

Program Manual

To run KeyGen

1. cd to the directory containing KeyGen.java
2. Enter "javac KeyGen.java"
3. Enter "java KeyGen"

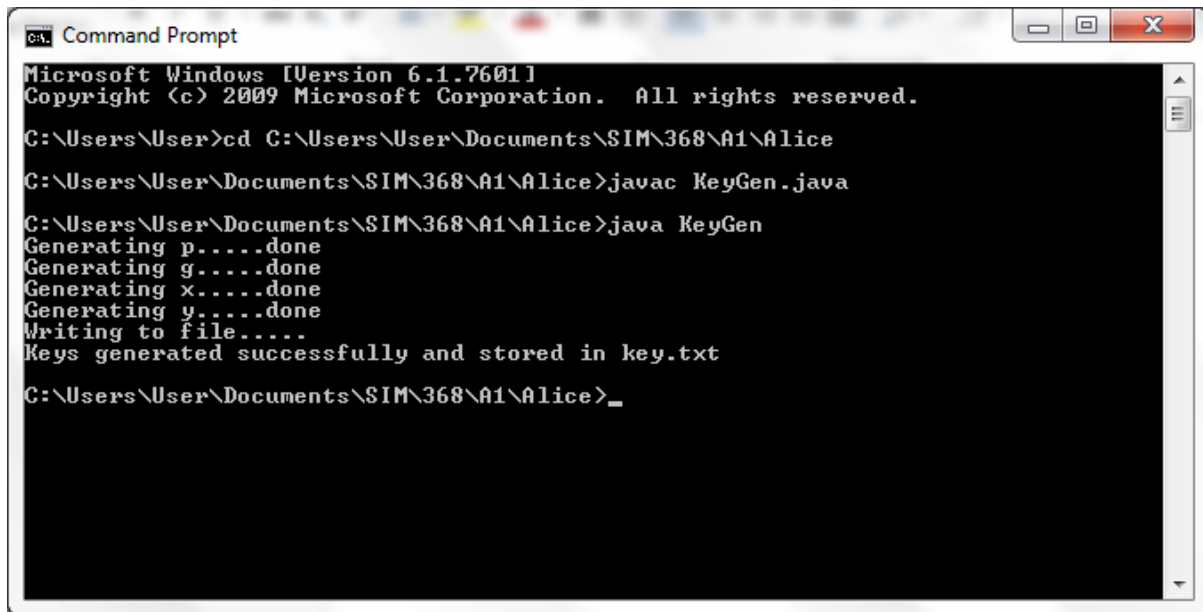
To run Host

1. cd to the directory containing Host.java
2. Enter "javac Host.java"
- 3a To run the with the default name "Alice" and default port 5555
Enter "java Host"
- 3b To run with a specific name
Enter "java Host <name>" eg. "java Host Alicia"
- 3c To run with a specific name and port
Enter "java Host <name> <port>" eg. "java Host Alicia 4444"

To run Client

1. cd to the directory containing Client.java
2. Enter "javac Client.java"
- 3a To run with default name "Bob" default server IP address "127.0.0.1" and default server port 5555
Enter "java Client"
- 3b To run with a specific name
Enter "java Client <clientname>" eg. "java Client Bart"
- 3c To run with a specific name and server IP address
Enter "java Client <clientname> <IP address>" eg. "java Client Bart 192.168.1.5"
- 3d To run with a specific name, IP address and port
Enter "java Client <clientname> <IP address> <port>" eg. "java Client Bart 192.168.1.5 4444"

