LZSCC.311 Coursework Stage 2 Specification

Due: Tuesday Week 7 via Moodle

Marking: Week 7

Total mark allocation: 45%

You are asked to implement a distributed auctioning system using Java RMI. This auctioning system should consist of a central auctioning server and two separate client programs.

Level 3: Advanced Auction Logic (10%)

This system will empower users with the option to choose different auction styles based on their preferences and product characteristics. Please implement two advanced auction logic:

- **Reverse auction**: This type allows a buyer to browse the same auction items sold by different sellers. A sensible buyer will choose the lowest price among the various sellers.
- **Double auction**: In this model, multiple buyers and sellers enter an auction simultaneously. The auction server will settle the auction by matching the bidding and selling prices. Double auction should ensure that the matched buyer enables the seller to achieve the maximum profit, represented by the difference between the bidding and selling price.

The auction server should be able to host different auction styles chosen by the user, namely forward auction (in Stage 1), reverse auction, and double auction. To test the forward and reverse auctions, it is necessary to have at least three buyers and sellers, respectively. For the double auction testing, ensure a minimum number of three buyers and three sellers participating simultaneously.

Level 4: Access Control (10%)

The system implementation so far is insecure; it has no mechanism to mitigate the following cases:

- tampering with bids (one buyer modifying or stopping another buyer's bid),

- closing the bidding by a user who did not create the auction,
- accepting a bid that is the same or lower than the current bid.

Implement logic to ensure the right level of access for different users to protect against the above attacks. Depending on how you designed your system, you might need to add functionality to register user accounts.

Level 5: Digital Signature in Auction System (8%)

To provide security and trust within the auction system, you are required to implement a suitable digital signature. This implementation aims to verify the integrity and origin of the auction transactions by utilising the Java *"java.security.Signature"* class to introduce digital signature functionality within the auction server.

Create a mechanism enabling the client to verify the server's identity by using its digital signature. To test the result of verification, print both the received hash digest and the hash digest of the original message.

You can assume that registered users already have access to their associated keys. For example, user IDs and pre-generated keys can be loaded from a file on disk. Additionally, the auction server can self-sign the certificate.

Mark Scheme

Level 3

Reverse auction — 5 marks
Double auction — 5 marks

Level 4

Test case 1 — 5 marks
Test case 2 — 5 marks

Level 5

Auction server creates digital signature — 4 marks
User verify digital signature — 4 marks