Project Overview

Design and develop a peer-to-peer privacy-preserving auction system using applied cryptography. Your solution must address all security requirements below, with detailed justification of how the chosen cryptographic mechanisms provide the required properties. You may develop a user interface of your choice.

System Operation

Auction Announcements
When a user initiates an auction, the announcement must reach all system users without revealing the seller's identity. The announcement contains only:

- Item description
- Auction closing date
- Optional minimum bid value

Bidding Process
All users can submit public bids while maintaining bidder anonymity from all participants, including the seller. Bids are distributed to all users for verification and contain only:

- Item identification
- Bid value

Winner Revelation
At auction conclusion, only the seller and the winning bidder can access each other's identities. All other bidders remain anonymous, even to the seller.

Security Requirements

Your system must guarantee:

- **Anonymity**: Seller and bidder identities remain confidential throughout the auction process
- **Authenticity**: Verification that bids originate from legitimate system participants
- **Integrity**: Protection against bid tampering or modification
- **Non-repudiation**: Winning bidders cannot deny their bids
- **Trusted timestamping**: Verifiable timestamps to resolve ties (earliest bid wins)
- **Selective identity disclosure**: Mutual identity revelation between seller and winner only

Architecture Constraints

The system operates peer-to-peer, with all announcements and bids distributed to all users regardless of their participation in specific auctions. If necessary, you may use central servers for:

- User registry
- User discovery
- Bid distribution
- Trusted services (e.g., Certification Authorities, trusted timestamping)
  All communications between clients and servers must protect the content's confidentiality and integrity.

Deliverables

You must submit all deliverables by **December 9th**.

- Submit all the source code clearly documented for assessment purposes.

- Submit a report up to 10 pages containing detailed justifications demonstrating how your solution achieves each security requirement.

Project discussion

All groups are required to attend a 20-minute evaluation session on **December 11th**. During this session, all members must take part in a discussion of the developed system with the coordinating professor. Attendance is mandatory for every student. Failure to participate will result in a final classification of “Não Admitido (NA)”