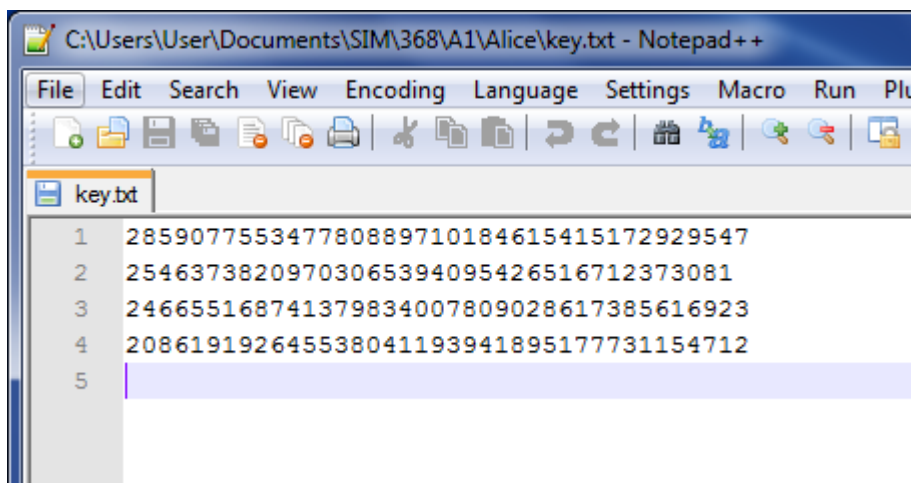
Running KeyGen



```
ca\ Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

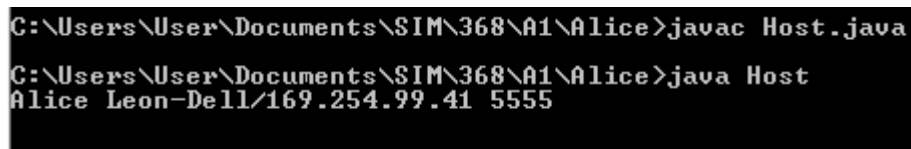
C:\Users\User>cd C:\Users\User\Documents\SIM\368\A1\Alice
C:\Users\User\Documents\SIM\368\A1\Alice>javac KeyGen.java
C:\Users\User\Documents\SIM\368\A1\Alice>java KeyGen
Generating p.....done
Generating g.....done
Generating x.....done
Generating y.....done
Writing to file.....
Keys generated successfully and stored in key.txt
C:\Users\User\Documents\SIM\368\A1\Alice>_
```

Keys generated in key.txt



```
C:\Users\User\Documents\SIM\368\A1\Alice\key.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plu
key.txt
1 285907755347780889710184615415172929547
2 25463738209703065394095426516712373081
3 246655168741379834007809028617385616923
4 208619192645538041193941895177731154712
5
```

Executing Host

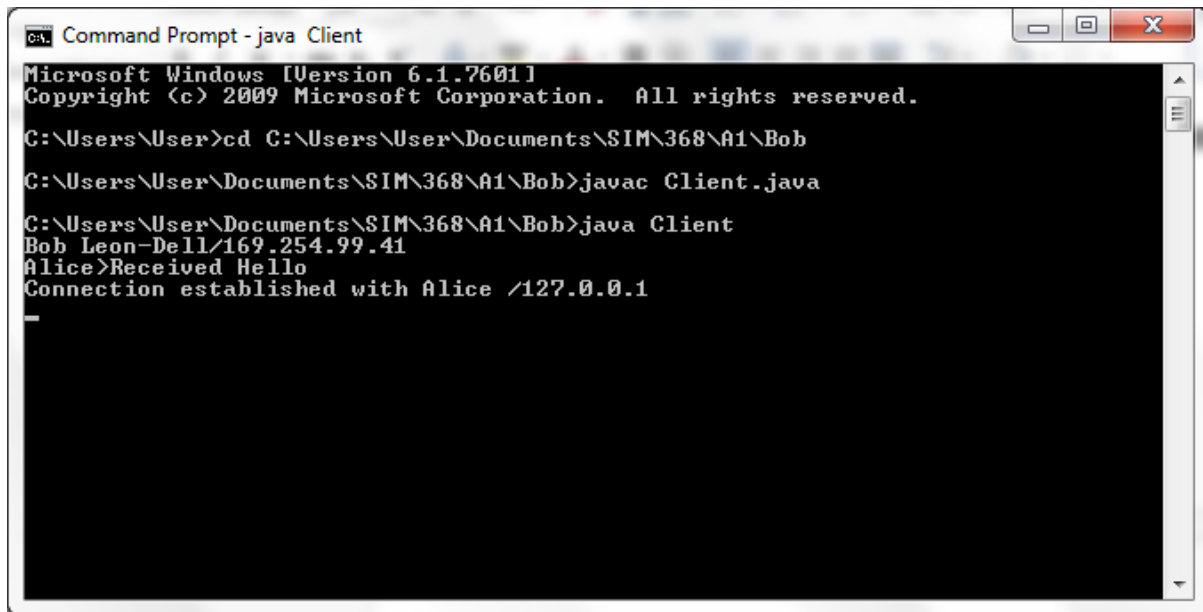


```
C:\Users\User\Documents\SIM\368\A1\Alice>javac Host.java
C:\Users\User\Documents\SIM\368\A1\Alice>java Host
Alice Leon-Dell/169.254.99.41 5555
```

