San Jose State University

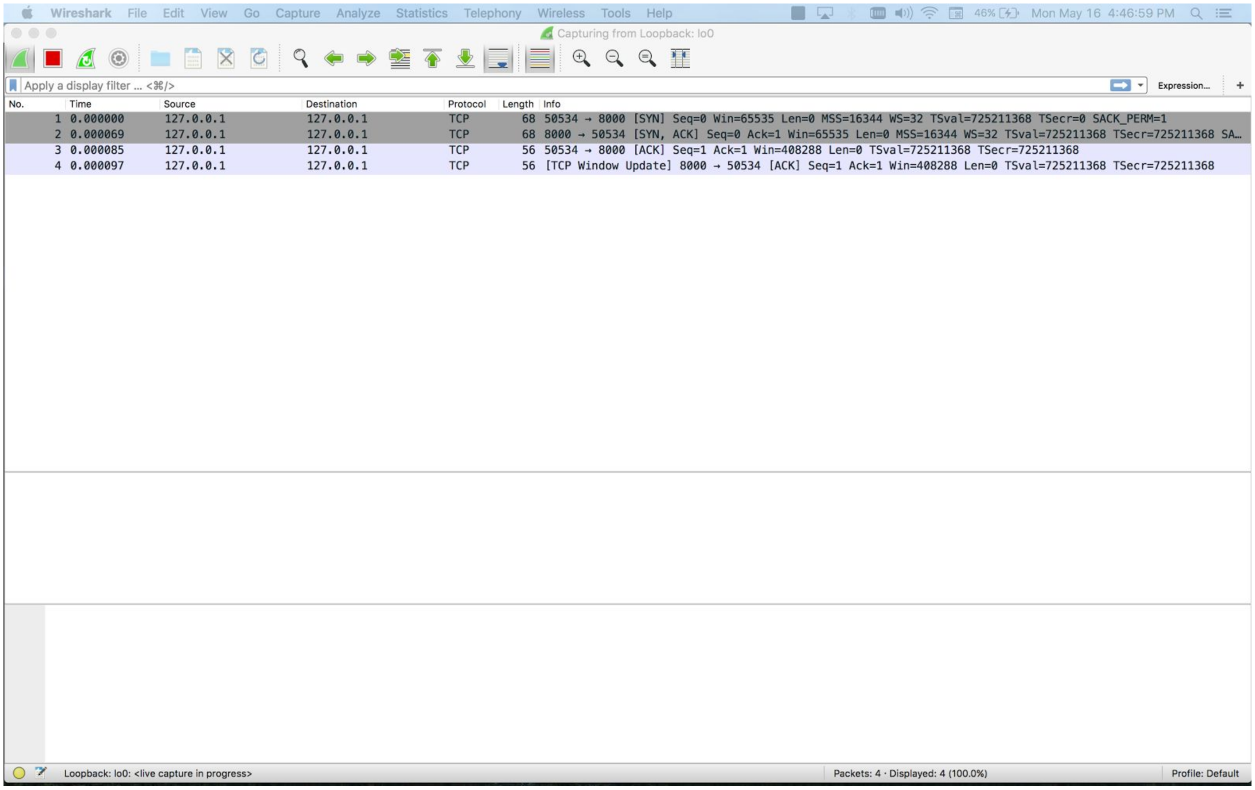
ELECTRICAL ENGINEERING DEPARTMENT

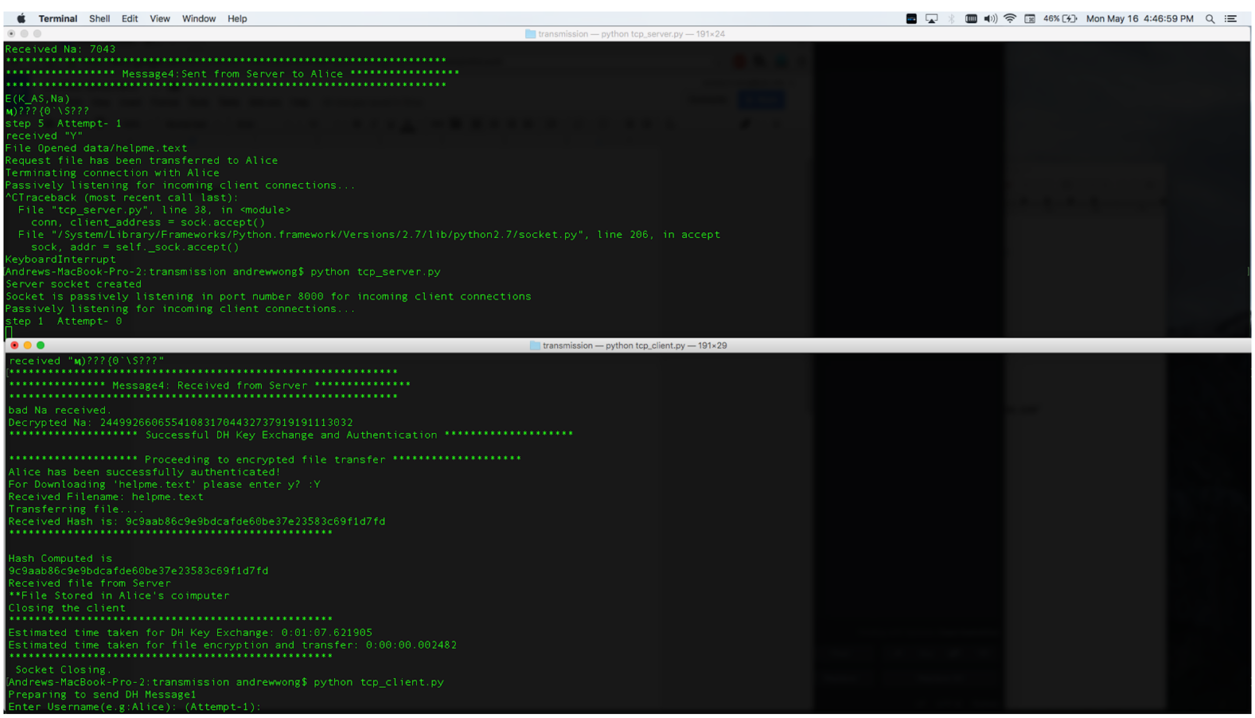
EE 282/CMPE209

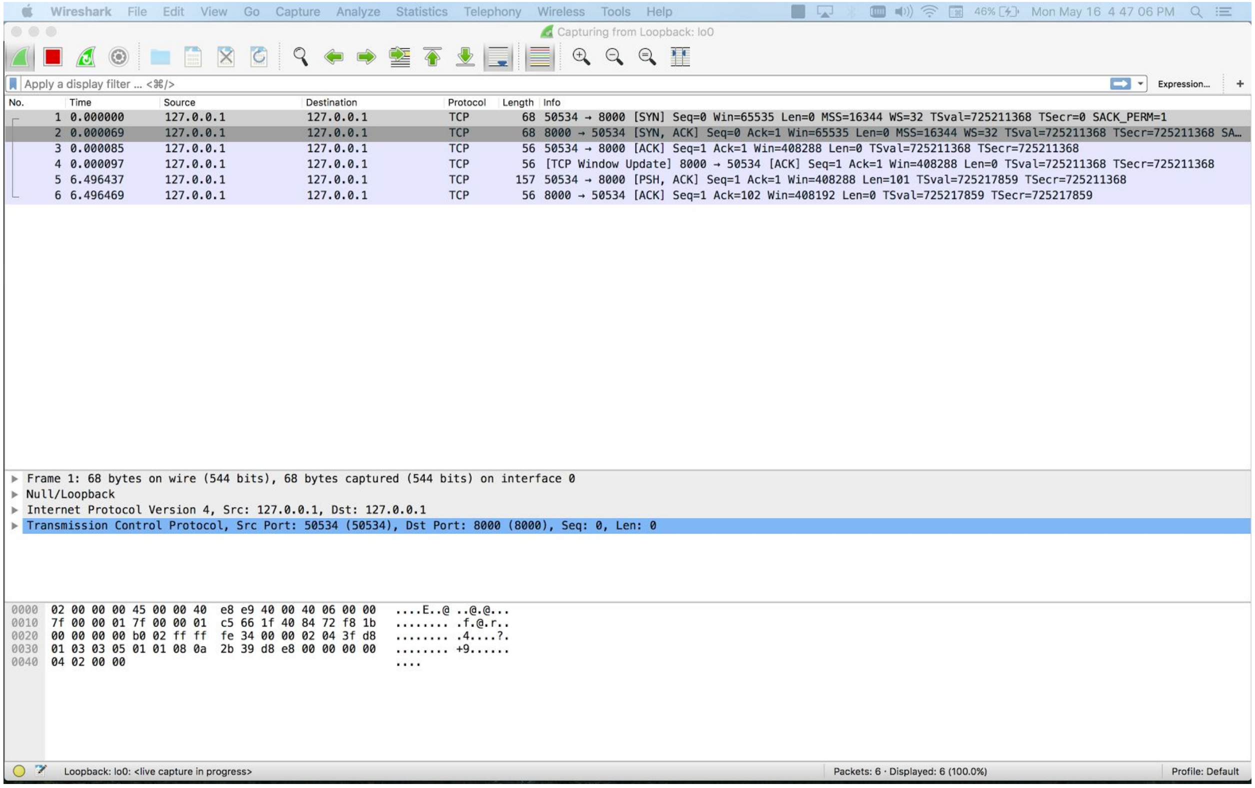
SECURE CLIENT-SERVER FILE TRANSFER PART – 2

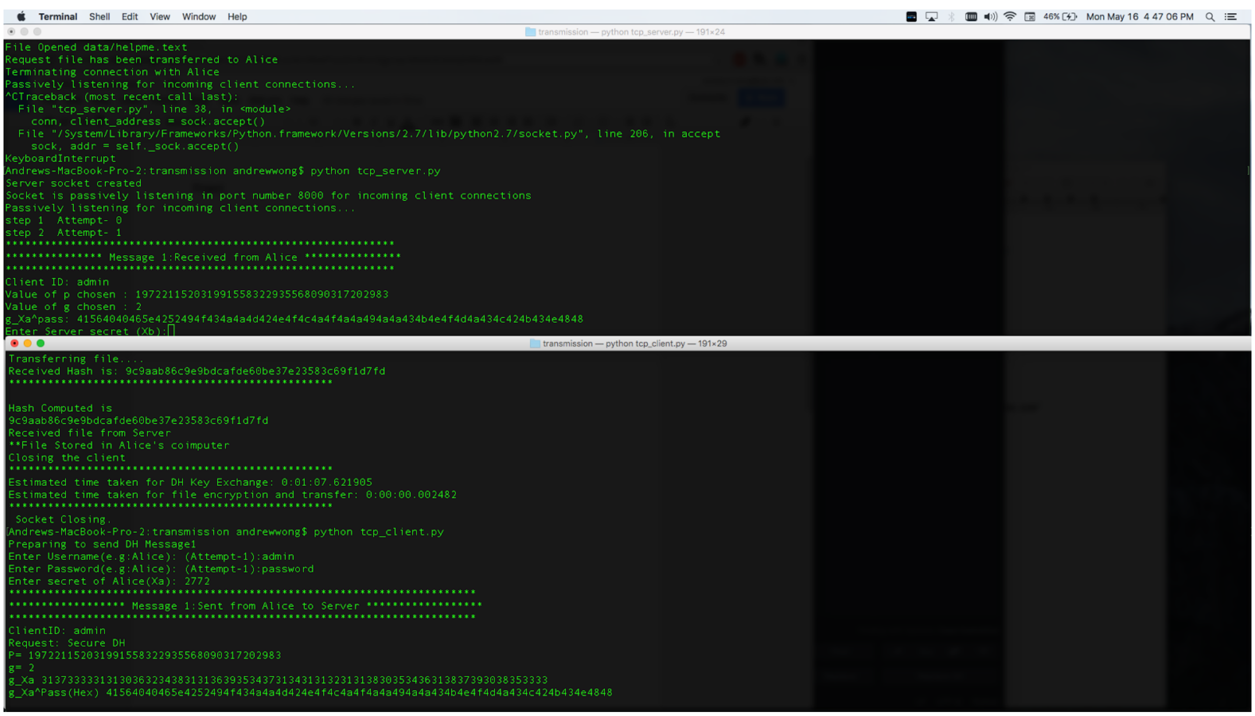
Andrew Wong 010782772
