Exercise 1:

```
at java.base/sun.nio.cs.StreamDecoder.readBytes(StreamDecoder at java.base/sun.nio.cs.StreamDecoder.implRead(StreamDecoder at java.base/sun.nio.cs.StreamDecoder.implRead(StreamDecoder at java.base/sun.nio.cs.StreamDecoder.implRead(StreamDecoder.jijuliaolmstead@Julias-MacBook-Pro % cd desktop/@it/CaesarCipher/src at java.base/java.io.BufferedReader.read(InputStreamRea juliaolmstead@Julias-MacBook-Pro src % java CaesarCipherClient.java at java.base/java.io.BufferedReader.readline(BufferedReader.ja at java.base/java.io.BufferedReader.readline(BufferedReader at java.base/java.io.BufferedReader at java.b
                                                                                                                                                                                                                                                                                                                                                                                                                                                                  1) · //terminate vm
src — java CaesarCipherClient.java — 80×24
at java.base/sun.nio.cs.StreamDecoder.implRead(StreamDecod
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      src — java CaesarCipherClient.java — 80×24
     at java.base/sun.nio.cs.StreamDecoder.implRead(StreamDecoder.j Last login: Sat Nov 6 21:00:26 on ttys002 at java.base/java.io.lnputStreamReader.read(InputStreamReader.jjuliaolmstead@Julias-MacBook-Pro x cd desktop/Git/CaesarCipher/src at java.base/java.io.BufferedReader.readLine(BufferedReader.je juliaolmstead@Julias-MacBook-Pro src % java CaesarCipherClient.java at java.base/java.io.BufferedReader.readLine(BufferedReader at java.base/java.io.BufferedReader.readLine(BufferedReader at java.base/java.io.BufferedReader.readLine(BufferedReader at java.base/java.io.BufferedReader.readLine(BufferedReader at java.base/java.io.BufferedReader.geder at java.base/java.io.BufferedReader.geder at CaesarCipherServer.main(CaesarCipherServer.Java:56) place send the key juliaolmstead@Julias-MacBook-Pro src % java CaesarCipherClient.java hmmm please send the key geder at language send the key geder for connection at language send the key geder fo
   juliaolmstead@Julias-MacBook-Pro src % ja

Listening for connection ...

Connection successful

Listening for input ...

Message from client: hmmm

Message from client: bbbb

Decrypted: aaa

Message from client: PPPP

Decrypted: 0000

Message from client: NPPPPPPP

Decrypted: MO000000

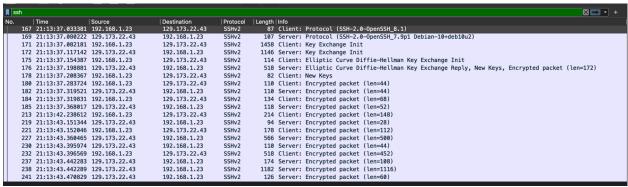
Message from client: TpnfujnftJtubzvq

Decrypted: SometimesIstayup

Message from client: Cblb

Decrypted: Baka
                                                                                                                                                                                                                                                                                                                                                                                            aaaa
0000
M0000000
                                                                                                                                                                                                                                                                                                                                                                                              SometimesIstayup
                                                                                                                                                                                                                                                                                                                                                                                              Baka
       Decrypted: Baka
                                                       Message from client: Itkhz
                                                   at java.base/sun.nio.cs.StreamDecoder.implRead(StreamDecod
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    src — java CaesarCipherClient.java — 80×24
   Decrypted: amazeballs
Message from client: XJJG
Decrypted: COOL
Message from client: YVHiYvidzg
Decrypted: DAMnDanniel
Message from client: WvxfvodoVBVDIrdoc
Decrypted: BackatitAGAINwith
Message from client: oczRCDOZQVIN
Decrypted: theWHITEVANS
```

Exercise 2



Open protocol

167	21:13:37.033381 192.168.1.23	129.173.22.43	SSHv2	87 Client: Protocol (SSH-2.0-OpenSSH_8.1)
	21:13:37.080222 129.173.22.43	192.168.1.23	SSHv2	107 Server: Protocol (SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2)

Open the ssh connec.

Negotiations start

- 1					
I	171 21:13:37.082181	192.168.1.23	129.173.22.43	SSHv2	1458 Client: Key Exchange Init
Π	172 21:13:37.117142	129.173.22.43	192.168.1.23	SSHv2	1146 Server: Key Exchange Init

Client sends several parameters negotiation, compression, and cryptography algorithms.