Name of host, IP address of host and port number is shown.

Host is running and listening to the opened port 5555

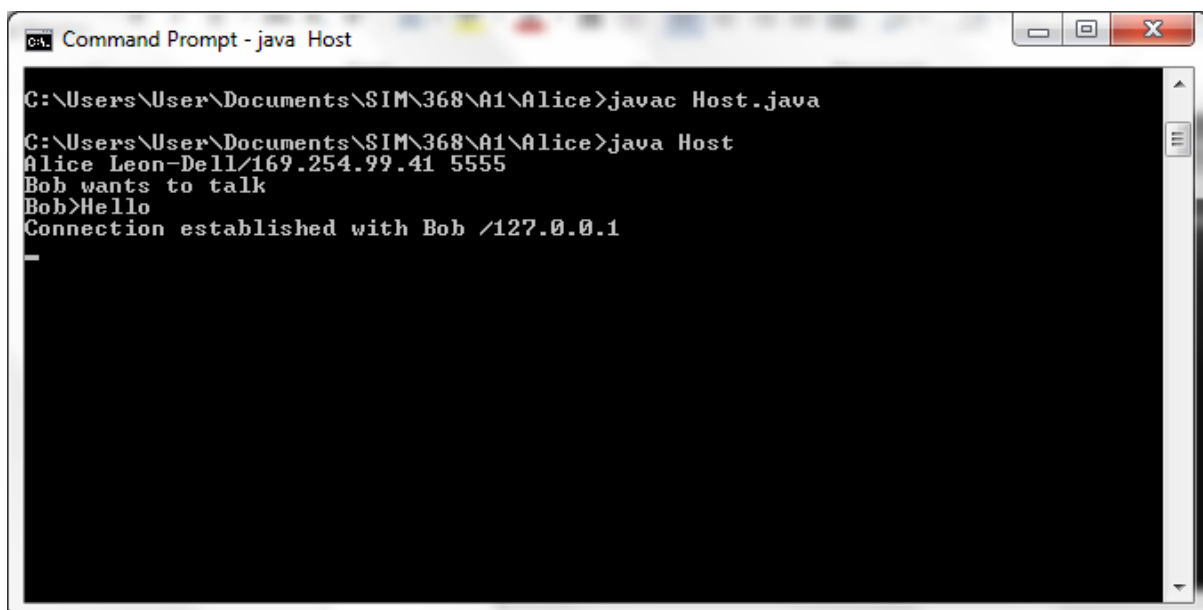
Executing Client



```
Command Prompt - java Client
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User>cd C:\Users\User\Documents\SIM\368\A1\Bob
C:\Users\User\Documents\SIM\368\A1\Bob>javac Client.java
C:\Users\User\Documents\SIM\368\A1\Bob>java Client
Bob Leon-Dell/169.254.99.41
Alice>Received Hello
Connection established with Alice /127.0.0.1
```