Venkat Babu Manchikalapudi 010747698

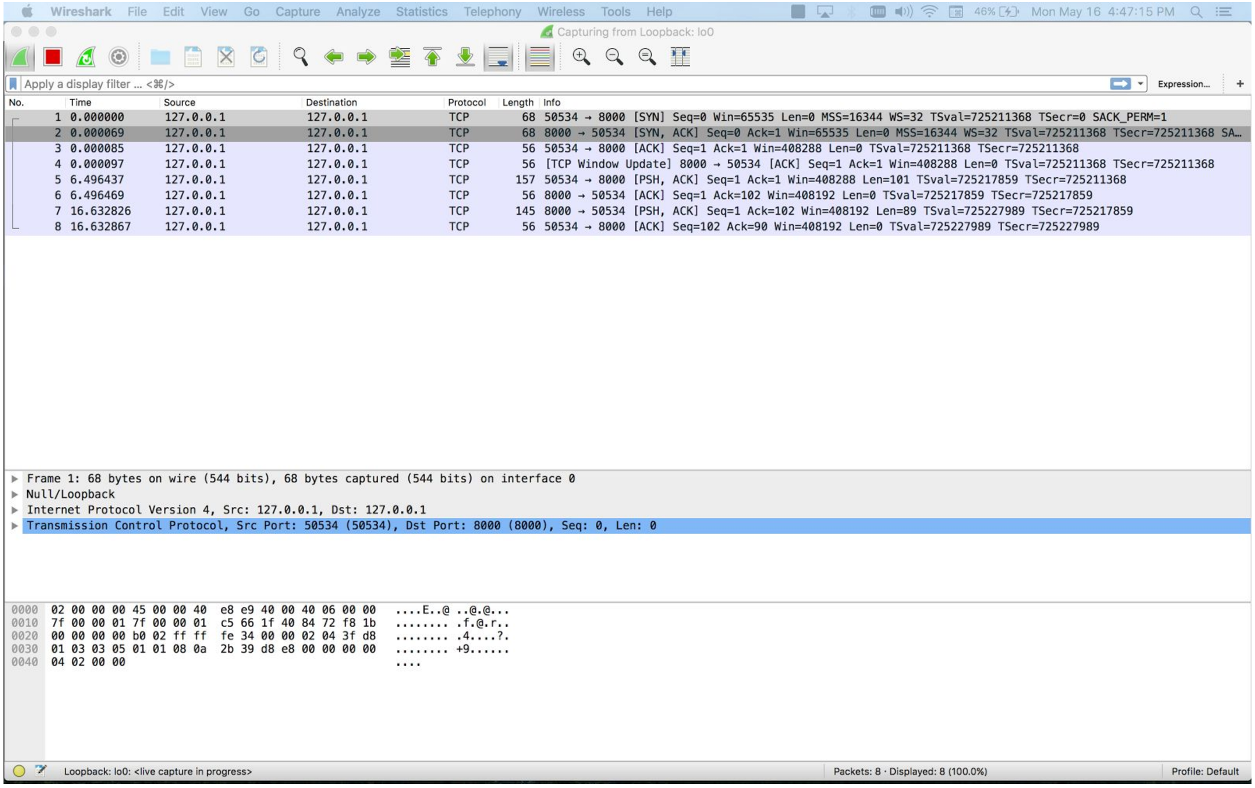
1. *Wireshark Traces of messages exchanged between the client during the a successful session.* ***[Upper Screen is wireshare communication, upper of Lower screen is Server and lower of Lower screen is Client]***

