Secure Election System - Project Report

This document provides a detailed overview of the Secure Election System project. It includes a comprehensive project description, clear step-by-step instructions for execution, screenshots for verification, and a breakdown of contributions among all team members.

---

1) Project Description

Overview

The Secure Election System is designed to provide a secure way for people to vote electronically, to eliminate voters having to be physically present at designated election locations. This project demonstrates a secure electronic voting system designed with two central authorities: **Central Legitimization Agency (CLA)** and **Central Tabulating Facility (CTF)**. The system is engineered to ensure voter authentication, privacy, integrity, and transparency throughout the election process.

Project Objectives

- Implement Secure Election Protocol with two central facilities (CLA and CLF) that meets the following requirements:
    - Only authorized voters can vote before the election ends.
    - No one can vote more than once.
    - No one can determine for whom anyone else voted.
    - No one can duplicate anyone else's votes.
    - Every voter can make sure that his vote has been taken into account in the final tabulation.
    - Everyone knows who voted and who didn't.
- RSA-based encryption for privacy.
- One-time use validation numbers to ensure that voters can only vote once.
- Clear separation between voter verification and vote tabulation.

Core Components

- Central Legitimization Agency (CLA): Authenticates and validates voter identities against stored credentials and issues validation numbers to voters who are authorized to vote.
- Central Tabulating Facility (CTF): Receives votes and verifies the authenticity of each validation number and records the vote. Decrypts votes using RSA keys and tallies the results.
- Voter: Encrypts vote and submits to the CTF along with the validation number issued by CLA.
- RSA Encryption: Used for authentication and secure key exchange.

---

2) Development Environment

The project was developed with the following setup:

- **Programming Language: Java**
- **Build Tool:**
- **IDE: IntelliJ IDEA**
- **Java Version: Compatible with JDK 8+**
- **File Structure:**
    - **src/: Contains Java source files**
    - **data/: Contains text files for validation numbers, voter information, vote tallies**

---

3) How to Run Your Program

Step 1: Open the Command Prompt and Navigate to the Project Directory

Compile all class files.

javac CTF/CTF.java CLA/CLA.java Voter/Voter.java Keys/*.java

Step 2: Generate Keys

java Keys.KeyGeneration

A pair of RSA keys is created and saved as **public_key.txt** and **private_key.txt** in the **Keys** directory. These keys will be used to encrypt/decrypt the votes for security.

Step 3: Start the CLA

java CLA.CLA

- CLA waits for voter login (ID and password).
- If the credentials match those in VoterID.txt and VoterPassword.txt, the CLA:
    - Issues a **validation number** from ValidationNumbers.txt.
    - Records that this number has been used in UsedValidationNumbers.txt.

Each validation number is **unique** and **one-time-use only**.

Step 4: Start the CLF

java CTF.CTF

- CTF accepts a vote with an attached **validation number**.
- It checks if:
    - The validation number is legitimate.
    - The number has not been used before.
- If both conditions pass:
    - The encrypted vote is **decrypted** using private_key.txt.
    - The vote is recorded in VoteTally.txt.

Step 5: Simulate a Voter Session

java Voter.Voter

- Prompts the user for ID and password.
- Communicates with the CLA to obtain a validation number.
- Prompts for the vote (e.g., Candidate A, B, etc.).
- Encrypts the vote using the public key.
- Submits the encrypted vote and validation number to the CTF.

Step 6: View Final Vote Tally

A count of how many votes each candidate received can be found in **data/VoteTally.txt**

---

4) Screenshots of Each Test

CLA Authentication

```
Main Menu:
1. Login
2. Exit
Select an option: 1
Enter your Voter ID: alma4
Enter your Password: ijkl
Attempting to connect to CTF at port 8888...
Connection established with CTF.
Login successful!
```

CLA Issuing a Validation Number

```
Election Menu:
1. Get Validation Number
2. Vote for a Candidate
3. View Results
4. Logout
Your choice: 1
Connecting to CLA on port 7777...
DEBUG: Raw response from CLA ? 91388864
Your validation number is: 91388864
DEBUG: validationNumber now holds ? 91388864
```

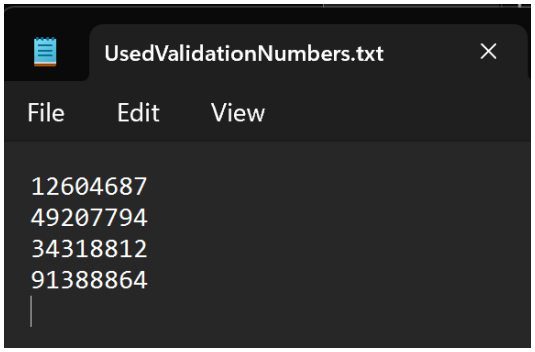
Voter casting a vote

```
Election Menu:
1. Get Validation Number
2. Vote for a Candidate
3. View Results
4. Logout
Your choice: 2
Connecting to CTF on port 8888...
List of Candidates:
-------- Election Race --------
Alice - Total Votes: 3
Bob - Total Votes: 2

1. Person 1
2. Person 2
Please vote by sending 1 or 2

Enter your vote (number): 1
Vote recorded successfully for: Alice
```

Encrypted Vote Submission and Validation Number submitted to CTF

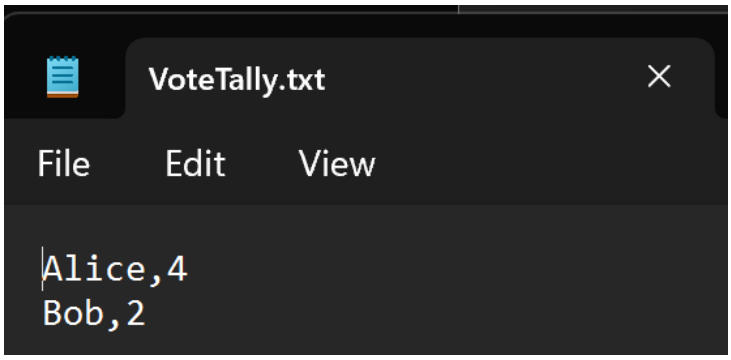


CTF Vote Verification and Tallying

```
Election Menu:
1. Get Validation Number
2. Vote for a Candidate
3. View Results
4. Logout
Your choice: 3
Requesting results from CTF (port 8888)...
Connected to CTF. Fetching result...

--- Current Vote Tally ---
-------- Election Race --------
Alice - Total Votes: 4
Bob - Total Votes: 2
```

VoteTally.txt Content



Attempt to vote twice

```
Election Menu:
1. Get Validation Number
2. Vote for a Candidate
3. View Results
4. Logout
Your choice: 2
Connecting to CTF on port 8888...
You have already voted. Vote denied.
```

---

5) Contribution to the Project

This project was completed by:

1. **Anvaya Chandrika Gudibanda Sreesha (CIN : 403266159)**

a. Built over the core socket setup to extend validation flow, vote eligibility checks, and result handling across Voter, CLA, and CTF by identifying issues and debugging core logic.

b. Refined user prompts, added edge-case handling, and ensured smooth end-to-end interaction experience.

2. **Kevin Loi (CIN : 403333252)**

    a. CLA/CTF/Voter Server socket

    b. User Login, validation number generation, vote tally

3. **Alma Campos (CIN : 307114150)**

    a. Conducted testing and validation of CLA/CTF/Voter Server socket

    b. Structured and authored project documentation.