At Alice



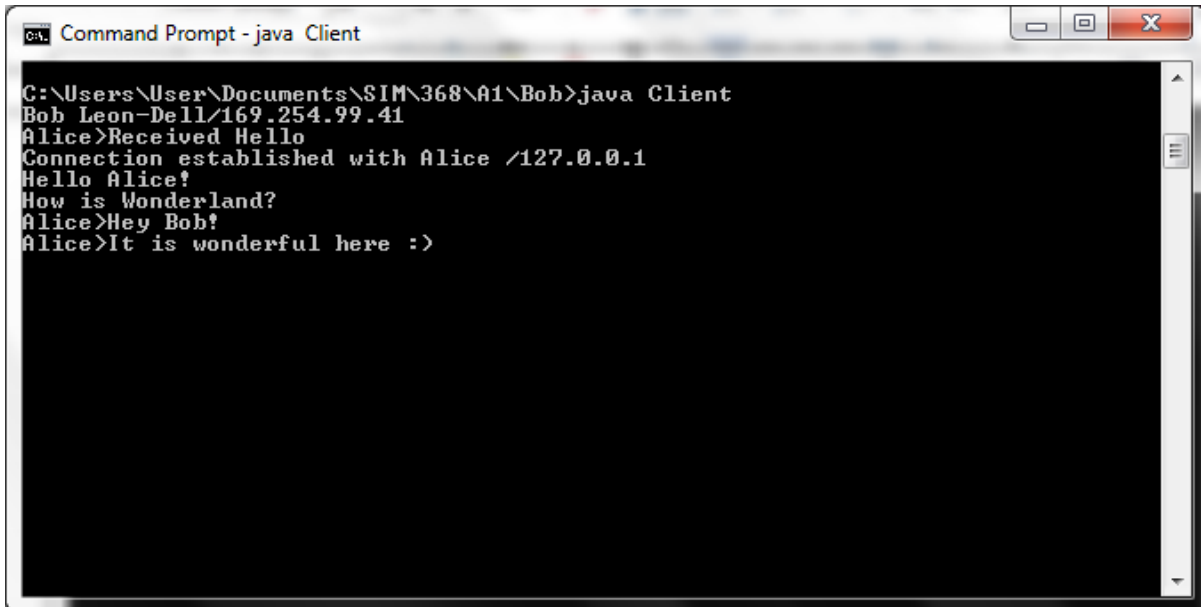
```
Command Prompt - java Host
C:\Users\User\Documents\SIM\368\A1\Alice>javac Host.java
C:\Users\User\Documents\SIM\368\A1\Alice>java Host
Alice Leon-Dell/169.254.99.41 5555
Bob wants to talk
Bob>Hello
Connection established with Bob /127.0.0.1
```

What happens is

1. Bob sends a connection request to Alice
2. Alice then sends her public key to Bob
3. Bob generates an ephemeral Diffie-Hellman key pair based on the parameters from Alice
4. Bob computes the Diffie-Hellman key based on his ephemeral secret key and Alice public key
5. Bob sets the Diffie-Hellman key as the shared RC4 key
6. Encrypts a message "Hello" using the shared key and sends his public key and the message to Alice
7. Alice generates the Diffie-Hellman key using her secret key and Bob's public key
8. Set the Diffie-Hellman key as the shared RC4 key
9. Decrypts the message with the RC4 key and prints the message on the screen

