CS 6349 Network Security

Implementation of a Real-Time e-commerce Broker System

Overview:

This project is an implementation an e-Commerce broker system which will facilitate anonymous online purchase process between a Client and an e-Commerce Website. Done by Yinglue Chen, Venkata Sai Rohith Kilambi, Sampath Grandhi for Network Security CS6349.001 Fall 18 by Prof. Kamil Sarac.

Features:

- Authentication
- Message Integrity verification
- Privacy/Confidentiality
- Anonymity
- Non-repudiation

Language used: Java

- The broker runs at 5000 port.
- The Server runs at 6000 port.
- The Server2 runs at 1234 port.

Packages used:

- javax.crypto, java.security for the cryptographic techniques(encryption and decryption)
- java.net for the socket.

Files:

1. GenerateKeys.java

This is used for generating the public-private key pair. The lengths of the keys for client, broker, and seller are 3072 bits, 1024 bits, and 2048 bits respectively. This file should be executed first to generate keys for each of the components.

2. InputPort.java

This file is for the broker. When executing this file, a CSV file containing the information about the sellers and ports will be automatically generated, which will be used later for the communication between broker and seller.

3. InputUserPwd.java

This file is for the broker. When executing this file, a CSV file containing the information about the usernames and the hash values of the users' passwords will be automatically generated, which will be used later for the verification when the client logs in to the broker.

4. Broker.java

Executing this file, the broker system will start. During the process, the broker will keep listening until one client tries to log in. Once the client inputs a valid seller name, the broker will connect to the corresponding seller, and then the purchase can be performed.

5. Client.java

Executing this file, the client system will start. During the process, the client connects to the broker by logging into the broker system. Once logged in, the client must input a valid seller name. Once entered, the broker will connect to the corresponding seller. Then the client and seller can communicate with each other, where the broker cannot decrypt messages sent between client and seller and the seller doesn't know who the client is. The client shall send a request to the broker asking the seller to send the product catalog After receiving the product list, the client can select the product ID, the product is sent to the client via the broker and is downloaded into the client's system.

6. Server.java

Executing this file, the server system will start. During the process, the server will keep listening for requests from the broker. The server verifies the broker and sends the product list to be served to the client. Upon receiving a request containing the product ID (after the broker completes the transaction) the seller delivers the product to the client. Server2.java is also implemented in the same manner.

Instructions:

1. First, run the following files. Change the path for the output files.

- GenerateKeys.java (change the key length and the file names to suit the client, broker, and seller)
- InputPort.java
- InputUserPwd.java

2. Run Server.java, Server2.java. Change the path for public key and private key files.

3. Run Broker.java. Change the path for public key and private key files.

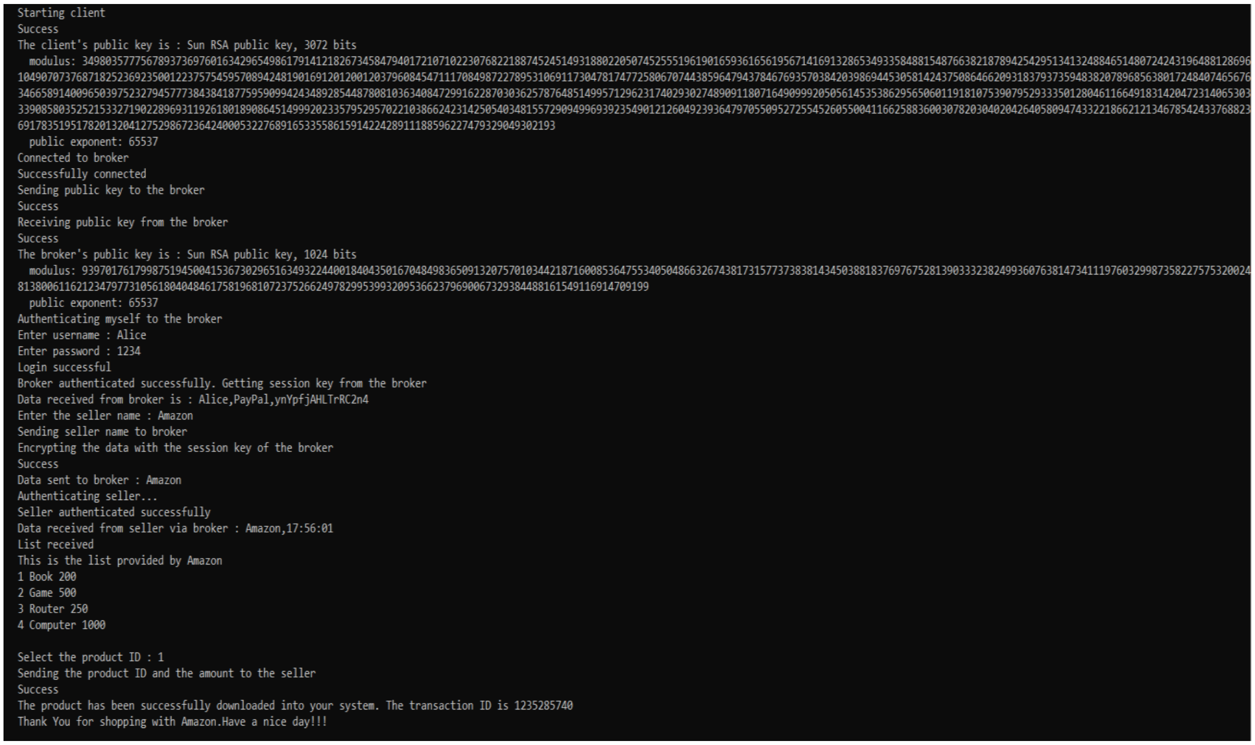
4. Run Client.java. Change the path for public key and private key files.

