

B00780639
Julia Olmstead

Exercise 1:

```
src — java CaesarCipherServer.java — 80x24
at java.base/sun.nio.cs.StreamDecoder.readBytes(StreamDeco
at java.base/sun.nio.cs.StreamDecoder.implRead(StreamDecod
at java.base/sun.nio.cs.StreamDecoder.read(StreamDecoder.j
at java.base/java.io.InputStreamReader.read(InputStreamRea
at java.base/java.io.BufferedReader.fill(BufferedReader.ja
at java.base/java.io.BufferedReader.readLine(BufferedReader
at java.base/java.io.BufferedReader.readLine(BufferedReader
at CaesarCipherServer.main(CaesarCipherServer.java:56)
juliaolmstead@Julias-MacBook-Pro src % java CaesarCipherServ
Listening for connection ...
Connection successful
Listening for input ...
Message from client: Test
Message from client: wow
Message from client: Please send the key
Message from client: tvt
Decrypted: Uwu
Message from client: Itkhz
Decrypted: Julia
Message from client: hr
Decrypted: is
Message from client: Bnnk
Decrypted: Cool
[

src — java CaesarCipherClient.java — 80x24
Last login: Sat Nov 6 20:57:12 on ttys002
juliaolmstead@Julias-MacBook-Pro ~ % cd desktop/Git/CaesarCipher/src
juliaolmstead@Julias-MacBook-Pro src % java CaesarCipherClient.java
Test
echo: Test
wow
echo: wow
Please send the key
echo: 25
uwu
Julia
is
Cool
[

src — java CaesarCipherServer.java — 80x24
at java.base/sun.nio.cs.StreamDecoder.implRead(StreamDecod
at java.base/sun.nio.cs.StreamDecoder.read(StreamDecoder.j
at java.base/java.io.InputStreamReader.read(InputStreamRea
at java.base/java.io.BufferedReader.fill(BufferedReader.ja
at java.base/java.io.BufferedReader.readLine(BufferedReader
at java.base/java.io.BufferedReader.readLine(BufferedReader
at CaesarCipherServer.main(CaesarCipherServer.java:56)
juliaolmstead@Julias-MacBook-Pro src % java CaesarCipherServ
Listening for connection ...
Connection successful
Listening for input ...
Message from client: hmmm
Message from client: Please send the key
Message from client: bbbb
Decrypted: aaaa
Message from client: PPPP
Decrypted: OOOO
Message from client: NPPPPPPP
Decrypted: MOOOOOOOO
Message from client: TpnfujnftJtubzvq
Decrypted: SometimesIstayup
Message from client: Cblb
Decrypted: Baka
[

src — java CaesarCipherClient.java — 80x24
Last login: Sat Nov 6 21:00:26 on ttys002
juliaolmstead@Julias-MacBook-Pro ~ % cd desktop/Git/CaesarCipher/src
juliaolmstead@Julias-MacBook-Pro src % java CaesarCipherClient.java
hmmm
echo: hmmm
Please send the key
echo: 1
aaaa
OOOO
MOOOOOOOO
SometimesIstayup
Baka
[

src — java CaesarCipherServer.java — 80x24
at java.base/sun.nio.cs.StreamDecoder.implRead(StreamDecod
at java.base/sun.nio.cs.StreamDecoder.read(StreamDecoder.j
at java.base/java.io.InputStreamReader.read(InputStreamRea
at java.base/java.io.BufferedReader.fill(BufferedReader.ja
at java.base/java.io.BufferedReader.readLine(BufferedReader
at java.base/java.io.BufferedReader.readLine(BufferedReader
at CaesarCipherServer.main(CaesarCipherServer.java:56)
juliaolmstead@Julias-MacBook-Pro src % java CaesarCipherServ
Listening for connection ...
Connection successful
Listening for input ...
Message from client: I am tired
Message from client: Please send the key
Message from client: vhwzvwggn
Decrypted: amazeballs
Message from client: XJJG
Decrypted: COOL
Message from client: YVHiYvidzg
Decrypted: DAMnDaniel
Message from client: WvxfvodoVBVDIrdoc
Decrypted: BackatitAGAINwith
Message from client: oczRCDOZQVIN
Decrypted: theWHITEVANS
[

src — java CaesarCipherClient.java — 80x24
Last login: Sat Nov 6 20:59:13 on ttys002
juliaolmstead@Julias-MacBook-Pro ~ % cd desktop/Git/CaesarCipher/src
juliaolmstead@Julias-MacBook-Pro src % java CaesarCipherClient.java
I am tired
echo: I am tired
Please send the key
echo: 21
amazeballs
COOL
DAMn Daniel
BackatitAGAINwith
theWHITEVANS
[
```