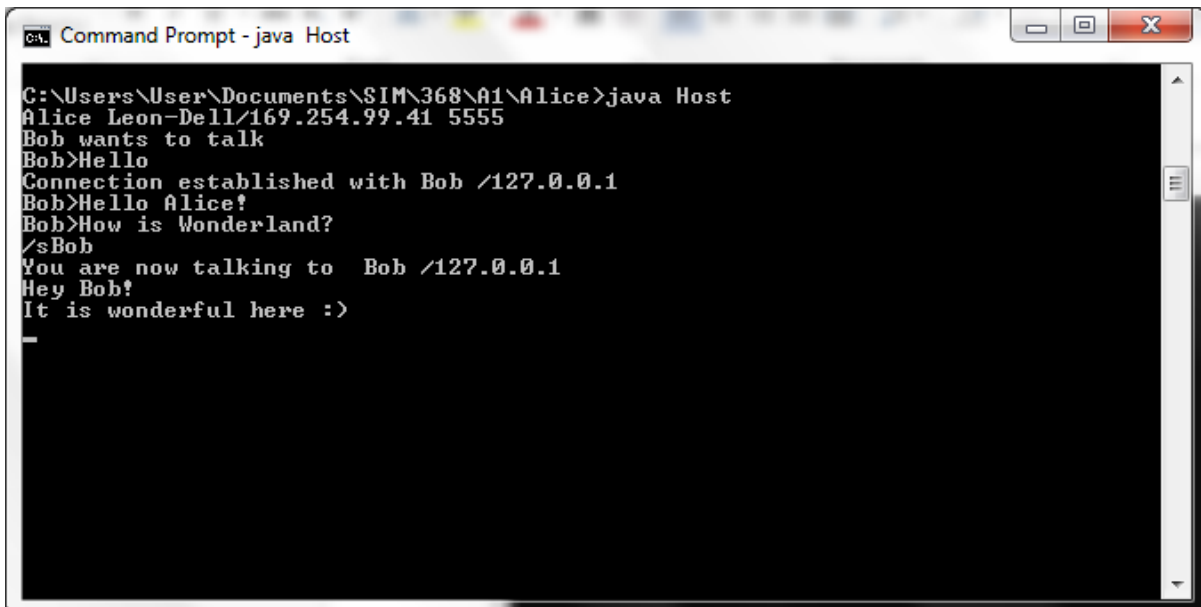
10. Encrypts a message "Received Hello" with the shared key and sends it back to Bob
11. Bob decrypts the message and prints it to the screen
12. Connection is established

Communicating at Bob



```
C:\Users\User\Documents\SIM\368\A1\Bob>java Client
Bob Leon-Dell/169.254.99.41
Alice>Received Hello
Connection established with Alice /127.0.0.1
Hello Alice!
How is Wonderland?
Alice>Hey Bob!
Alice>It is wonderful here :>
```

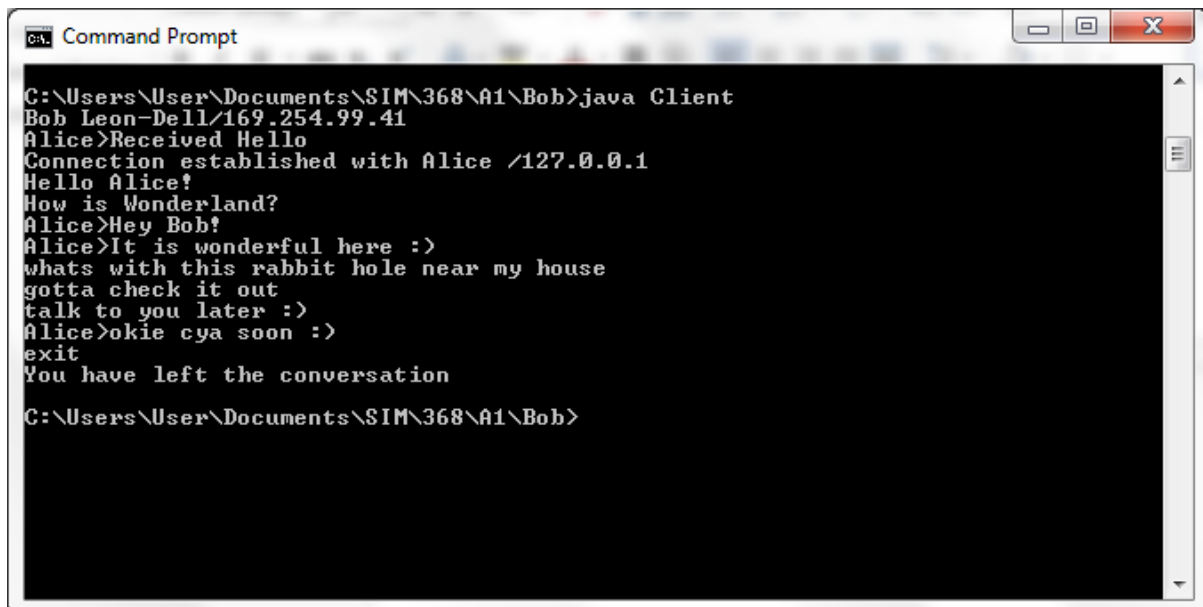
Communicating at Alice



```
C:\Users\User\Documents\SIM\368\A1\Alice>java Host
Alice Leon-Dell/169.254.99.41 5555
Bob wants to talk
Bob>Hello
Connection established with Bob /127.0.0.1
Bob>Hello Alice!
Bob>How is Wonderland?
/sBob
You are now talking to Bob /127.0.0.1
Hey Bob!
It is wonderful here :>
```

