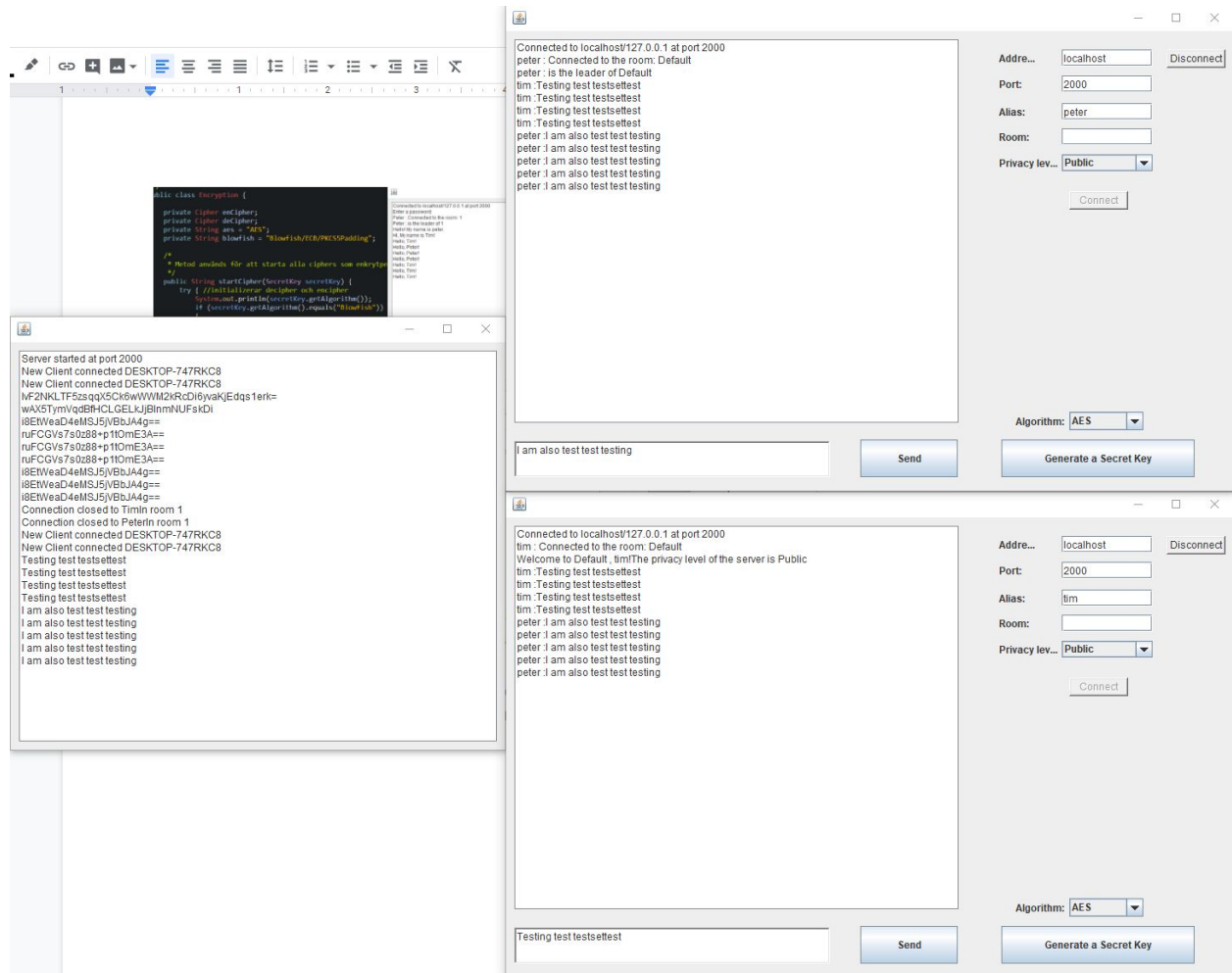


1:1

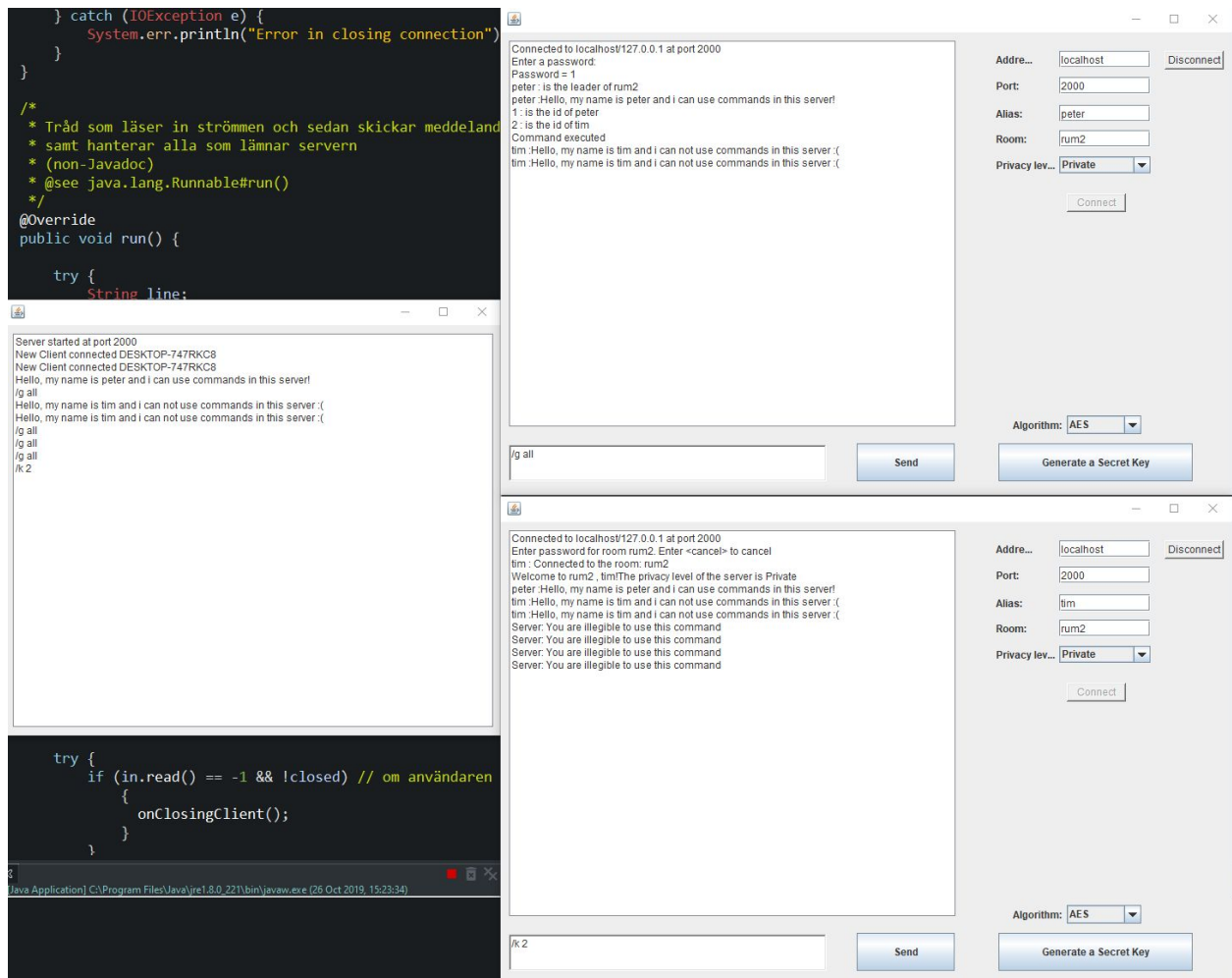
Exempel på krypterade meddelanden igenom servern.