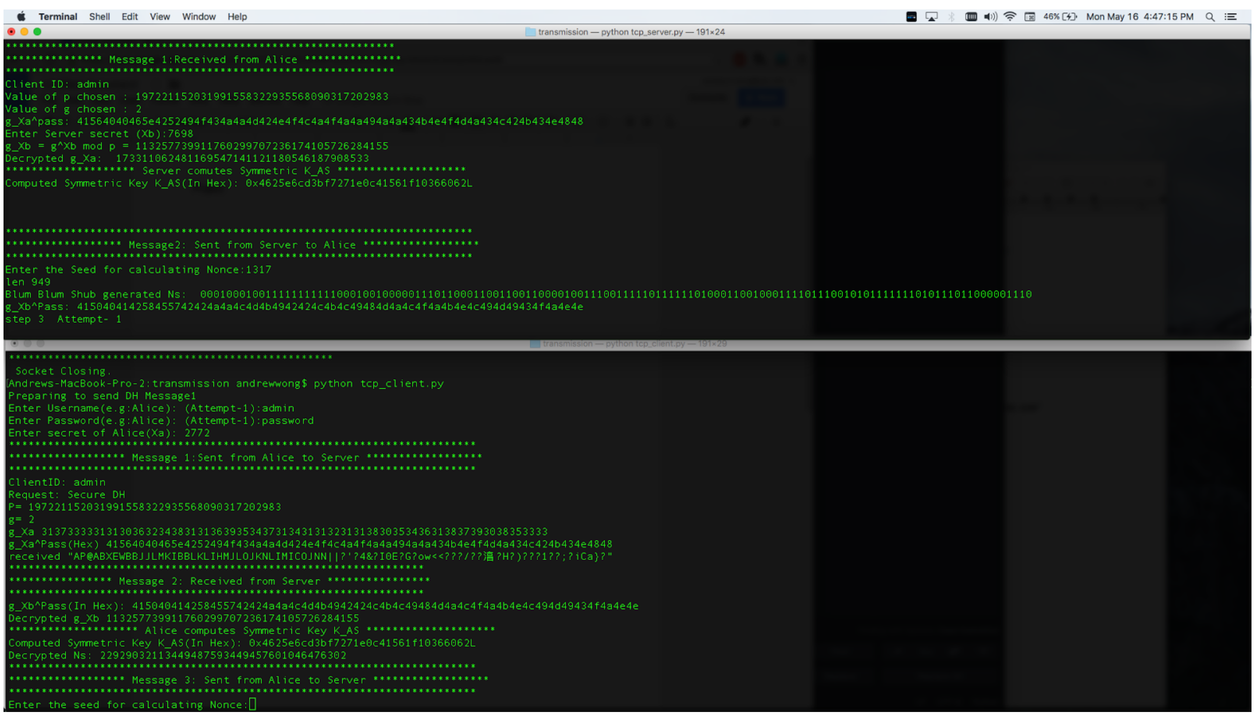


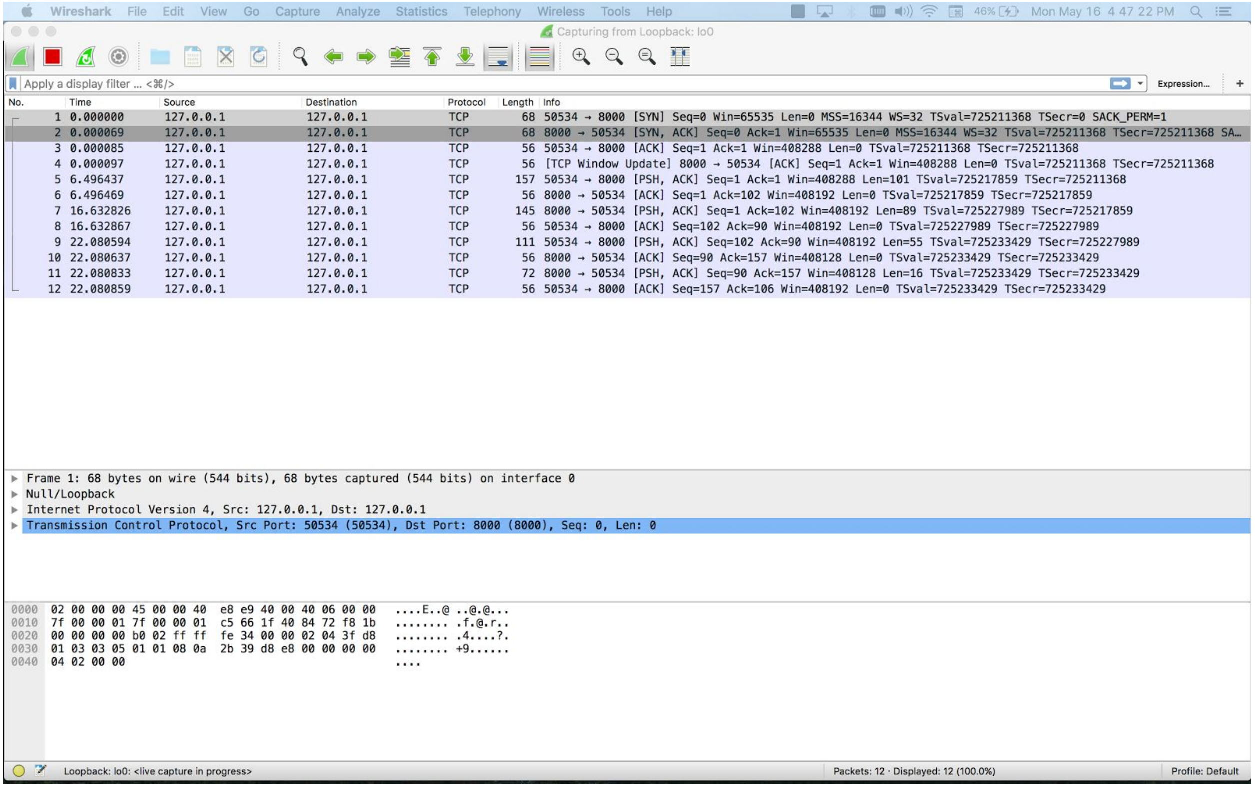



Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mon May 16 4 47 06 PM
Capturing from Loopback: lo0
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 127.0.0.1 127.0.0.1 TCP 68 50534 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=32 TSval=725211368 TSecr=0 SACK_PERM=1
2 0.000069 127.0.0.1 127.0.0.1 TCP 68 8000 → 50534 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=32 TSval=725211368 TSecr=725211368 SA…
3 0.000085 127.0.0.1 127.0.0.1 TCP 56 50534 → 8000 [ACK] Seq=1 Ack=1 Win=408288 Len=0 TSval=725211368 TSecr=725211368
4 0.000097 127.0.0.1 127.0.0.1 TCP 56 [TCP Window Update] 8000 → 50534 [ACK] Seq=1 Ack=1 Win=408288 Len=0 TSval=725211368 TSecr=725211368
5 6.496437 127.0.0.1 127.0.0.1 TCP 157 50534 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=408288 Len=101 TSval=725217859 TSecr=725211368
6 6.496469 127.0.0.1 127.0.0.1 TCP 56 8000 → 50534 [ACK] Seq=1 Ack=102 Win=408192 Len=0 TSval=725217859 TSecr=725217859
Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 50534 (50534), Dst Port: 8000 (8000), Seq: 0, Len: 0
0000 02 00 00 00 45 00 00 40 e8 e9 40 00 40 06 00 00 ....E..@ ..@.@...
0010 7f 00 00 01 7f 00 00 01 c5 66 1f 40 84 72 f8 1b .... .f.@.r..
0020 00 00 00 00 b0 02 ff ff fe 34 00 00 02 04 3f d8 .... .4....?.
0030 01 03 03 05 01 01 08 0a 2b 39 d8 e8 00 00 00 00 .... +9......
0040 04 02 00 00 ....
Loopback: lo0: <live capture in progress>
Packets: 6 · Displayed: 6 (100.0%)
Profile: Default