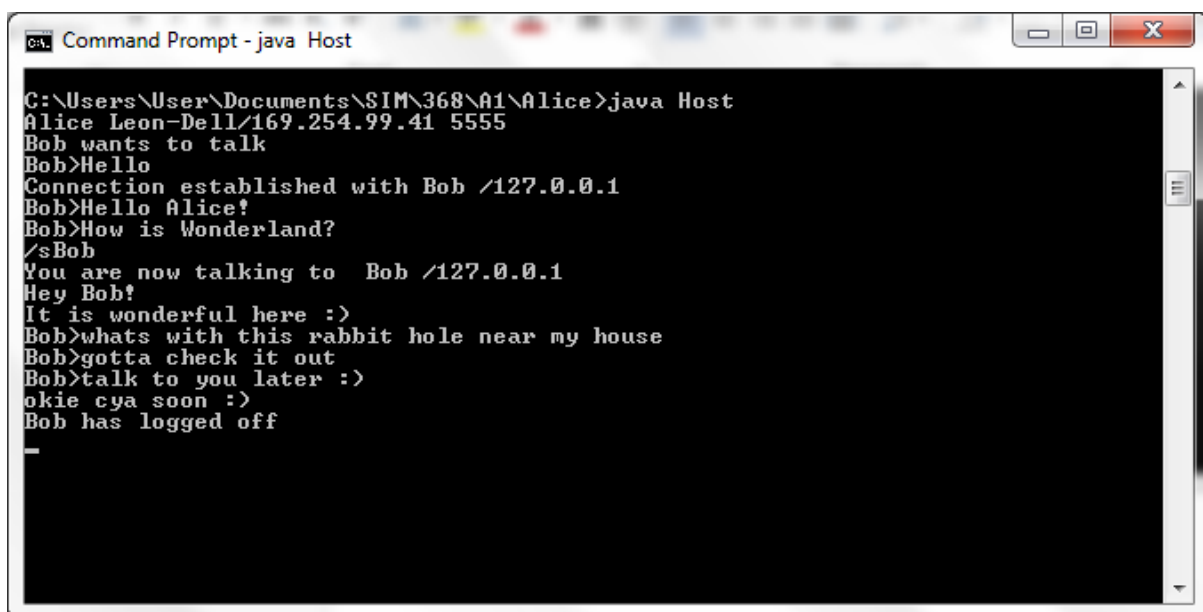
Exiting conversation

Bob types "exit"



```
C:\Users\User\Documents\SIM\368\A1\Bob>java Client
Bob Leon-Dell/169.254.99.41
Alice>Received Hello
Connection established with Alice /127.0.0.1
Hello Alice!
How is Wonderland?
Alice>Hey Bob!
Alice>It is wonderful here :>
whats with this rabbit hole near my house
gotta check it out
talk to you later :>
Alice>okie cya soon :>
exit
You have left the conversation
C:\Users\User\Documents\SIM\368\A1\Bob>
```

At Alice side



```
C:\Users\User\Documents\SIM\368\A1\Alice>java Host
Alice Leon-Dell/169.254.99.41 5555
Bob wants to talk
Bob>Hello
Connection established with Bob /127.0.0.1
Bob>Hello Alice!
Bob>How is Wonderland?
/sBob
You are now talking to Bob /127.0.0.1
Hey Bob!
It is wonderful here :>
Bob>whats with this rabbit hole near my house
Bob>gotta check it out
Bob>talk to you later :>
okie cya soon :>
Bob has logged off
-
```

