

## Lab-4(1RVU23CSE431)

### Exp – 1 => Symmetric Key Ciphers

```
shiva143@Shiva: /mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Symmetric Key Ciphers
File
    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:e9:76:46 brd ff:ff:ff:ff:ff:ff
    inet 172.26.112.9/20 brd 172.26.127.255 scope global eth0
    valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fee9:7646/64 scope link
    valid_lft forever preferred_lft forever
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Symmetric Key Ciphers$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:e9:76:46 brd ff:ff:ff:ff:ff:ff
    inet 172.26.112.9/20 brd 172.26.127.255 scope global eth0
    valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fee9:7646/64 scope link
    valid_lft forever preferred_lft forever
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Symmetric Key Ciphers$ ./server
Symmetric server listening on port 65431...
Decrypted message from client: Hello from symmetric client
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Symmetric Key Ciphers$ ./server
Symmetric server listening on port 65431...
Decrypted message from client: Hello from symmetric client
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Symmetric Key Ciphers$ ./server
Symmetric server listening on port 65431...
Decrypted message from client: Hello from symmetric client
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Symmetric Key Ciphers$
Received from server: Hello from symmetric server
```

```
Command Prompt
C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Symmetric Key Ciphers>list
'list' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Symmetric Key Ciphers>ip addr show eth0
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Symmetric Key Ciphers>python client.py
Received from server: Hello from symmetric server

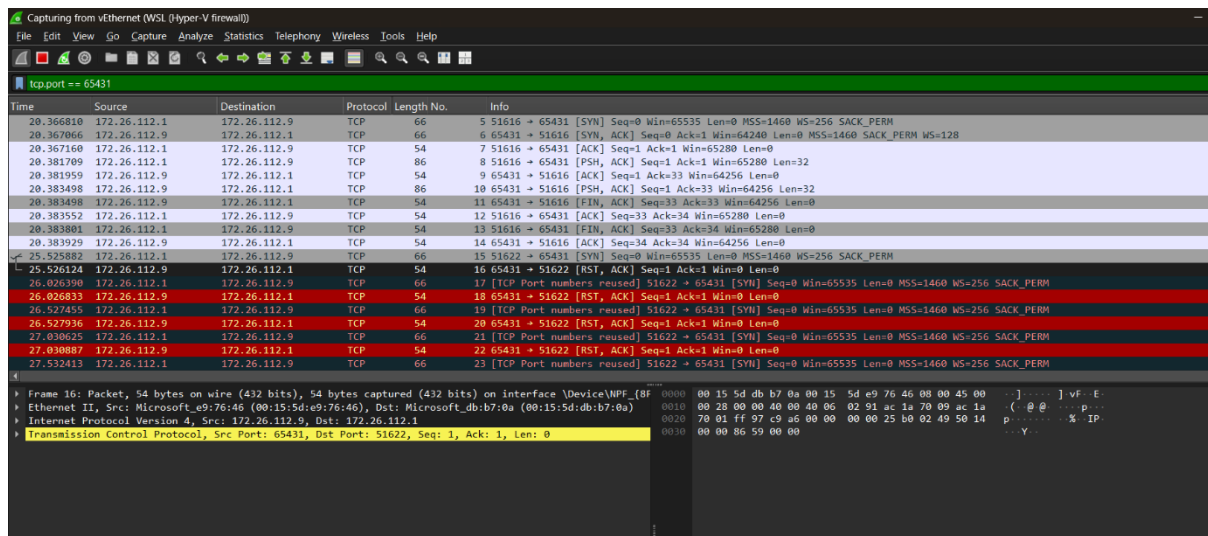
C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Symmetric Key Ciphers>python client.py
Received from server: Hello from symmetric server

C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Symmetric Key Ciphers>python client.py
Traceback (most recent call last):
  File "C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Symmetric Key Ciphers\client.py", line 37, in <module>
    s.connect((HOST, PORT))
    ~~~~~~^~~~~~
ConnectionRefusedError: [WinError 10061] No connection could be made because the target machine actively refused it

C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Symmetric Key Ciphers>python client.py
Received from server: Hello from symmetric server

C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Symmetric Key Ciphers>
```