Working Scenario:

1. Client enters username as “Alice”, Password as “1234”
2. Client inputs the server as Amazon and hits Enter which then sends a request for the product catalog.
3. Upon receiving a product catalog, the client selects a product ID and sends it to the broker for the transaction.
4. After successful completion of the transaction, the product is delivered by the server and received by the client.

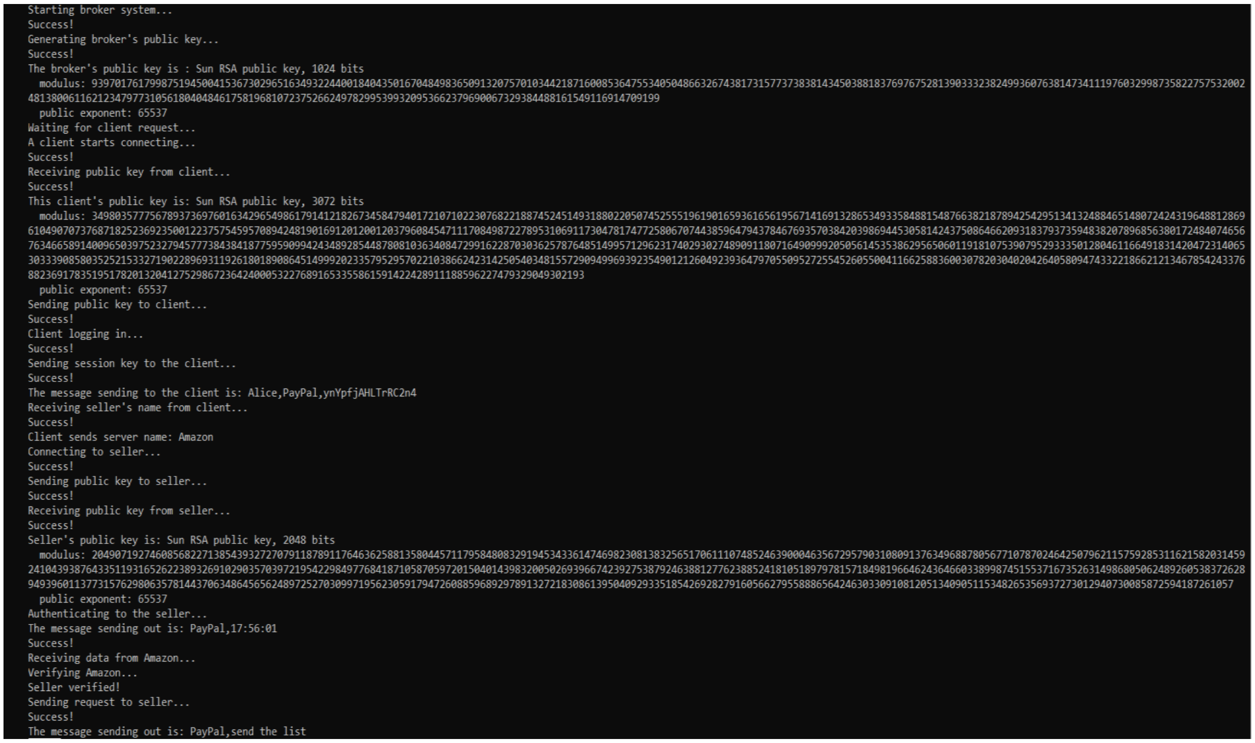
Screenshots:

1. Sample output log from the client after successful completion of a transaction.



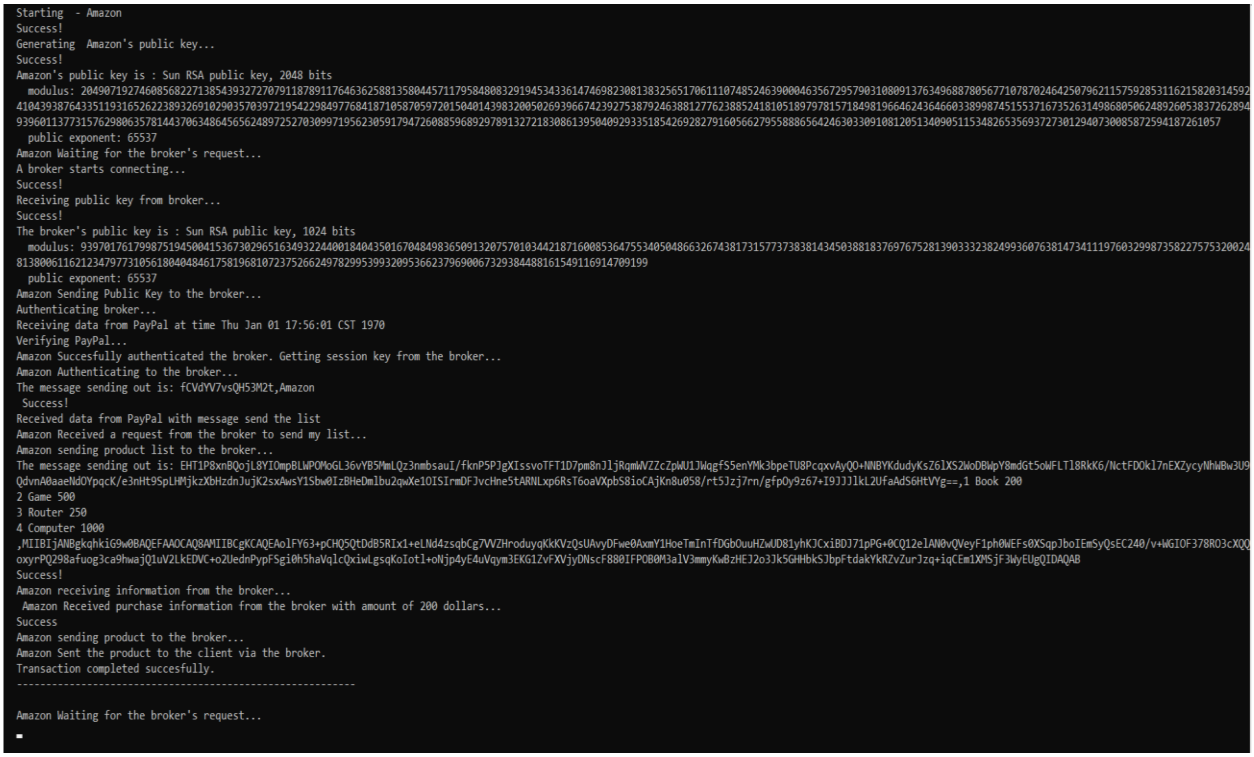
```
Starting client
Success
The client's public key is : Sun RSA public key, 3072 bits
  modulus: 34980357775678937369760163429654986179141218267345847940172107102230768221887452451493188022050745255519619016593616561956714169132865349335848815487663821878942542951341324884651480724243196488128696
10490707376871825236923500122375754595708942481901691201200120379608454711170849872278953106911730478174772580670744385964794378467693570384203986944530581424375086466209318379373594838207896856380172484074656 76
34665891400965039752327945777384384187759590994243489285448780810363408472991622870303625787648514995712962317402930274890911807164909992050561453538629565060119181075390795293335012804611664918314204723140653 03
33908580352521533271902289693119261801890864514999202335795295702210386624231425054034815572909499693923549012126049239364797055095272554526055004116625883600307820304020426405809474332218662121346785424337688 23
69178351951782013204127529867236424000532276891653355861591422428911188596227479329049302193
  public exponent: 65537
Connected to broker
Successfully connected
Sending public key to the broker
Success
Receiving public key from the broker
Success
The broker's public key is : Sun RSA public key, 1024 bits
  modulus: 93970176179987519450041536730296516349322440018404350167048498365091320757010344218716008536475534050486632674381731577373838143450388183769767528139033323824993607638147341119760329987358227575320024
813800611621234797731056180404846175819681072375266249782995399320953662379690067329384488161549116914709199
  public exponent: 65537
Authenticating myself to the broker
Enter username : Alice
Enter password : 1234
Login successful
Broker authenticated successfully. Getting session key from the broker
Data received from broker is : Alice,PayPal,ynYpfjAHLTrRC2n4
Enter the seller name : Amazon
Sending seller name to broker
Encrypting the data with the session key of the broker
Success
Data sent to broker : Amazon
Authenticating seller...
Seller authenticated successfully
Data received from seller via broker : Amazon,17:56:01
List received
This is the list provided by Amazon
1 Book 200
2 Game 500
3 Router 250
4 Computer 1000

Select the product ID : 1
Sending the product ID and the amount to the seller
Success
The product has been successfully downloaded into your system. The transaction ID is 1235285740
Thank You for shopping with Amazon.Have a nice day!!!
```

