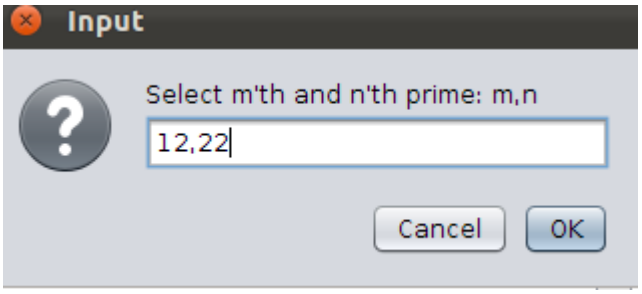
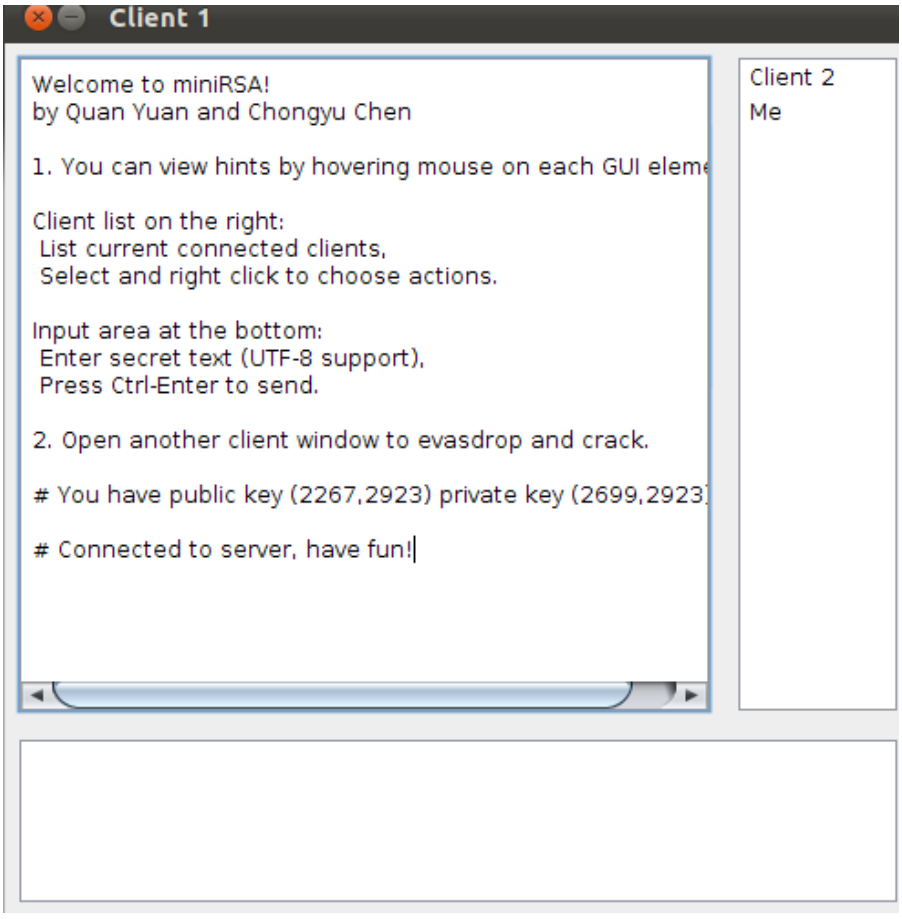
RSA Chat Assignment—By Chongyu Chen and Quan Yuan

URL for code repository:
https://github.com/mikeccy/miniRSA

Program is written in Java with GUI for interaction.
1. Run “make” to compile all files.
2. Start server first with “make run”
3. Start client with “make run_client”
4. When client starts, first enter m’th and n’th prime number to generate public and private keys for client.



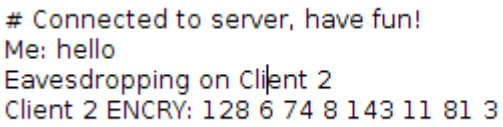
5. For example, now two clients are connected to server, GUI is like this (program supports multiple clients):



6. You can view hints by hovering mouse on each GUI element.
   Client list on the right:
   List current connected clients,
   Select and right click to choose actions.

   Input area at the bottom:
   Enter secret text (UTF-8 support),
   Press Ctrl-Enter to send.

7. Open another client window to eavesdrop and crack.
8. If eavesdrop is enabled by client 1, client 1 can see the encrypted message between client 2 and server.



9.If cracked is enabled by client 1, client 1 can know client 2's private key and decrypted message between client 2 and server.