Exercise 2

No.	Time	Source	Destination	Protocol	Length	Info
167	21:13:37.033381	192.168.1.23	129.173.22.43	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_8.1)
169	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)
171	21:13:37.082181	192.168.1.23	129.173.22.43	SSHv2	1458	Client: Key Exchange Init
172	21:13:37.117142	129.173.22.43	192.168.1.23	SSHv2	1146	Server: Key Exchange Init
175	21:13:37.154387	192.168.1.23	129.173.22.43	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
176	21:13:37.198881	129.173.22.43	192.168.1.23	SSHv2	518	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)
178	21:13:37.208367	192.168.1.23	129.173.22.43	SSHv2	82	Client: New Keys
180	21:13:37.283724	192.168.1.23	129.173.22.43	SSHv2	110	Client: Encrypted packet (len=44)
182	21:13:37.319521	129.173.22.43	192.168.1.23	SSHv2	110	Server: Encrypted packet (len=44)
184	21:13:37.319831	192.168.1.23	129.173.22.43	SSHv2	134	Client: Encrypted packet (len=68)
185	21:13:37.368017	129.173.22.43	192.168.1.23	SSHv2	118	Server: Encrypted packet (len=52)
213	21:13:42.238612	192.168.1.23	129.173.22.43	SSHv2	214	Client: Encrypted packet (len=148)
219	21:13:43.151344	129.173.22.43	192.168.1.23	SSHv2	94	Server: Encrypted packet (len=28)
221	21:13:43.152046	192.168.1.23	129.173.22.43	SSHv2	178	Client: Encrypted packet (len=112)
227	21:13:43.360465	129.173.22.43	192.168.1.23	SSHv2	566	Server: Encrypted packet (len=500)
230	21:13:43.395974	129.173.22.43	192.168.1.23	SSHv2	110	Server: Encrypted packet (len=44)
232	21:13:43.396569	192.168.1.23	129.173.22.43	SSHv2	518	Client: Encrypted packet (len=452)
237	21:13:43.442283	129.173.22.43	192.168.1.23	SSHv2	174	Server: Encrypted packet (len=108)
238	21:13:43.442289	129.173.22.43	192.168.1.23	SSHv2	1182	Server: Encrypted packet (len=1116)
241	21:13:43.470829	129.173.22.43	192.168.1.23	SSHv2	126	Server: Encrypted packet (len=60)

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)
169	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

171	21:13:37.082181	192.168.1.23	129.173.22.43	SSHv2	1458	Client: Key Exchange Init
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	21:13:37.154387	192.168.1.23	129.173.22.43	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
176	21:13:37.198881	129.173.22.43	192.168.1.23	SSHv2	518	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)

Client negotiates dh params

Server replies to the above

Have some keys

178	21:13:37.208367	192.168.1.23	129.173.22.43	SSHv2	82	Client: New Keys
-----	-----------------	--------------	---------------	-------	----	------------------

Acknowledgement message

Encryption from here on out

241 21:13:43.470829 129.173.22.43 192.168.1.23 SSHv2 126 Server: Encrypted packet (len=60)