2. Sample output log from the broker after successful completion of a transaction.



```
Starting broker system...
Success!
Generating broker's public key...
Success!
The broker's public key is : Sun RSA public key, 1024 bits
  modulus: 93970176179987519450041536730296516349322440018404350167048498365091320757010344218716008536475534050486632674381731577373838143450388183769767528139033323824993607638147341119760329987358227575320002
4813800611621234797731056180404846175819681072375266249782995399320953662379690067329384488161549116914709199
  public exponent: 65537
Waiting for client request...
A client starts connecting...
Success!
Receiving public key from client...
Success!
This client's public key is: Sun RSA public key, 3072 bits
  modulus: 3498035777567893736976016342965498617914121826734584794017210710223076822188745245149318802205074525551961901659361656195671416913286534933584881548766382187894254295134132488465148072424319648812869
6104907073768718252369235001223757545957089424819016912012001203796084547111708498722789531069117304781747725806707443859647943784676935703842039869445305814243750864662093183793735948382078968563801724840746 56
7634665891400965039752327945777384384187759590994243489285448780810363408472991622870303625787648514995712962317402930274890911807164909992050561453538629565060119181075390795293335012804611664918314204723140 65
30333908580352521533271902289693119261801890864514999202335795295702210386624231425054034815572909499693923549012126049239364797055095272554526055004116625883600307820304020426405809474332218662121346785424337 6
88236917835195178201320412752986723642400053227689165335586159142242891118859622747932904930219 3
  public exponent: 65537
Sending public key to client...
Success!
Client logging in...
Success!
Sending session key to the client...
Success!
The message sending to the client is: Alice,PayPal,ynYpfjAHLTrRC2n4
Receiving seller's name from client...
Success!
Client sends server name: Amazon
Connecting to seller...
Success!
Sending public key to seller...
Success!
Receiving public key from seller...
Success!
Seller's public key is: Sun RSA public key, 2048 bits
  modulus: 2049071927460856822713854393272707911878911764636258813580445711795848083291945343361474698230813832565170611107485246390004635672957903108091376349688780567710787024642507962115759285311621582031459
2410439387643351193165262238932691029035703972195422984977684187105870597201504014398320050269396674239275387924638812776238852418105189797815718498196646243646603389987451553716735263149868050624892605383726 28
9493960113773157629806357814437063486456562489725270309971956230591794726088596892978913272183086139504092933518542692827916056627955888656424630330910812051340905115348265356937273012940730085872594187261057
  public exponent: 65537
Authenticating to the seller...
The message sending out is: PayPal,17:56:01
Success!
Receiving data from Amazon...
Verifying Amazon...
Seller verified!
Sending request to seller...
Success!
The message sending out is: PayPal,send the list
```

