: Log-0-1.txt
20-97-logFile: Log-0-1.txt
140312969528896-1 De 3
101
0-97-logFile: Log-0-1.txt
140312977921600-0 De 2
101
0-97-logFile: Log-0-1.txt
140312977921600-0 good bye 8
101
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
*FREE
0-309-buf: K*****
140312977921600-0 connect 1
63 12
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 .KSJDFhkj 9
0-97-logFile: Log-0-1.txt
140312969528896-1 yes
5 5
0-97-logFile: Log-0-1.txt
50-97-logFile: Log-0-1.txt
140312969528896-1 5
101
0-97-logFile: Log-0-1.txt
140312969528896-1 good bye 8
101
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
*FREE
0-309-buf: *****G
140312969528896-1 connect 0
37 12
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 no 2
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
]

.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?
Enter <yes> to accept and <no> to deny the request
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

0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 yes
2 5
0-97-logFile: Log-0-1.txt
20-97-logFile: Log-0-1.txt
140312969528896-1 De 3
101
0-97-logFile: Log-0-1.txt
140312977921600-0 De 2
101
0-97-logFile: Log-0-1.txt
140312977921600-0 good bye 8
101
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
*FREE
0-309-buf: K*****
140312977921600-0 connect 1
63 12
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 .KSJDFhkj 9
0-97-logFile: Log-0-1.txt
140312969528896-1 yes
5 5
0-97-logFile: Log-0-1.txt
50-97-logFile: Log-0-1.txt
140312969528896-1 5
101
0-97-logFile: Log-0-1.txt
140312969528896-1 good bye 8
101
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
*FREE
0-309-buf: *****G
140312969528896-1 connect 0
37 12
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
140312977921600-0 no 2
0-97-logFile: Log-0-1.txt
0-97-logFile: Log-0-1.txt
]

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

```
sairohan@sairohan: ~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7$ cd Q-4
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4$ g++ mitm-decrypt.cpp -o mitm-decrypt
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4$ ./mitm-decrypt
Enter the value of g : 39
Enter the value of a : 79
Enter the client id's by giving space between them
1
2
hey
1
5
ello
sairohan@sairohan:~/Documents/SF_LAB/lab7/SF-LAB-7/Q-4$
```

- Decrypted messages using log file are stored in decrypted-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
Q-4 > Log-0-1.txt
1
2
3 Client-1:
4 connect 0
5 32
6 Server:
7 Would you like to chat with Client-1?
8 Enter <yes> to accept and <no> to deny the request
9 32
10 Client-0:
11 yes
12 2
13 Server:
14 Client has accepted your connection request
15 You can now chat with the client
16 2
17 Client-1:
18 D00
19 Client-0:
20 D0
21 Client-0:
22 good bye
23
24
25
26
27
28 Client-0:
29 connect 1
30 63
31 Server:
32 Would you like to chat with Client-0?
decrypted-Log-0-1.txt u x
Q-4 > decrypted-Log-0-1.txt
1
2
3 Client-1:
4 connect 0
5 32
6 Server:
7 Would you like to chat with Client-1?
8 Enter <yes> to accept and <no> to deny the request
9 32
10 yes
11 2
12 Server:
13 Client has accepted your connection request
14 You can now chat with the client
15 2
16 Client-1:
17 hey
18 Client-0:
19 hi
20 Client-0:
21 good bye
22
23
24
25
26
27 Client-0:
28 connect 1
29 63
30 Server:
31 Would you like to chat with Client-0?
32 Enter <yes> to accept and <no> to deny the request
Ln 1, Col 1 Spaces: 4 UTF-8 LF Plain Text
```

```
Q-4 > Log-0-1.txt
28 Client-0:
29 connect 1
30 63
31 Server:
32 Would you like to chat with Client-0?
33 Enter <yes> to accept and <no> to deny the request
34 63
35 Server:
36 Connection request pending
37 Please wait!
38 Client-1:
39 yes
40 5
41 Server:
42 Client has accepted your connection request
43 You can now chat with the client
44 5
45 Client-1:
46 66/
47 Client-1:
48 good bye
49
50
51
52
53
54 Client-1:
55 connect 0
56 37
57 Server:
58 Would you like to chat with Client-1?
59 Enter <yes> to accept and <no> to deny the request

Q-4 > decrypted-Log-0-1.txt
27 Client-0:
28 connect 1
29 63
30 Server:
31 Would you like to chat with Client-0?
32 Enter <yes> to accept and <no> to deny the request
33 63
34 Server:
35 Connection request pending
36 Please wait!
37 yes
38 5
39 Server:
40 Client has accepted your connection request
41 You can now chat with the client
42 5
43 Client-1:
44 hello
45 Client-1:
46 good bye
47
48
49
50
51
52 Client-1:
53 connect 0
54 37
55 Server:
56 Would you like to chat with Client-1?
57 Enter <yes> to accept and <no> to deny the request
58 37
```

```
Q-4 > Log-0-1.txt
54 Client-1:
55 connect 0
56 37
57 Server:
58 Would you like to chat with Client-1?
59 Enter <yes> to accept and <no> to deny the request
60 37
61 Client-0:
62 no
63 Server:
64 Client has denied your connection request
65
66 ----

Q-4 > decrypted-Log-0-1.txt
52 Client-1:
53 connect 0
54 37
55 Server:
56 Would you like to chat with Client-1?
57 Enter <yes> to accept and <no> to deny the request
58 37
59 no
60 Server:
61 Client has denied your connection request
62
63 ----
64
```