▶ Frame 241: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface en0, id 0
 ▶ Ethernet II, Src: Netgear_2f:ee:26 (bc:a5:11:2f:ee:26), Dst: Apple_be:c8:6c (90:9c:4a:be:c8:6c)
 ▶ Internet Protocol Version 4, Src: 129.173.22.43, Dst: 192.168.1.23
 ▶ Transmission Control Protocol, Src Port: 22, Dst Port: 57333, Seq: 3466, Ack: 2302, Len: 60
 ▼ SSH Protocol
 SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none)
 Packet Length (encrypted): de97803e
 Encrypted Packet: 67fca9f8e4966f594012e77df21eb9998ff8c567f9cd46b7790eaa86a6d617c01209c0a7...
 MAC: 92ec30d2150e7fcc56c9953e1180294f
 [Direction: server-to-client]

No.	Time	Source	Destination	Protocol	Length/Info
164	21:13:36.979505	129.173.22.43	129.173.22.43	TCP	78 57333 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=849419105 TSecr=0 SACK_PERM=1
165	21:13:37.031772	129.173.22.43	192.168.1.23	TCP	74 22 → 57333 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2257843168 TSecr=849419158
166	21:13:37.031981	192.168.1.23	129.173.22.43	TCP	66 57333 → 22 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=849419157 TSecr=2257843168
167	21:13:37.033301	192.168.1.23	129.173.22.43	SSHv2	87 Client: Protocol (SSH-2.0-openssh_8.1)
168	21:13:37.076272	129.173.22.43	192.168.1.23	TCP	66 22 → 57333 [ACK] Seq=1 Ack=22 Win=65152 Len=0 TSval=2257843215 TSecr=849419158
169	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)
170	21:13:37.080325	192.168.1.23	129.173.22.43	TCP	66 57333 → 22 [ACK] Seq=22 Ack=42 Win=131712 Len=0 TSval=849419204 TSecr=2257843216
171	21:13:37.082181	192.168.1.23	129.173.22.43	SSHv2	1458 Client: Key Exchange Init
172	21:13:37.117142	192.173.22.43	192.168.1.23	SSHv2	1146 Server: Key Exchange Init
173	21:13:37.117322	192.168.1.23	129.173.22.43	TCP	66 57333 → 22 [ACK] Seq=1414 Ack=1122 Win=130624 Len=0 TSval=849419240 TSecr=2257843254
174	21:13:37.154203	192.173.22.43	192.168.1.23	TCP	66 22 → 57333 [ACK] Seq=1122 Ack=1414 Win=64128 Len=0 TSval=2257843292 TSecr=849419205
175	21:13:37.154387	192.168.1.23	129.173.22.43	SSHv2	114 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
176	21:13:37.198881	129.173.22.43	192.168.1.23	SSHv2	518 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)
177	21:13:37.199018	192.168.1.23	129.173.22.43	TCP	66 57333 → 22 [ACK] Seq=1462 Ack=1574 Win=130560 Len=0 TSval=849419319 TSecr=2257843337
178	21:13:37.208367	192.168.1.23	129.173.22.43	SSHv2	82 Client: New Keys
179	21:13:37.283540	129.173.22.43	192.168.1.23	TCP	66 22 → 57333 [ACK] Seq=1574 Ack=1478 Win=64128 Len=0 TSval=2257843422 TSecr=849419328
180	21:13:37.283724	192.168.1.23	129.173.22.43	SSHv2	110 Client: Encrypted packet (len=44)
181	21:13:37.319512	129.173.22.43	192.168.1.23	TCP	66 22 → 57333 [ACK] Seq=1574 Ack=1522 Win=64128 Len=0 TSval=2257843458 TSecr=849419403
182	21:13:37.319521	129.173.22.43	192.168.1.23	SSHv2	110 Server: Encrypted packet (len=44)
183	21:13:37.319679	192.168.1.23	129.173.22.43	TCP	66 57333 → 22 [ACK] Seq=1522 Ack=1618 Win=131008 Len=0 TSval=849419438 TSecr=2257843458
184	21:13:37.319831	192.168.1.23	129.173.22.43	SSHv2	134 Client: Encrypted packet (len=68)
185	21:13:37.368017	129.173.22.43	192.168.1.23	SSHv2	118 Server: Encrypted packet (len=52)
186	21:13:37.368218	192.168.1.23	129.173.22.43	TCP	66 57333 → 22 [ACK] Seq=1590 Ack=1670 Win=131008 Len=0 TSval=849419485 TSecr=2257843506
213	21:13:42.238612	192.168.1.23	129.173.22.43	SSHv2	214 Client: Encrypted packet (len=148)
214	21:13:42.321468	129.173.22.43	192.168.1.23	TCP	66 22 → 57333 [ACK] Seq=1670 Ack=1738 Win=64128 Len=0 TSval=2257848459 TSecr=849424345
219	21:13:43.151344	129.173.22.43	192.168.1.23	SSHv2	94 Server: Encrypted packet (len=28)
220	21:13:43.151572	192.168.1.23	129.173.22.43	TCP	66 57333 → 22 [ACK] Seq=1738 Ack=1698 Win=131008 Len=0 TSval=849425254 TSecr=2257849291
221	21:13:43.152046	192.168.1.23	129.173.22.43	SSHv2	178 Client: Encrypted packet (len=112)
222	21:13:43.192114	129.173.22.43	192.168.1.23	TCP	66 22 → 57333 [ACK] Seq=1698 Ack=1850 Win=64128 Len=0 TSval=2257849331 TSecr=849425254