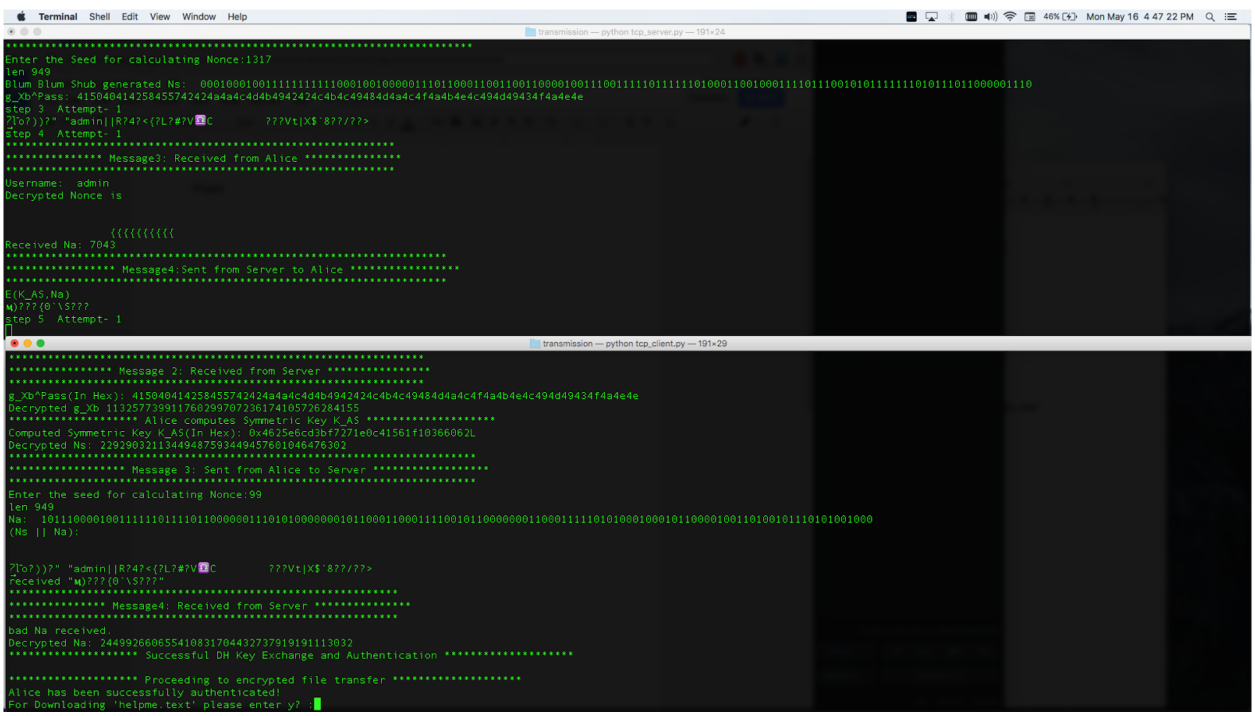

Terminal Shell Edit View Window Help
Mon May 16 4 47 06 PM
transmission — python tcp_server.py — 191×24
File Opened data/helpme.text
Request file has been transferred to Alice
Terminating connection with Alice
Passively listening for incoming client connections...
^CTraceback (most recent call last):
File "tcp_server.py", line 38, in <module>
conn, client_address = sock.accept()
File "/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/socket.py", line 206, in accept
sock, addr = self._sock.accept()
KeyboardInterrupt
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_server.py
Server socket created
Socket is passively listening in port number 8000 for incoming client connections
Passively listening for incoming client connections...
step 1 Attempt- 0
step 2 Attempt- 1
*************** Message 1:Received from Alice ***************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 41564040465e4252494f434a4a4d424e4f4c4a4f4a4a494a4a434b4e4f4d4a434c424b434e4848
Enter Server secret (Xb):
transmission — python tcp_client.py — 191×29
Transferring file....
Received Hash is: 9c9aab86c9e9bdcafde60be37e23583c69f1d7fd
Hash Computed is
9c9aab86c9e9bdcafde60be37e23583c69f1d7fd
Received file from Server
**File Stored in Alice's coimputer
Closing the client
Estimated time taken for DH Key Exchange: 0:01:07.621905
Estimated time taken for file encryption and transfer: 0:00:00.002482
Socket Closing.
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_client.py
Preparing to send DH Message1
Enter Username(e.g:Alice): (Attempt-1):admin
Enter Password(e.g:Alice): (Attempt-1):password
Enter secret of Alice(Xa): 2772
****************** Message 1:Sent from Alice to Server ******************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 313733333131303632343831313639353437313431313231313830353436313837393038353333
g_Xa^Pass(Hex) 41564040465e4252494f434a4a4d424e4f4c4a4f4a4a494a4a434b4e4f4d4a434c424b434e4848


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
46% Mon May 16 4:47:15 PM
Capturing from Loopback: lo0
Apply a display filter ... <⌘/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 127.0.0.1 127.0.0.1 TCP 68 50534 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=32 TSval=725211368 TSecr=0 SACK_PERM=1
2 0.000069 127.0.0.1 127.0.0.1 TCP 68 8000 → 50534 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=32 TSval=725211368 TSecr=725211368 SA…
3 0.000085 127.0.0.1 127.0.0.1 TCP 56 50534 → 8000 [ACK] Seq=1 Ack=1 Win=408288 Len=0 TSval=725211368 TSecr=725211368
4 0.000097 127.0.0.1 127.0.0.1 TCP 56 [TCP Window Update] 8000 → 50534 [ACK] Seq=1 Ack=1 Win=408288 Len=0 TSval=725211368 TSecr=725211368
5 6.496437 127.0.0.1 127.0.0.1 TCP 157 50534 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=408288 Len=101 TSval=725217859 TSecr=725211368
6 6.496469 127.0.0.1 127.0.0.1 TCP 56 8000 → 50534 [ACK] Seq=1 Ack=102 Win=408192 Len=0 TSval=725217859 TSecr=725217859
7 16.632826 127.0.0.1 127.0.0.1 TCP 145 8000 → 50534 [PSH, ACK] Seq=1 Ack=102 Win=408192 Len=89 TSval=725227989 TSecr=725217859
8 16.632867 127.0.0.1 127.0.0.1 TCP 56 50534 → 8000 [ACK] Seq=102 Ack=90 Win=408192 Len=0 TSval=725227989 TSecr=725227989
Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 50534 (50534), Dst Port: 8000 (8000), Seq: 0, Len: 0
0000 02 00 00 00 45 00 00 40 e8 e9 40 00 40 06 00 00 ....E..@ ..@.@...
0010 7f 00 00 01 7f 00 00 01 c5 66 1f 40 84 72 f8 1b .... .f.@.r..
0020 00 00 00 00 b0 02 ff ff fe 34 00 00 02 04 3f d8 .... .4....?.
0030 01 03 03 05 01 01 08 0a 2b 39 d8 e8 00 00 00 00 .... +9......
0040 04 02 00 00 ....
Loopback: lo0: <live capture in progress>
Packets: 8 · Displayed: 8 (100.0%)
Profile: Default