Klienterna krypterar och dekrypterar, servern skickar endast igenom meddelanden. Server till vänster som endast visar vad klienterna skickat och två olika klienter till höger som tar in text i genom sockar och strömmar



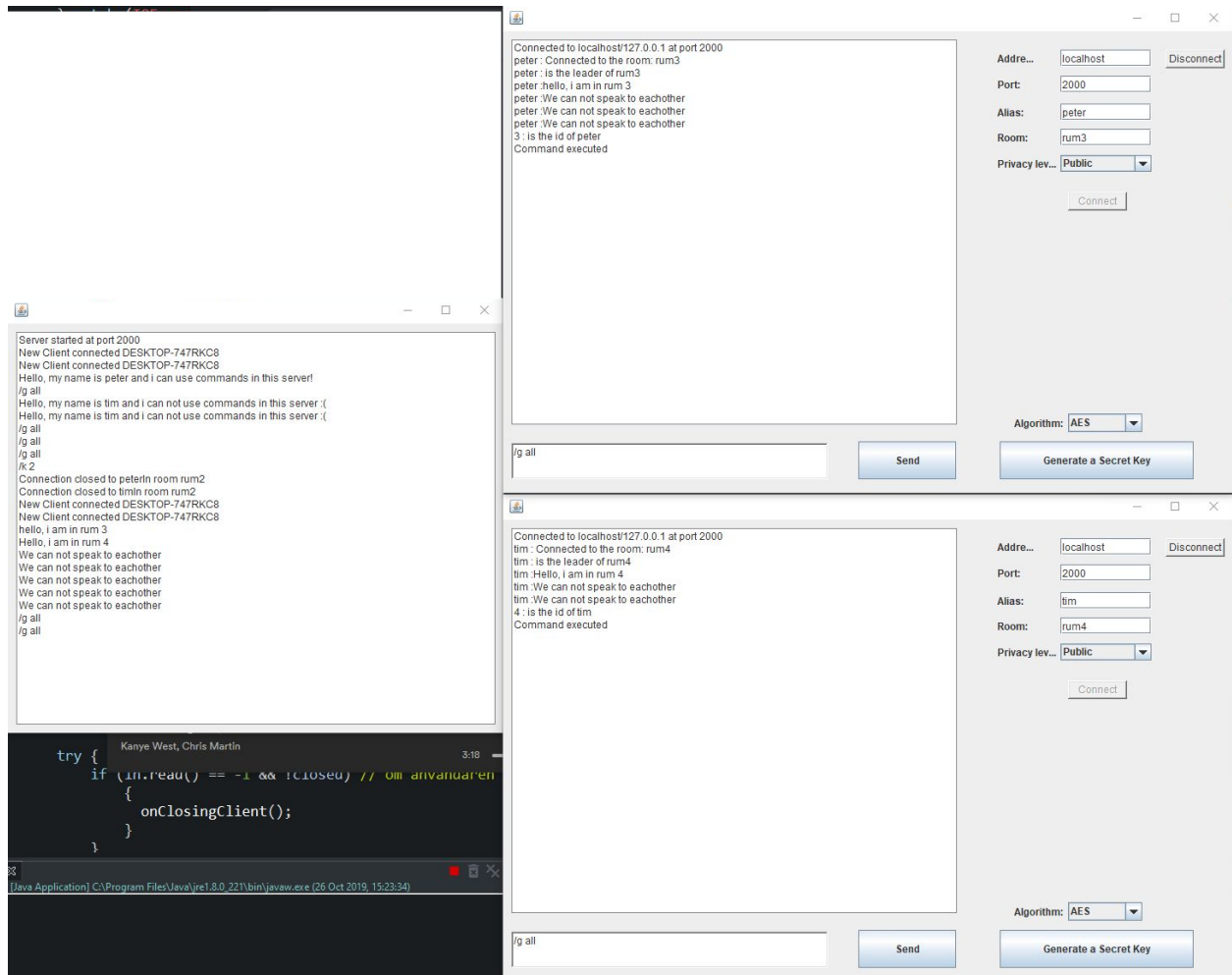
1:2

Exempel på chat genom en vanlig publik kanal där alias och meddelande visas på varje klient. Server till vänster klienter till höger. Ingen kryptering används på publika servrar.