▶ Frame 167: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface en0, id 0
 ▶ Ethernet II, Src: Apple_be:c8:6c (90:9c:4a:be:c8:6c), Dst: Netgear_2f:ee:26 (bc:a5:11:2f:ee:26)
 ▶ Internet Protocol Version 4, Src: 192.168.1.23, Dst: 129.173.22.43
 ▶ Transmission Control Protocol, Src Port: 57333, Dst Port: 22, Seq: 1, Ack: 1, Len: 21
 ▼ SSH Protocol
 Protocol: SSH-2.0-OpenSSH_8.1
 [Direction: client-to-server]

0040 f3 e0 53 53 48 2d 32 2e 30 2d 4f 70 65 6e 53 53 · SSH-2.0-OpenSSH

SSH Protocol (ssh), 21 bytes

Packets: 365 · Displayed: 42 (11.5%) · Dropped: 0 (0.0%) · Profile: Default

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

tcp.port==57529						
No.	Time	Source	Destination	Protocol	Length	Info
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_PERM=1
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=2259494078 TSecr=851064970
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)
18	21:41:07.939275	129.173.22.43	192.168.1.23	TCP	66	22 → 57529 [ACK] Seq=1 Ack=22 Win=65152 Len=0 TSval=2259494122 TSecr=851065011
19	21:41:07.943180	129.173.22.43	192.168.1.23	SSHv2	107	Server: Protocol (SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2)
20	21:41:07.943334	192.168.1.23	129.173.22.43	TCP	66	57529 → 22 [ACK] Seq=22 Ack=42 Win=131712 Len=0 TSval=851065056 TSecr=2259494126
21	21:41:07.946718	192.168.1.23	129.173.22.43	SSHv2	1458	Client: Key Exchange Init
22	21:41:07.979793	129.173.22.43	192.168.1.23	SSHv2	1146	Server: Key Exchange Init
23	21:41:07.980211	192.168.1.23	129.173.22.43	TCP	66	57529 → 22 [ACK] Seq=1414 Ack=1122 Win=130624 Len=0 TSval=851065091 TSecr=2259494163
24	21:41:08.027627	129.173.22.43	192.168.1.23	TCP	66	22 → 57529 [ACK] Seq=1122 Ack=1414 Win=64128 Len=0 TSval=2259494213 TSecr=851065059
25	21:41:08.027798	192.168.1.23	129.173.22.43	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
26	21:41:08.064650	129.173.22.43	192.168.1.23	TCP	66	22 → 57529 [ACK] Seq=1122 Ack=1462 Win=64128 Len=0 TSval=2259494248 TSecr=851065138
27	21:41:08.067503	129.173.22.43	192.168.1.23	SSHv2	518	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=172)
28	21:41:08.067697	192.168.1.23	129.173.22.43	TCP	66	57529 → 22 [ACK] Seq=1462 Ack=1574 Win=130560 Len=0 TSval=851065177 TSecr=2259494252
29	21:41:08.079955	192.168.1.23	129.173.22.43	SSHv2	82	Client: New Keys
30	21:41:08.202879	129.173.22.43	192.168.1.23	TCP	66	22 → 57529 [ACK] Seq=1574 Ack=1478 Win=64128 Len=0 TSval=2259494345 TSecr=851065189