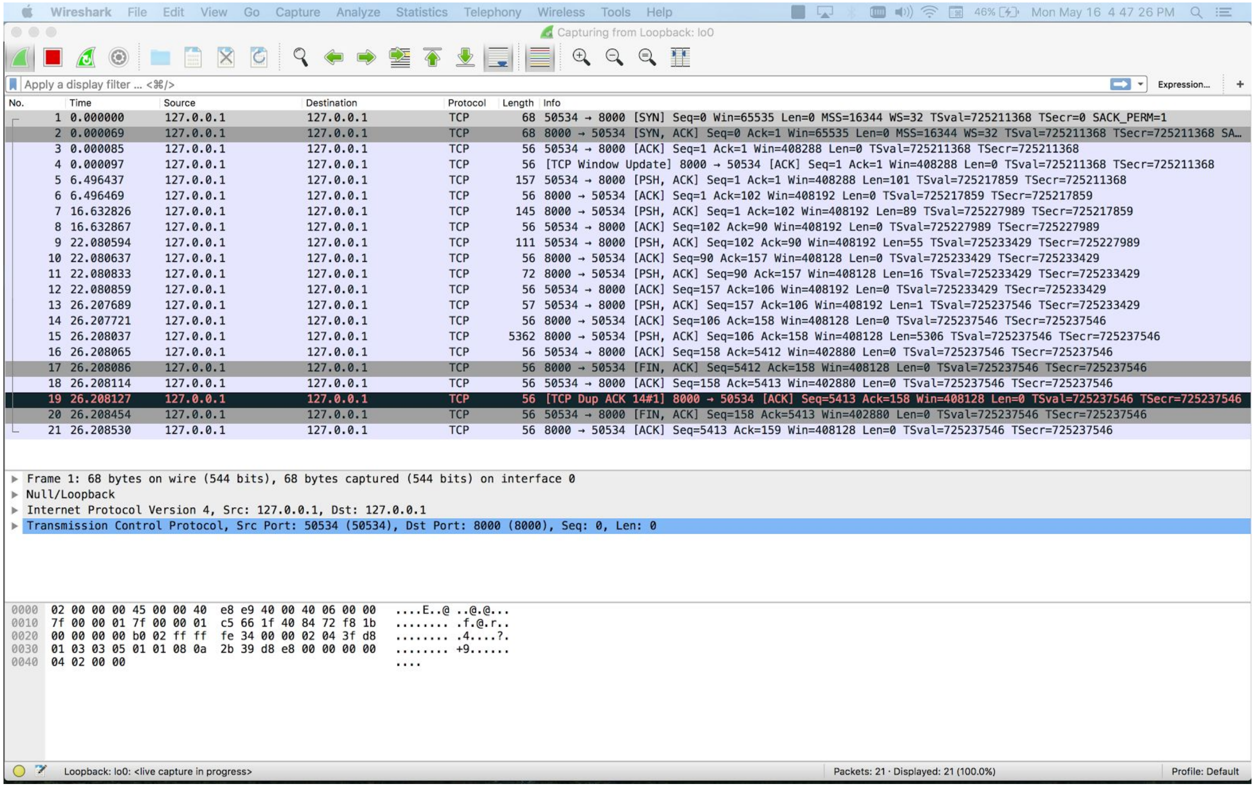

Terminal Shell Edit View Window Help
46% Mon May 16 4:47:15 PM
transmission — python tcp_server.py — 191×24
*************** Message 1:Received from Alice ***************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 41564040465e4252494f434a4a4d424e4f4c4a4f4a4a494a4a434b4e4f4d4a434c424b434e4848
Enter Server secret (Xb):7698
g_Xb = g^Xb mod p = 113257739911760299707236174105726284155
Decrypted g_Xa: 173311062481169547141121180546187908533
******************** Server comutes Symmetric K_AS ********************
Computed Symmetric Key K_AS(In Hex): 0x4625e6cd3bf7271e0c41561f10366062L
****************** Message2: Sent from Server to Alice ******************
Enter the Seed for calculating Nonce:1317
len 949
Blum Blum Shub generated Ns: 0001000100111111111110001001000001110110001100110011000010011100111110111111010001100100011110111001010111111101011101100001110
g_Xb^Pass: 415040414258455742424a4a4c4d4b4942424c4b4c49484d4a4c4f4a4b4e4c494d49434f4a4e4e
step 3 Attempt- 1
transmission — python tcp_client.py — 191×29
Socket Closing.
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_client.py
Preparing to send DH Message1
Enter Username(e.g:Alice): (Attempt-1):admin
Enter Password(e.g:Alice): (Attempt-1):password
Enter secret of Alice(Xa): 2772
****************** Message 1:Sent from Alice to Server ******************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 313733333131303632343831313639353437313431313231313830353436313837393038353333
g_Xa^Pass(Hex) 41564040465e4252494f434a4a4d424e4f4c4a4f4a4a494a4a434b4e4f4d4a434c424b434e4848
received "AP@ABXEWBBJJLMKIBBLKLIHMJLOJKNLIMICOJNN||?'?4&?I0E?G?ow<<???/??澹?H?)???1??;?iCa}?"
**************** Message 2: Received from Server ****************
g_Xb^Pass(In Hex): 415040414258455742424a4a4c4d4b4942424c4b4c49484d4a4c4f4a4b4e4c494d49434f4a4e4e
Decrypted g_Xb 113257739911760299707236174105726284155
******************** Alice computes Symmetric Key K_AS ********************
Computed Symmetric Key K_AS(In Hex): 0x4625e6cd3bf7271e0c41561f10366062L
Decrypted Ns: 229290321134494875934494576010464763O2
****************** Message 3: Sent from Alice to Server ******************
Enter the seed for calculating Nonce:

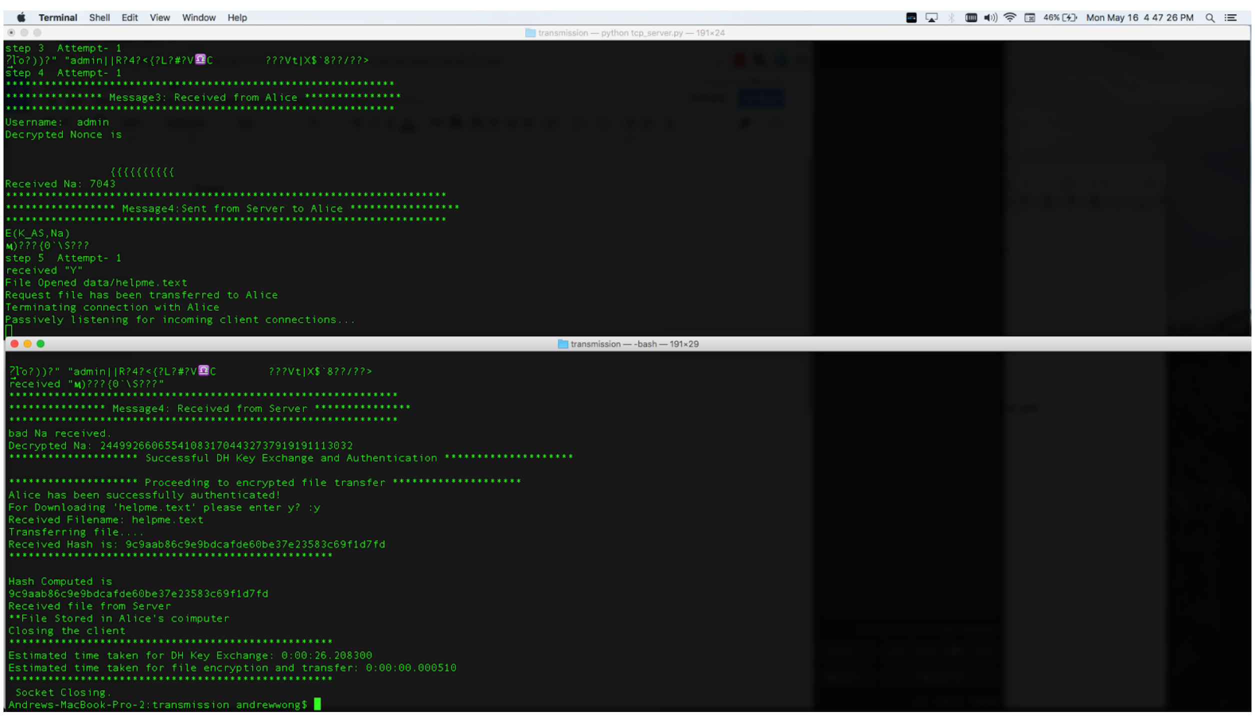


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mon May 16 4 47 22 PM
Capturing from Loopback: lo0
Apply a display filter … <⌘/>
Expression…
No. Time Source Destination Protocol Length Info
1 0.000000 127.0.0.1 127.0.0.1 TCP 68 50534 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=16344 WS=32 TSval=725211368 TSecr=0 SACK_PERM=1
2 0.000069 127.0.0.1 127.0.0.1 TCP 68 8000 → 50534 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=16344 WS=32 TSval=725211368 TSecr=725211368 SA…
3 0.000085 127.0.0.1 127.0.0.1 TCP 56 50534 → 8000 [ACK] Seq=1 Ack=1 Win=408288 Len=0 TSval=725211368 TSecr=725211368
4 0.000097 127.0.0.1 127.0.0.1 TCP 56 [TCP Window Update] 8000 → 50534 [ACK] Seq=1 Ack=1 Win=408288 Len=0 TSval=725211368 TSecr=725211368
5 6.496437 127.0.0.1 127.0.0.1 TCP 157 50534 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=408288 Len=101 TSval=725217859 TSecr=725211368
6 6.496469 127.0.0.1 127.0.0.1 TCP 56 8000 → 50534 [ACK] Seq=1 Ack=102 Win=408192 Len=0 TSval=725217859 TSecr=725217859
7 16.632826 127.0.0.1 127.0.0.1 TCP 145 8000 → 50534 [PSH, ACK] Seq=1 Ack=102 Win=408192 Len=89 TSval=725227989 TSecr=725217859
8 16.632867 127.0.0.1 127.0.0.1 TCP 56 50534 → 8000 [ACK] Seq=102 Ack=90 Win=408192 Len=0 TSval=725227989 TSecr=725227989
9 22.080594 127.0.0.1 127.0.0.1 TCP 111 50534 → 8000 [PSH, ACK] Seq=102 Ack=90 Win=408192 Len=55 TSval=725233429 TSecr=725227989
10 22.080637 127.0.0.1 127.0.0.1 TCP 56 8000 → 50534 [ACK] Seq=90 Ack=157 Win=408128 Len=0 TSval=725233429 TSecr=725233429
11 22.080833 127.0.0.1 127.0.0.1 TCP 72 8000 → 50534 [PSH, ACK] Seq=90 Ack=157 Win=408128 Len=16 TSval=725233429 TSecr=725233429
12 22.080859 127.0.0.1 127.0.0.1 TCP 56 50534 → 8000 [ACK] Seq=157 Ack=106 Win=408192 Len=0 TSval=725233429 TSecr=725233429
Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 50534 (50534), Dst Port: 8000 (8000), Seq: 0, Len: 0
0000 02 00 00 00 45 00 00 40 e8 e9 40 00 40 06 00 00 ....E..@ ..@.@...
0010 7f 00 00 01 7f 00 00 01 c5 66 1f 40 84 72 f8 1b .... .f.@.r..
0020 00 00 00 00 b0 02 ff ff fe 34 00 00 02 04 3f d8 .... .4....?.
0030 01 03 03 05 01 01 08 0a 2b 39 d8 e8 00 00 00 00 .... +9......
0040 04 02 00 00 ....
Loopback: lo0: <live capture in progress>
Packets: 12 · Displayed: 12 (100.0%)
Profile: Default