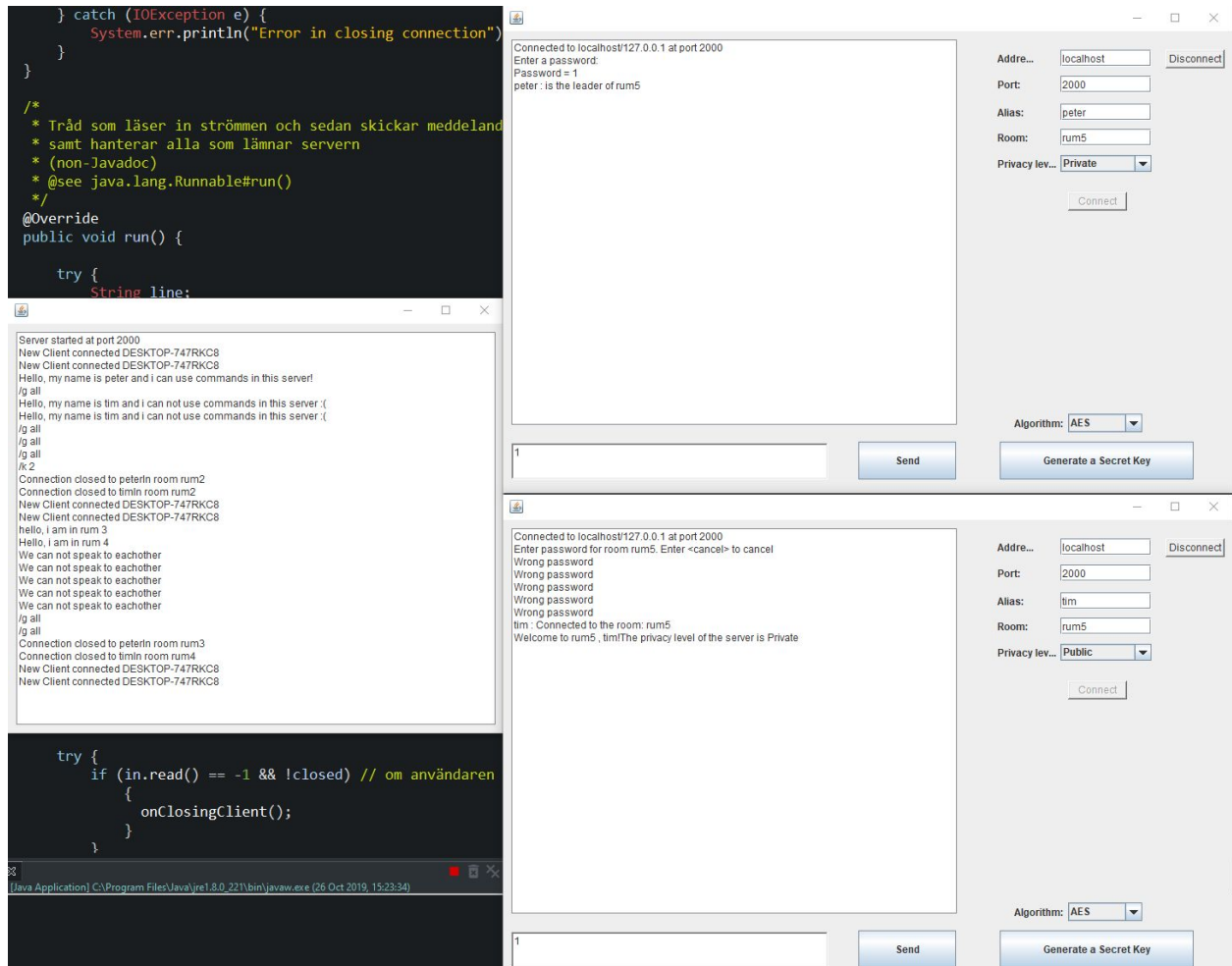
1:3

Exempel på privat server som behöver lösenord och inte använder kryptering där ledaren kan använda kommandon som /g all där man hämtar id på alla i servern och exempel på icke-ledare som inte har tillåtelse till kommandon.