# -wireshark



## Exp-2 => Asymmetric Key Ciphers

```
shiva143@Shiva: /mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Asymmetric Key Ciphers
.....*.....
at .....*.....
cha.....*.....
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Asymmetric Key Ciphers$ openssl rsa -pubou
t -in private.pem -out public.pem
writing RSA key
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Asymmetric Key Ciphers$ ls
client.py private.pem public.pem server.c
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Asymmetric Key Ciphers$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:e9:76:46 brd ff:ff:ff:ff:ff:ff
    inet 172.26.112.9/20 brd 172.26.127.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fee9:7646/64 scope link
        valid_lft forever preferred_lft forever
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Asymmetric Key Ciphers$ gcc server.c -o as
ym_server -lssl -lcrypto -Wno-deprecated-declarations
shiva143@Shiva:/mnt/c/Users/shiva/College Work/Labs-Network Security/Lab4/src/Asymmetric Key Ciphers$ ./asym_server
Asymmetric server listening on port 65432...
Decrypted message from client: Hello from asymmetric client
```

```
Command Prompt
Microsoft Windows [Version 10.0.26200.7705]
(c) Microsoft Corporation. All rights reserved.

C:\Users\shiva>cd "C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Asymmetric Key Ciphers"

C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Asymmetric Key Ciphers>python client.py
Received encrypted data from server: 9a169f31988147f860569798f0aa12efffed873e1739378b0f9e69345f9170d3ef309a130c2f6bb99
354d7be5c355265071d7527af6c5e125d95af92aac47d84ace1a3168e5b2034b9fd18012f0e7c5610634098cf57b0a918c9c24dd06ef764e34454adc
05ef06a07b15c606364953529d84f57ef927e4a75d7ecd181f9efdbacf55d2dbe1f827a489894fcdacd9752fd043b16fabcd2a4a342afe556f62d14e
139e3a0f5037fce4b74a0e055c6bd0e971bd8faec62c509f54be27d544512f4765db4a646cdfab04e0c0abc24b7b6f69489f50388706dc7196b5a29
8f6ef7c1a5d37c1b62e9f3bca7408c57b71cd899549c73068c8f569145e1fc4a5afc

C:\Users\shiva\College Work\Labs-Network Security\Lab4\src\Asymmetric Key Ciphers>
```

## -wireshark

Capturing from vEthernet (WSL (Hyper-V firewall))

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 65432

Time	Source	Destination	Protocol	Length	No.	Info
284.785218	172.26.112.1	172.26.112.9	TCP	66	85	50311 → 65432 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
284.785534	172.26.112.9	172.26.112.1	TCP	66	86	65432 → 50311 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
284.785633	172.26.112.1	172.26.112.9	TCP	54	87	50311 → 65432 [ACK] Seq=1 Ack=1 Win=65280 Len=0
284.785686	172.26.112.1	172.26.112.9	TCP	310	88	50311 → 65432 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=256
284.785912	172.26.112.9	172.26.112.1	TCP	54	89	65432 → 50311 [ACK] Seq=1 Ack=257 Win=64128 Len=0
284.794156	172.26.112.9	172.26.112.1	TCP	310	90	65432 → 50311 [PSH, ACK] Seq=1 Ack=257 Win=64128 Len=256
284.794156	172.26.112.9	172.26.112.1	TCP	54	91	65432 → 50311 [FIN, ACK] Seq=257 Ack=257 Win=64128 Len=0
284.794247	172.26.112.1	172.26.112.9	TCP	54	92	50311 → 65432 [ACK] Seq=257 Ack=258 Win=65024 Len=0
284.794459	172.26.112.1	172.26.112.9	TCP	54	93	50311 → 65432 [FIN, ACK] Seq=257 Ack=258 Win=65024 Len=0
284.794611	172.26.112.9	172.26.112.1	TCP	54	94	65432 → 50311 [ACK] Seq=258 Ack=258 Win=64128 Len=0

Frame 91: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{8F0010-0020-70 01 ff 98 c4 87 c1 03 22 a8 d6 a5 33 92 50 11} p 0

Ethernet II, Src: Microsoft\_e9:76:46 (00:15:5d:e9:76:46), Dst: Microsoft\_db:b7:0a (00:15:5d:db:b7:0a)

Internet Protocol Version 4, Src: 172.26.112.9, Dst: 172.26.112.1

Transmission Control Protocol, Src Port: 65432, Dst Port: 50311, Seq: 257, Len: 0

0000 00 15 5d db b7 0a 00 15 5d e9 76 46 08 00 45 00 ...] ...] VF: E-

0010 00 23 03 33 40 00 40 06 29 5d ac 1a 70 09 ac 1a (-30 @ )] p -

0020 70 01 ff 98 c4 87 c1 03 22 a8 d6 a5 33 92 50 11 p ... s p

0030 01 f5 c3 9a 00 00