Terminal Shell Edit View Window Help
Mon May 16 4 47 22 PM
transmission — python tcp_server.py — 191×24
Enter the Seed for calculating Nonce:1317
len 949
Blum Blum Shub generated Ns: 00010001001111111111100010010000011101100011001100110000100111001111101111110100011001000111101110010101111111010111011000001110
g_Xb^Pass: 41504041425845574242 4a4a4c4d4b4942424c4b4c49484d4a4c4f4a4b4e4c494d49434f4a4e4e
step 3 Attempt- 1
step 4 Attempt- 1
*************** Message3: Received from Alice ***************
Username: admin
Decrypted Nonce is
Received Na: 7043
***************** Message4:Sent from Server to Alice *****************
E(K_AS,Na)
step 5 Attempt- 1
transmission — python tcp_client.py — 191×29
**************** Message 2: Received from Server ****************
g_Xb^Pass(In Hex): 415040414258455742424a4a4c4d4b4942424c4b4c49484d4a4c4f4a4b4e4c494d49434f4a4e4e
Decrypted g_Xb 113257739911760299707236174105726284155
******************** Alice computes Symmetric Key K_AS ********************
Computed Symmetric Key K_AS(In Hex): 0x4625e6cd3bf7271e0c41561f10366062L
Decrypted Ns: 229290321134494875934494576010464763 02
****************** Message 3: Sent from Alice to Server ******************
Enter the seed for calculating Nonce:99
len 949
Na: 10111000010011111101111011000000111010100000001011000110001111001011000000001100011111010100010001011000010011010010111010101001000
(Ns || Na):
*************** Message4: Received from Server ***************
bad Na received.
Decrypted Na: 244992660655410831704432737919191113032
******************** Successful DH Key Exchange and Authentication ********************
******************** Proceeding to encrypted file transfer ********************
Alice has been successfully authenticated!
For Downloading 'helpme.text' please enter y? :





2. Snaps of your output sample for the experiment in Step 2 (successful authentication), as well as Step 6 (Error Response) ***[upper of Lower screen is Server and lower of Lower screen is Client]***

a. Successful Authentication

transmission — python tcp_server.py — 100×24

```
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_server.py
Server socket created
Socket is passively listening in port number 8000 for incoming client connections
Passively listening for incoming client connections...
step 1  Attempt- 0
step 2  Attempt- 1
***********************************************************
*************** Message 1:Received from Alice ***************
***********************************************************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 41564040465e4252494f434a4a4d424e4f4c4a4f4a4a494a4a434b4e4f4d4a434c424b434e4848
Enter Server secret (Xb):
```

transmission — python tcp_client.py — 101×28

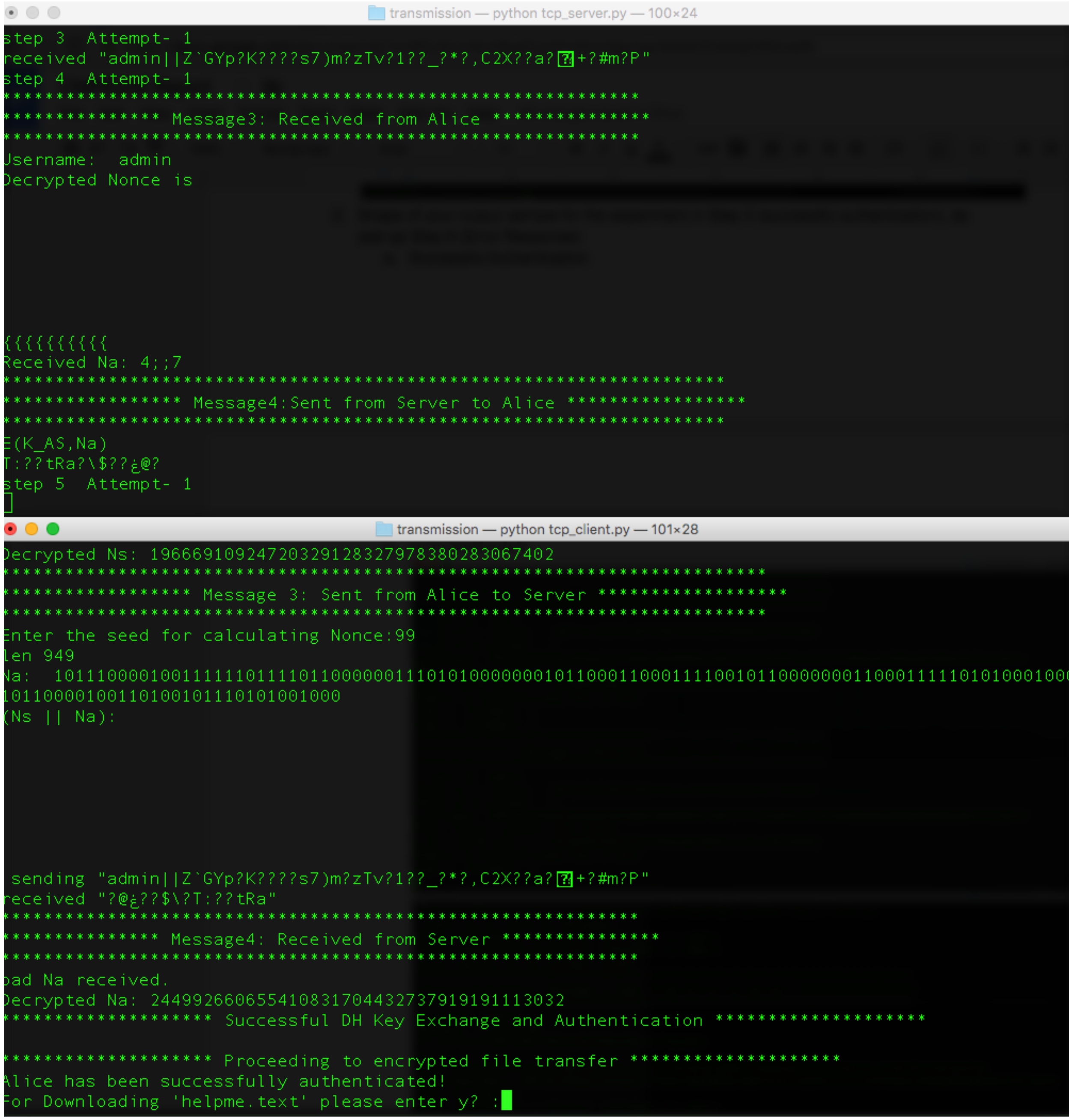
```
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_client.py
Preparing to send DH Message1
Enter Username(e.g:Alice): (Attempt-1):admin
Enter Password(e.g:Alice): (Attempt-1):password
Enter secret of Alice(Xa): 2772
***********************************************************************
****************** Message 1:Sent from Alice to Server ******************
***********************************************************************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 3137333331313036323438313136393534373134313132313138303534363138373930383533333
g_Xa^Pass(Hex) 41564040465e4252494f434a4a4d424e4f4c4a4f4a4a494a4a434b4e4f4d4a434c424b434e4848
```