Server (Alice) options

/s<clientname>

Switch to the client specified

/c<clientname>

Close the connection with a client

/l

List all current sessions

/exit

Closes all sessions and exits program

Client (Bob) options

exit

Disconnects from host and exits the client program

An example of multiple sessions

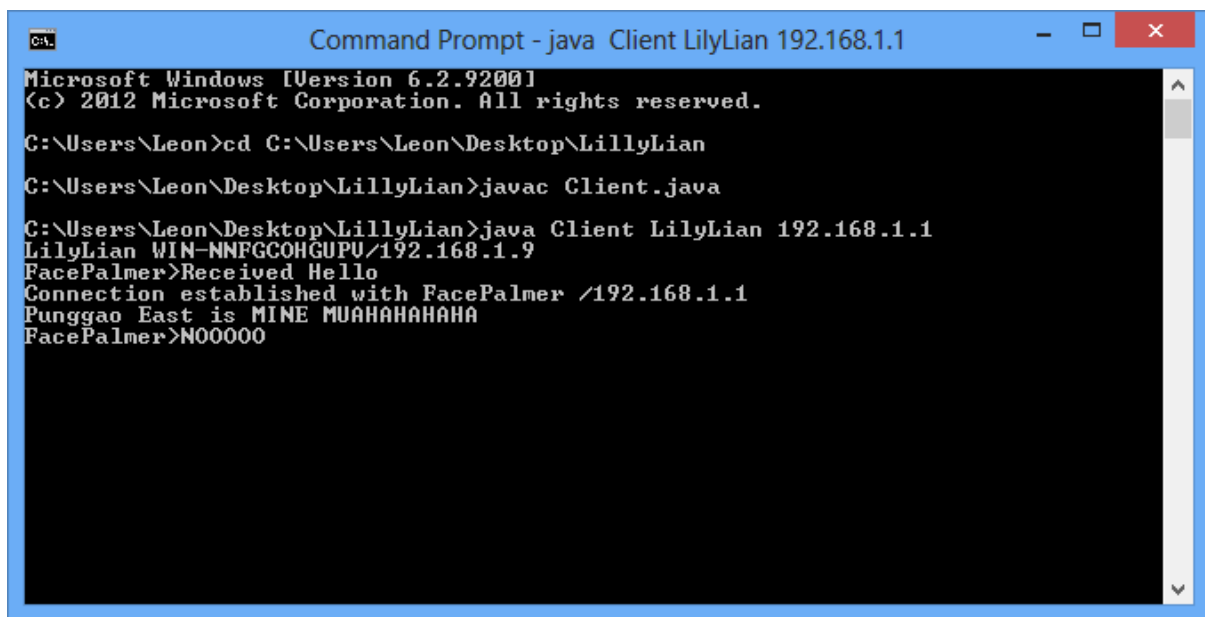
Host: FacePalmer

```
Command Prompt - java Host FacePalmer
C:\Users\User\Documents\SIM\368\A1\Alice>java Host FacePalmer
FacePalmer Leon-Dell/169.254.99.41 5555
Lawra wants to talk
Lawra>Hello
Connection established with Lawra /127.0.0.1
Lawra>Hello darling... I love you loads. More than I sometimes show... Sorry. Love love.
/s Lawra
You are now talking to Lawra /127.0.0.1
Hello Lawra i'm having a message now :)
LilyLian wants to talk
LilyLian>Hello
Connection established with LilyLian /192.168.1.9
LilyLian>Punggao East is MINE MUAHAHAHAHA
/sLilyLian
You are now talking to LilyLian /192.168.1.9
N00000
Lawra>I hope you are having a good message. I have some mangoes for you. I love you and miss you loads
Koh wants to talk
Koh>Hello
Connection established with Koh /192.168.1.10
Koh>Anyone want a collerectal check up?
/sKoh
You are now talking to Koh /192.168.1.10
/sLawra
You are now talking to Lawra /127.0.0.1
Help me...
```