31	21:41:08.203244	192.168.1.23	129.173.22.43	SSHv2	110	Client: Encrypted packet (len=44)
32	21:41:08.244176	129.173.22.43	192.168.1.23	TCP	66	22 → 57529 [ACK] Seq=1574 Ack=1522 Win=64128 Len=0 TSval=2259494428 TSecr=851065311
33	21:41:08.244185	129.173.22.43	192.168.1.23	SSHv2	110	Server: Encrypted packet (len=44)
34	21:41:08.244383	192.168.1.23	129.173.22.43	TCP	66	57529 → 22 [ACK] Seq=1522 Ack=1618 Win=131008 Len=0 TSval=851065352 TSecr=2259494428
35	21:41:08.244617	192.168.1.23	129.173.22.43	SSHv2	134	Client: Encrypted packet (len=68)
36	21:41:08.308689	129.173.22.43	192.168.1.23	SSHv2	118	Server: Encrypted packet (len=52)
37	21:41:08.308830	192.168.1.23	129.173.22.43	TCP	66	57529 → 22 [ACK] Seq=1590 Ack=1670 Win=131008 Len=0 TSval=851065415 TSecr=2259494479
69	21:41:18.732240	192.168.1.23	129.173.22.43	SSHv2	214	Client: Encrypted packet (len=148)
71	21:41:18.817677	129.173.22.43	192.168.1.23	TCP	66	22 → 57529 [ACK] Seq=1670 Ack=1738 Win=64128 Len=0 TSval=2259505001 TSecr=851075823
90	21:41:19.345410	129.173.22.43	192.168.1.23	SSHv2	94	Server: Encrypted packet (len=28)
91	21:41:19.345704	192.168.1.23	129.173.22.43	TCP	66	57529 → 22 [ACK] Seq=1738 Ack=1698 Win=131008 Len=0 TSval=851076433 TSecr=2259505390
92	21:41:19.346350	192.168.1.23	129.173.22.43	SSHv2	128	Client: Encrypted packet (len=112)
▶ Frame 29: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface en0, id 0						
▶ Ethernet II, Src: Apple_bec8:6c (90:9c:4a:bec8:6c), Dst: Netgear_2f:ee:26 (bc:a5:11:2f:ee:26)						
▶ Internet Protocol Version 4, Src: 192.168.1.23, Dst: 129.173.22.43						
▶ Transmission Control Protocol, Src Port: 57529, Dst Port: 22, Seq: 1462, Ack: 1574, Len: 16						
▼ SSH Protocol						
SSH Version 2 (encryption:chacha20-poly1305@openssh.com mac:<implicit> compression:none)						
Packet Length: 12						
Padding Length: 10						
▼ Key Exchange (method:curve25519-sha256)						
Message Code: New Keys (21)						
Padding String: 000000000000000000000000						
[Direction: client-to-server]						
0040 25 6c 00 00 0c 0a 15 00 00 00 00 00 00 00 %l.....						
SSH Protocol (ssh), 16 bytes						
Packets: 234 · Displayed: 84 (35.9%) · Dropped: 0 (0.0%) · Profile: Default						

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	TCP	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	TCP	66	57529 → 22 [ACK] Seq=2651 Ack=4143 Win=131072 Len=0 TSval=851081881 TSecr=2259511