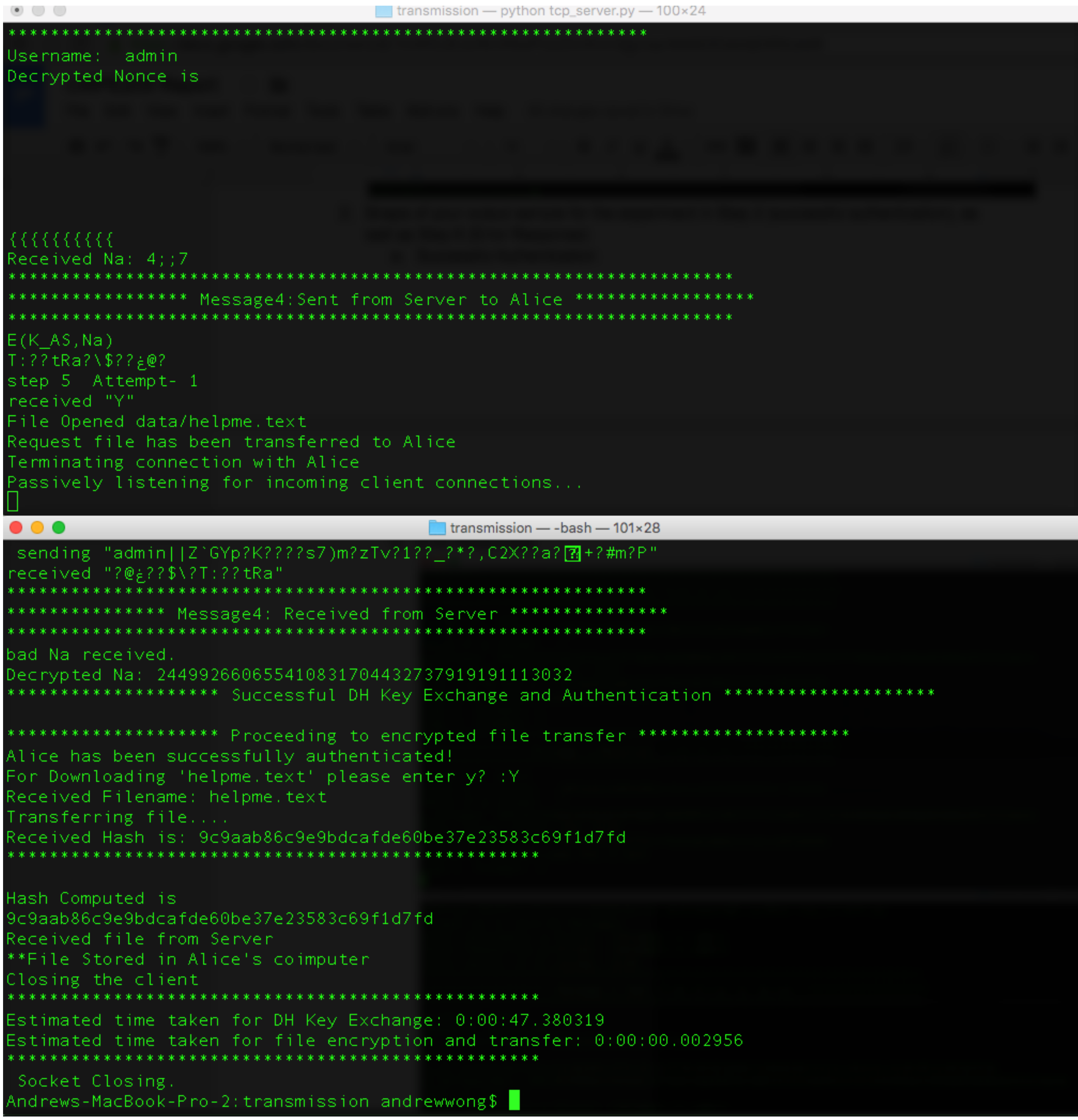
transmission — python tcp_server.py — 100×24

```
*************** Message 1:Received from Alice ***************
*************************************************************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 41564040465e4252494f434a4a4d424e4f4c4a4f4a4a494a4a434b4e4f4d4a434c424b434e4848
Enter Server secret (Xb):7698
g_Xb = g^Xb mod p = 113257739911760299707236174105726284155
Decrypted g_Xa:  173311062481169547141121180546187908533
******************** Server comutes Symmetric K_AS ********************
Computed Symmetric Key K_AS(In Hex): 0x4625e6cd3bf7271e0c41561f10366062L



*************************************************************************
****************** Message2: Sent from Server to Alice ******************
*************************************************************************
Enter the Seed for calculating Nonce:1217
len 949
Blum Blum Shub generated Ns:  000011101100101110110101100100100111101011000111111111001101001100010
0010010001011110001100010111100000011001110111100000001010
g_Xb^Pass: 4150404142584557424 24a4a4c4d4b4942424c4b4c49484d4a4c4f4a4b4e4c494d49434f4a4e4e
step 3  Attempt- 1
```

transmission — python tcp_client.py — 101×28

```
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_client.py
Preparing to send DH Message1
Enter Username(e.g:Alice): (Attempt-1):admin
Enter Password(e.g:Alice): (Attempt-1):password
Enter secret of Alice(Xa): 2772
*************************************************************************
****************** Message 1:Sent from Alice to Server ******************
*************************************************************************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 3137333331313036323438313136393534373134313132313138303534363138373930383533 33
g_Xa^Pass(Hex) 41564040465e4252494f434a4a4d424e4f4c4a4f4a4a494a4a434b4e4f4d4a434c424b434e4848
received "AP@ABXEWBBJJLMKIBBLKLIHMJLOJKNLIMICOJNN||m`?R?g???*?G????5??ƒ???>R?!??]?j???"
*****************************************************************
**************** Message 2: Received from Server ****************
*****************************************************************
g_Xb^Pass(In Hex): 415040414258455742424a4a4c4d4b4942424c4b4c49484d4a4c4f4a4b4e4c494d49434f4a4e4e
Decrypted g_Xb 113257739911760299707236174105726284155
******************** Alice computes Symmetric Key K_AS ********************
Computed Symmetric Key K_AS(In Hex): 0x4625e6cd3bf7271e0c41561f10366062L
Decrypted Ns: 196669109247203291283279783802 83067402
*************************************************************************
****************** Message 3: Sent from Alice to Server ******************
*************************************************************************
Enter the seed for calculating Nonce:
```


transmission — python tcp_server.py — 100×24
step 3 Attempt- 1
received "admin||Z`GYp?K????s7)m?zTv?1??_?*?,C2X??a?+?#m?P"
step 4 Attempt- 1
****
************** Message3: Received from Alice **************
****
Username: admin
Decrypted Nonce is
{{{{{{{{{{
Received Na: 4;;7
****
**************** Message4:Sent from Server to Alice *****************
****
E(K_AS,Na)
T:??tRa?\$??¿@?
step 5 Attempt- 1
transmission — python tcp_client.py — 101×28
Decrypted Ns: 196669109247203291283279783802830674O2
****
***************** Message 3: Sent from Alice to Server *****************
****
Enter the seed for calculating Nonce:99
len 949
Na: 10111000010011111101111011000000111010100000001011000110001111001011000000011000111110101000100
10110000100110100101110101001000
(Ns || Na):
sending "admin||Z`GYp?K????s7)m?zTv?1??_?*?,C2X??a?+?#m?P"
received "?@¿??$\?T:??tRa"
****
************** Message4: Received from Server **************
****
bad Na received.
Decrypted Na: 244992660655410831704432737919191113032
******************** Successful DH Key Exchange and Authentication ********************
******************** Proceeding to encrypted file transfer ********************
Alice has been successfully authenticated!
For Downloading 'helpme.text' please enter y? :



```
transmission — python tcp_server.py — 100×24
************************************************************
Username:  admin
Decrypted Nonce is




{{{{{{{{{{
Received Na: 4;;7
********************************************************************
***************** Message4:Sent from Server to Alice *****************
********************************************************************
E(K_AS,Na)
T:??tRa?\$??¿@?
step 5  Attempt- 1
received "Y"
File Opened data/helpme.text
Request file has been transferred to Alice
Terminating connection with Alice
Passively listening for incoming client connections...
```

```
transmission — -bash — 101×28
 sending "admin||Z`GYp?K????s7)m?zTv?1??_?*?,C2X??a??+?#m?P"
received "?@¿??$\?T:??tRa"
************************************************************
*************** Message4: Received from Server ***************
************************************************************
bad Na received.
Decrypted Na: 244992660655410831704432737919191113032
******************** Successful DH Key Exchange and Authentication ********************

******************** Proceeding to encrypted file transfer ********************
Alice has been successfully authenticated!
For Downloading 'helpme.text' please enter y? :Y
Received Filename: helpme.text
Transferring file....
Received Hash is: 9c9aab86c9e9bdcafde60be37e23583c69f1d7fd
**************************************************

Hash Computed is
9c9aab86c9e9bdcafde60be37e23583c69f1d7fd
Received file from Server
**File Stored in Alice's coimputer
Closing the client
**************************************************
Estimated time taken for DH Key Exchange: 0:00:47.380319
Estimated time taken for file encryption and transfer: 0:00:00.002956
**************************************************
 Socket Closing.
Andrews-MacBook-Pro-2:transmission andrewwong$
```