Client: Lawra

```
Command Prompt - java Client Lawra
C:\Users\User\Documents\SIM\368\A1\Bob>java Client Lawra
Lawra Leon-Dell/169.254.99.41
FacePalmer>Received Hello
Connection established with FacePalmer /127.0.0.1
Hello darling... I love you loads. More than I sometimes show... Sorry. Love love.
FacePalmer>Hello Lawra i'm having a message now :)
I hope you are having a good message. I have some mangoes for you. I love you and miss you loads
FacePalmer>Help me...
```

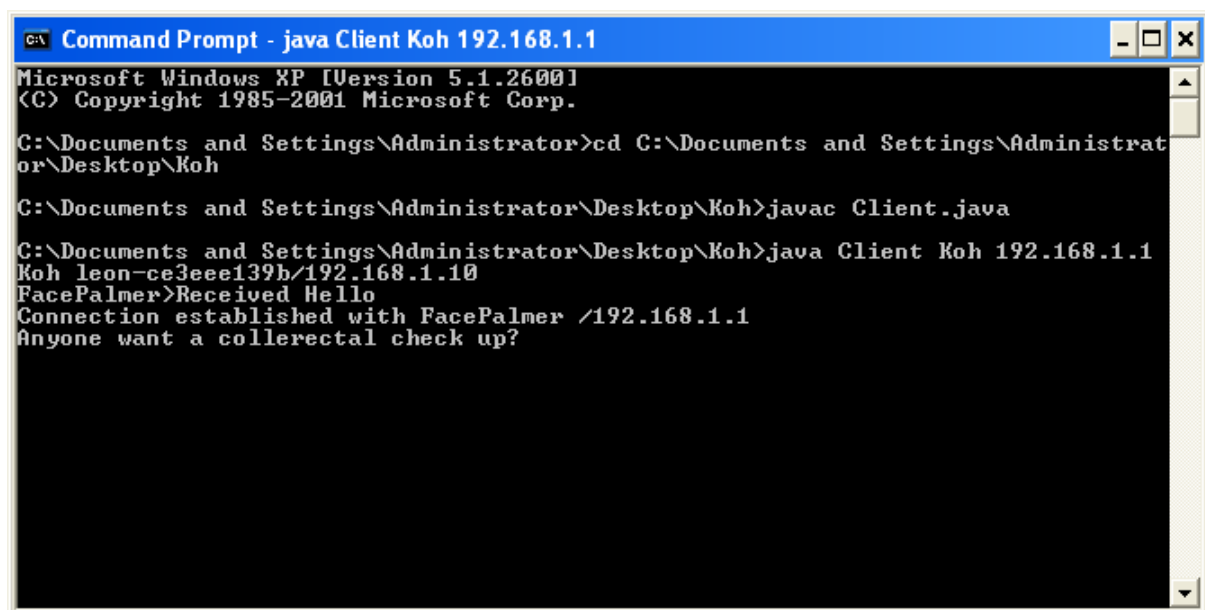
Client: LilyLian



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Leon>cd C:\Users\Leon\Desktop\LillyLian
C:\Users\Leon\Desktop\LillyLian>javac Client.java
C:\Users\Leon\Desktop\LillyLian>java Client LilyLian 192.168.1.1
LilyLian WIN-NNFGCOHGUPU/192.168.1.9
FacePalmer>Received Hello
Connection established with FacePalmer /192.168.1.1
Punggao East is MINE MUAHAHAHAHA
FacePalmer>N000000
```

Client: Koh



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd C:\Documents and Settings\Administrat
or\Desktop\Koh
C:\Documents and Settings\Administrator\Desktop\Koh>javac Client.java
C:\Documents and Settings\Administrator\Desktop\Koh>java Client Koh 192.168.1.1
Koh leon-ce3eee139b/192.168.1.10
FacePalmer>Received Hello
Connection established with FacePalmer /192.168.1.1
Anyone want a collerectal check up?
```


Additional Features

- ✓ Full-duplex communication
- ✓ Host can handle multiple clients