1:4

Exempel på olika rum, där personer som är i olika rum inte kan se vad som händer i andra rum samt att det finns en ledare i varje rum.



1:5

Exempel på privat rum med lösenord där klienten som försökte ansluta skrev in fel lösenord och inte lyckas ansluta till servern förrän rätt lösenord anges.

Funktioner och användning

- Funktioner i klient/server-program (IRC-chat):
- Oändligt antal användare.
- Oändligt antal rum.
- Alias för användare, ej unika, då ID används på användare för att kunna göra kommand på.
- Krypterade rum, där användare skickar igenom krypterade meddelanden.
- Publika rum, där det inte finns lösenord eller krypterade meddelanden.
- Privata rum, där man behöver lösenord för att ansluta.
- Generera nyckel knapp(AES eller Blowfish)
- Avsluta anslutning knapp som stänger av anslutning till server.
- Anslutning till specifik address och port

Krypteringsnyckel anges när "Secret" väljs i comboboxen och man kan välja en AES eller Blowfish nyckel, programmet känner igen vilken man lägger in.

Misslyckas den så skrivs det i listan.

Kommandon

- Kick
- Get id
- Pass lead

Server som kan hantera allting genom att skicka till rätt anslutna klienter

Det enda som klienterna gör är att skicka meddelanden och ta emot meddelanden samt kryptera och dekryptera meddelanden.

Servern håller koll på allting annat som vilket rum klienten är i, ID på klienten, klassificering på klienten.

Server kan startas med cmd med IRCServer <port>. anges ingen port är standardport = 2000

Hur man använder appen:

Server:

Starta IRCServer och ange port om det önskas, alternativt öppnas den i port 2000. Inget annat behövs göras.

Klient:

Starta IRCClient och ange rum och alias, anges inget blir namn automatiskt "Anonymous" och rum "Default"

Välj privacy i boxen, väljs private måste lösenord anges på servern, publik så händer inget speciellt.

Secret så måste krypteringsnyckel anges i filechoosarfönstret.

Klicka sedan på connect och man ansluts till servern och valda rummet.

Servern måste vara igång för att man ska kunna ansluta annars anges det att anslutningen misslyckades. För att sedan kunna ansluta igen måste man klicka på disconnect knappen för att connect knappen ska fungera igen.

Disconnect stänger socketen och anslutningen till servern samt att man behöver klicka på connect igen för att ansluta.

Reflektioner

Jag tycker att jag hade kunnat skicka objekt igenom klienten och sen titta i servern vad jag fick genom att använda instanceof eller readObject och sen specificera objekt och hantera exceptions om det inte är rätt inkommande. Jag försökte så gott jag kunde att fokusera på att allting skulle vara på serversidan och så lite som möjligt på klientsidan för att göra

en lätt klient, men jag tror att jag gick fel väg när jag valde att ha en lista på varje klient inom varje klient. Detta kan leda till att servern går sakta när större mängder klienter kommer in i servern. Jag tänkte senare att jag möjligtvis kunde skapa en server för varje rum, men med tanke på det begränsade antal portar så kanske det sätter jag gjorde på fungerar bättre.

Jag testade aldrig att ha ett större antal klienter anslutna till servern, men är ganska säker på att den inte skulle klara tusentals klienter då jag tvivlar på att den skulle lyckas ta emot alla samtidigt.

Jag tror att jag hanterade det på ett relativt bra sätt, men självklart att saker kunde gjorts bättre och det ska jag tänka på tills nästa gång jag försöker på mig någonting liknande.

André Normann
2019-11-01