b. Error Responses

```
************************************************************
*************** Message 1:Received from Alice ***************
************************************************************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
Enter Server secret (Xb):1234
g_Xb = g^Xb mod p = 161049218417163768896398823192136538956
Unable to Authneticate the client
step 1  Attempt- 1
step 2  Attempt- 2
************************************************************
*************** Message 1:Received from Alice ***************
************************************************************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
Enter Server secret (Xb):1234
g_Xb = g^Xb mod p = 161049218417163768896398823192136538956
Unable to Authneticate the client
step 1  Attempt- 2
```

```
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_client.py
Preparing to send DH Message1
Enter Username(e.g:Alice): (Attempt-1):admin
Enter Password(e.g:Alice): (Attempt-1):admin
Enter secret of Alice(Xa): 1234
***********************************************************************
****************** Message 1:Sent from Alice to Server ******************
***********************************************************************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 31363130343932313834313731363337363838393633393838323331393231333635333838393536
g_Xa^Pass(Hex) 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
back to step  1
Enter Username(e.g:Alice): (Attempt-2):admin
Enter Password(e.g:Alice): (Attempt-2):admin
Enter secret of Alice(Xa): 1234
***********************************************************************
****************** Message 1:Sent from Alice to Server ******************
***********************************************************************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 31363130343932313834313731363337363838393633393838323331393231333635333838393536
g_Xa^Pass(Hex) 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
back to step  1
Enter Username(e.g:Alice): (Attempt-3):
```

transmission — python tcp_se

```
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_server.py
Server socket created
Socket is passively listening in port number 8000 for incoming client connections
Passively listening for incoming client connections...
step 1  Attempt- 0
step 2  Attempt- 1
************************************************************
*************** Message 1:Received from Alice ***************
************************************************************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 50525c595a42494a434f4a4c4a4d484c4d4343424d484243434949484a42494a484d4e4843424e4d
Enter Server secret (Xb):1234
g_Xb = g^Xb mod p = 161049218417163768896398823192136538956
Unable to Authneticate the client
step 1  Attempt- 1
```

transmission — python tcp_c

```
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_client.py
Preparing to send DH Message1
Enter Username(e.g:Alice): (Attempt-1):admin
Enter Password(e.g:Alice): (Attempt-1):admin
Enter secret of Alice(Xa): 1234
************************************************************************
****************** Message 1:Sent from Alice to Server ******************
************************************************************************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 31363130343932313834313731363337363838393633393838323331393231333635333838393536
g_Xa^Pass(Hex) 50525c595a42494a434f4a4c4a4d484c4d4343424d484243434949484a42494a484d4e4843424e4d
back to step  1
Enter Username(e.g:Alice): (Attempt-2):
```

transmission — python

```
************************************************************
*************** Message 1:Received from Alice ***************
************************************************************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
Enter Server secret (Xb):1234
g_Xb = g^Xb mod p = 161049218417163768896398823192136538956
Unable to Authneticate the client
step 1  Attempt- 1
step 2  Attempt- 2
************************************************************
*************** Message 1:Received from Alice ***************
************************************************************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
Enter Server secret (Xb):1234
g_Xb = g^Xb mod p = 161049218417163768896398823192136538956
Unable to Authneticate the client
step 1  Attempt- 2
```

transmission — python

```
Andrews-MacBook-Pro-2:transmission andrewwong$ python tcp_client.py
Preparing to send DH Message1
Enter Username(e.g:Alice): (Attempt-1):admin
Enter Password(e.g:Alice): (Attempt-1):admin
Enter secret of Alice(Xa): 1234
************************************************************************
****************** Message 1:Sent from Alice to Server ******************
************************************************************************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 31363130343932313834313731363337363838393633393838323331393231333635333838393536
g_Xa^Pass(Hex) 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
back to step  1
Enter Username(e.g:Alice): (Attempt-2):admin
Enter Password(e.g:Alice): (Attempt-2):admin
Enter secret of Alice(Xa): 1234
************************************************************************
****************** Message 1:Sent from Alice to Server ******************
************************************************************************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 31363130343932313834313731363337363838393633393838323331393231333635333838393536
g_Xa^Pass(Hex) 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
back to step  1
Enter Username(e.g:Alice): (Attempt-3):
```

```
************************************************************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
Enter Server secret (Xb):1234
g_Xb = g^Xb mod p = 161049218417163768896398823192136538956
Unable to Authneticate the client
step 1  Attempt- 2
step 2  Attempt- 3
************************************************************
*************** Message 1:Received from Alice ***************
************************************************************
Client ID: admin
Value of p chosen : 197221152031991558322935568090317202983
Value of g chosen : 2
g_Xa^pass: 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
Enter Server secret (Xb):1234
g_Xb = g^Xb mod p = 161049218417163768896398823192136538956
Unable to Authneticate the client
step 1  Attempt- 3
3 attempts has reaches. The connection closes.
Passively listening for incoming client connections...
```

```
back to step  1
Enter Username(e.g:Alice): (Attempt-2):admin
Enter Password(e.g:Alice): (Attempt-2):admin
Enter secret of Alice(Xa): 1234
************************************************************************
****************** Message 1:Sent from Alice to Server ******************
************************************************************************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 31363130343932313834313731363337363838393633393838323331393231333635333838393536
g_Xa^Pass(Hex) 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
back to step  1
Enter Username(e.g:Alice): (Attempt-3):admin
Enter Password(e.g:Alice): (Attempt-3):admin
Enter secret of Alice(Xa): 1234
************************************************************************
****************** Message 1:Sent from Alice to Server ******************
************************************************************************
ClientID: admin
Request: Secure DH
P= 197221152031991558322935568090317202983
g= 2
g_Xa 31363130343932313834313731363337363838393633393838323331393231333635333838393536
g_Xa^Pass(Hex) 50525c595a42494a434f4a4c4a4d484c4d4343424d4842434349484a42494a484d4e4843424e4d
3 attempts has reached. bye.
 Socket Closing.
Andrews-MacBook-Pro-2:transmission andrewwong$
```

3.

Encrypted Key Exchange (also known as **EKE**) is a family of password authenticated key agreement methods described by Steven M bellovin and Michael Merritt. Although several of the forms of EKE in this paper were later found to be flawed, the surviving, refined, and enhanced forms of EKE effectively make this the first method to amplify a shared password into a shared key, where the shared key may subsequently be used to provide a zero knowledge password proof or other functions.

In the most general form of EKE, at least one party encrypts an ephemeral (one-time) public key using a password, and sends it to a second party, who decrypts it and uses it to negotiate a shared key with the first party.
Augmented-EKE, introduced the concept of **augmented** password authenticated key agreement for client/server scenarios. Augmented methods have the added goal of ensuring that password verification data stolen from a server cannot be used by an attacker to masquerade as the client, unless the attacker first determines the password (e.g. by performing a brute force attack on the stolen data).
A version of EKE based on Diffie hellman(DH), known as DH-EKE, has survived attack and has led to improved variations, such as the PAK family of methods in IEEE P1363.2.
With the US patent on EKE expiring in late 2011, an EAP authentication method using EKE was published as an IETF RFC.The EAP method uses the Diffie-Hellman variant of EKE.

This code advantages:

In our experiment compared to Diffie hellman, EKE has and advantage of mutual authentication and Data integrity as we have included Nonces(Na,Ns) in client and server and after three messages are exchanged in the EKE process in our code, the nonce Na, of the client is transferred to the server and both sided Na is checked after the fourth step or the fourth message where the server sends the encrypted nonce Na with Kas and client decrypts it with Kas it has and it gets the Na which is send by server and at this stage it compares both the Na's and if the Na initially chosen by client and Na at the end of 4th step send by server is the same then the client is authenticated by the server and if not client detects the fault and server detects the Ns which is wrong from the server and it also stops the connection. Plus it is also possible to unable to compute the Kas by exponentially computing "server's computed Xa Client's Nonce" and "Xs Server's Nonce" that resulting in authentication failure.
So the man in the middle or trudy which wants to connect to the server obviously will have the incorrect Na which it sends and so client detects it first identifying that it is intruder and then with the incorrect Na it has it will also send incorrect Ns back to the server which will eventually detects it after the fourth step.So the server declines the connection