3. Sample output log from the server after successful completion of a transaction.



```
Starting  - Amazon
Success!
Generating  Amazon's public key...
Success!
Amazon's public key is : Sun RSA public key, 2048 bits
  modulus: 20490719274608568227138543932727079118789117646362588135804457117958480832919453433614746982308138325651706111074852463900046356729579031080913763496887805677107870246425079621157592853116215820314592
4104393876433511931652622389326910290357039721954229849776841871058705972015040143983200502693966742392753879246388127762388524181051897978157184981966462436466033899874515537167352631498680506248926053837262894
93960113773157629806357814437063486456562489725270309971956230591794726088596892978913272183086139504092933518542692827916056627955888656424630330910812051340905115348265356937273012940730085872594187261057
  public exponent: 65537
Amazon Waiting for the broker's request...
A broker starts connecting...
Success!
Receiving public key from broker...
Success!
The broker's public key is : Sun RSA public key, 1024 bits
  modulus: 93970176179987519450041536730296516349322440018404350167048498365091320757010344218716008536475534050486632674381731577373838143450388183769767528139033323824993607638147341119760329987358227575320024
813800611621234797731056180404846175819681072375266249782995399320953662379690067329384488161549116914709199
  public exponent: 65537
Amazon Sending Public Key to the broker...
Authenticating broker...
Receiving data from PayPal at time Thu Jan 01 17:56:01 CST 1970
Verifying PayPal...
Amazon Succesfully authenticated the broker. Getting session key from the broker...
Amazon Authenticating to the broker...
The message sending out is: fCVdYV7vsQH53M2t,Amazon
 Success!
Received data from PayPal with message send the list
Amazon Received a request from the broker to send my list...
Amazon sending product list to the broker...
The message sending out is: EHT1P8xnBQojL8YIOmpBLWPOMoGL36vYB5MmLQz3nmbsauI/fknP5PJgXIssvoTFT1D7pm8nJljRqmWVZZcZpWU1JWqgfS5enYMk3bpeTU8PcqxvAyQO+NNBYKdudyKsZ6lXS2WoDBWpY8mdGt5oWFLTl8RkK6/NctFDOkl7nEXZycyNhWBw3U9
QdvnA0aaeNdOYpqcK/e3nHt9SpLHMjkzXbHzdnJujK2sxAwsY1Sbw0IzBHeDmlbu2qwXe1OISIrmDFJvcHne5tARNLxp6RsT6oaVXpbS8ioCAjKn8u058/rt5Jzj7rn/gfpOy9z67+I9JJJlkL2UfaAdS6HtVYg==,1 Book 200
2 Game 500
3 Router 250
4 Computer 1000
,MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAolFY63+pCHQ5QtDdB5RIx1+eLNd4zsqbCg7VVZHroduyqKkKVzQsUAvyDFwe0AxmY1HoeTmInTfDGbOuuHZwUD81yhKJCxiBDJ71pPG+0CQ12elAN0vQVeyF1ph0WEFs0XSqpJboIEmSyQsEC240/v+WGIOF378RO3cXQQ
oxyrPQ298afuog3ca9hwajQ1uV2LkEDVC+o2UednPypFSgi0h5haVqlcQxiwLgsqKoIotl+oNjp4yE4uVqym3EKG1ZvFXVjyDNscF880IFPOB0M3alV3mmyKwBzHEJ2o3Jk5GHHbkSJbpFtdakYkRZvZurJzq+iqCEm1XMSjF3WyEUgQIDAQAB
Success!
Amazon receiving information from the broker...
 Amazon Received purchase information from the broker with amount of 200 dollars...
Success
Amazon sending product to the broker...
Amazon Sent the product to the client via the broker.
Transaction completed succesfully.
----------------------------------------------------------

Amazon Waiting for the broker's request...
```