The server replies to these.

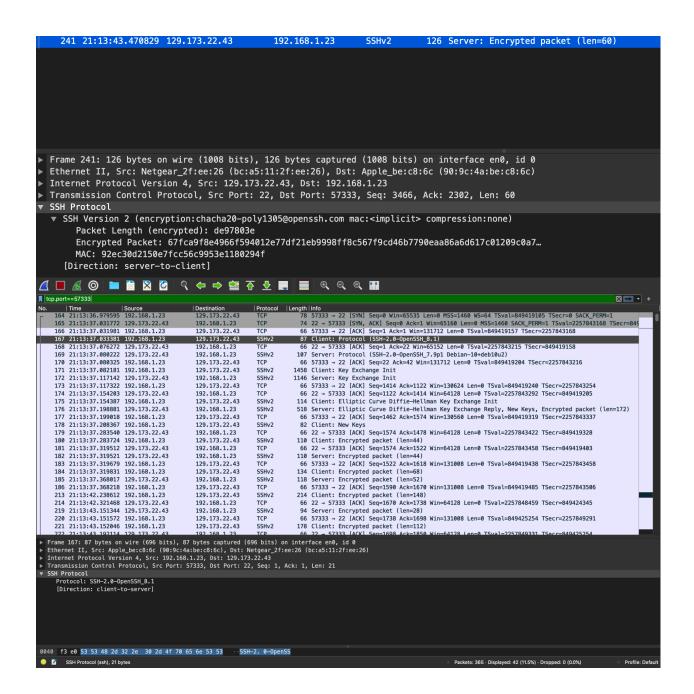
DH

175 21:13:37	1.154387 192.168.1.23	129.173.22.43	SSHv2	114	Client:	Elliptic	Curve	Diffie-Hellma	in Key	Exchange	Init					
	.198881 129.173.22.43	192.168.1.23	SSHv2				Curve	Diffie-Hellma	in Key	Exchange	Reply,	New Ke	ys, E	ncrypted	packet	(len=172)
	negotiates	dh params														
Server	replies to	the above														

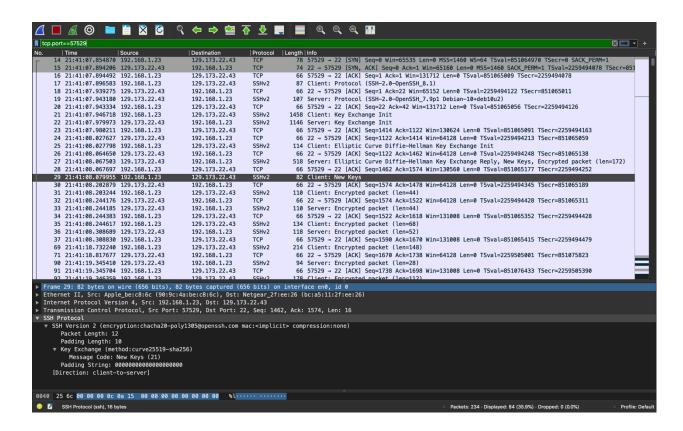
Have some keys

<u> </u>			
178 21:13:37.208367 192	.168.1.23 129.173.2	22.43 SSHv2 82	Client: New Keys

Acknowledgement message Encryption from here on out



New session continued below, was too tired to do assignment all at once.



Gray +blue before sshv2

_ 14 21:41:07.854870 192.168.1.23	129.173.22.43 TCP	78 57529 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=851064970 TSecr=0 SACK
15 21:41:07.894206 129.173.22.43	192.168.1.23 TCP	74 22 → 57529 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=22594
16 21:41:07.894492 192.168.1.23	129.173.22.43 TCP	66 57529 → 22 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=851065009 TSecr=2259494078
17 21:41:07.896583 192.168.1.23	129.173.22.43 SSHv2	87 Client: Protocol (SSH-2.0-OpenSSH 8.1)

These lads

182 21:41:24.825824 129.173.22.43	192.168.1.23 TCF	66 22 → 57529 [FIN, ACK] Seq=4142 Ack=2651 Win=64128 Len=0 TSval=2259511009 TSecr=85
183 21:41:24.826068 192.168.1.23	129.173.22.43 TCF	66 57529 → 22 [ACK] Seq=2651 Ack=4143 Win=131072 Len=0 TSval=851081881 TSecr=2259511