**CS 5780**

**Project Report**

**Secure Election System**

**Group ID: 7**

**Patel Smitkumar (306587208)**

**Patel Riddhiben (306612701)**

**Project Description**

The implementation will provide a secure way for people to vote electronically, which eliminates the hassle of physically being present at designated election locations.

Since computerized voting will not replace general elections unless there is a protocol that both maintains individual privacy and prevents cheating, the ideal protocol must meet these 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

Your design should use two central facilities: Central Tabulating Facility (CTF) and Central Legitimization Agency (CLA). CLA's main function is to certify the voters. Each voter will send a message to the CLA asking for a validation number, and CLA will return a random validation number to the user. The CLA retains a list of validation numbers as well as a list of validation numbers' recipients to prevent a voter from voting twice. Then, the CLA sends the same number the CTF. After a voter gets the validation number from CLA, the voter sends his/her vote and the validation number to CTF. CTF's main function is to count votes. CTF checks the validation number against a list of numbers received from the CLA. If the validation number is there, the CTF crosses it out (to prevent someone from voting twice). The CTF adds the identification number to the list of people who voted for a particular candidate and adds one to the tally. After the election ends, the CTF publishes the outcome.

All the data sent between a voter and CLA, between CLA and CTF, and between a voter and CTF should be encrypted. For simplicity, RSA will be used for encryption and decryption. Suppose each party involved in the protocol has a public key/private key pair. All voters know the public keys of CTF and CLA. CTF keeps a list of eligible users and their public keys in a text file. CTF amd CLA know the public key of each other.

**How to Run the Application?**

Run program in eclipse:

1. Run ctf.java:

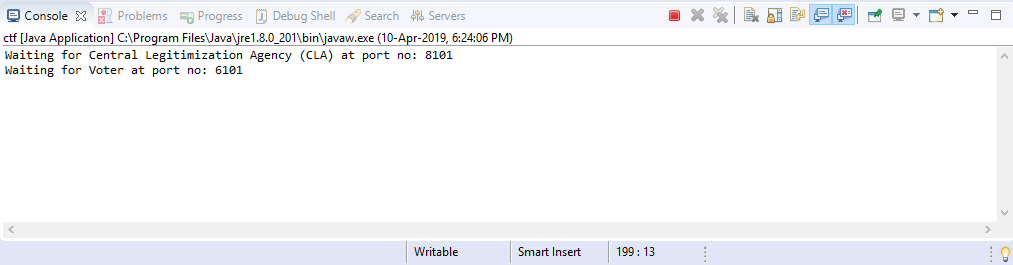
For data management below files are being used in program ctf.java

Raw\_\_Data.txt: Stores data related to voter public keys

candidateList.txt: Contains candidate name, candidate id and total vote received

CTF\_Login.txt: contains voter username and password

First run: Agency server will start-up listening at localhost on port 8101



Ctf.java handles voter request and manages voting related activities

1. Cla.java

First run: stablish connection with CTF facility listening on port 8101. If connection stablished, starts listening on localhost at port 7101 and handle voter request in reference to validation no. Generate validation number and update the data in below file. Also provide the validation no of voter on request received for vote.

ValidatioNos.txt: contains username and validation no separated by ‘,’.

1. Voter\_1.java:

This is the client application stablish the connection with ctf.java and allow user

to generate validation number, caste vote and allow user to see the no of votes

received to all candidates.

1. Candidate\_1.java

It is an entity class for a candidate that stores information about the candidate:

1. Candidate name
2. Candidate id
3. Candidate votes received (initially kept 0)

The cla.java create objects of candidate\_1.java according to the information available in the candidateList.txt

1. RSA.java

The java file does encryption and decryption tasks whenever server needed to generate RSA key for a user.

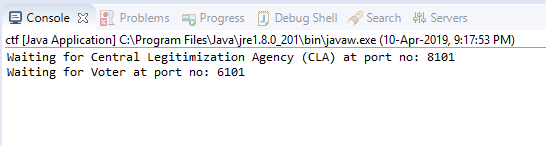
**Output**

Run Application in eclipse:

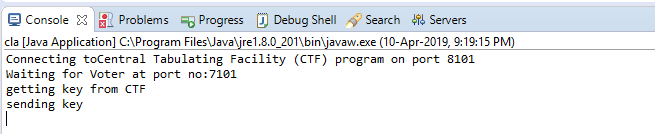
1. Create a new project with any name
2. Copy the Java files to the source directory
3. Copy the text files to the root directory of the project

Screen shots of application run:

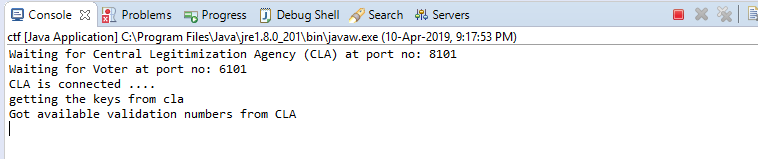
1. Run ctf.java (SERVER):



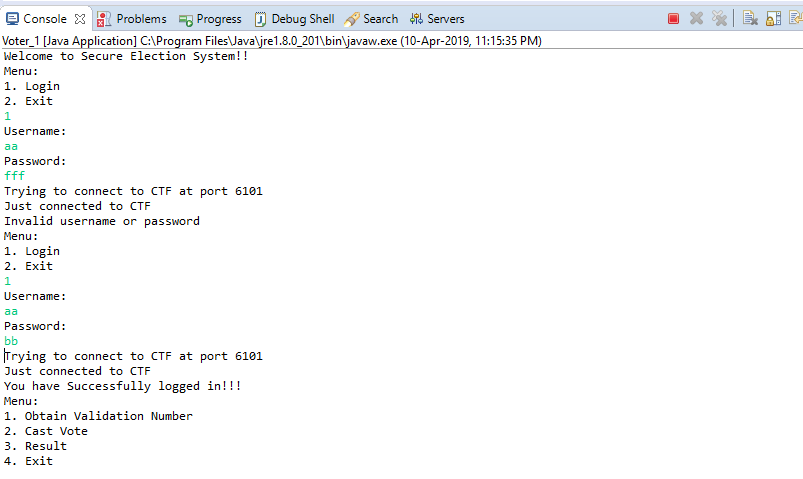
1. Run cla.java:



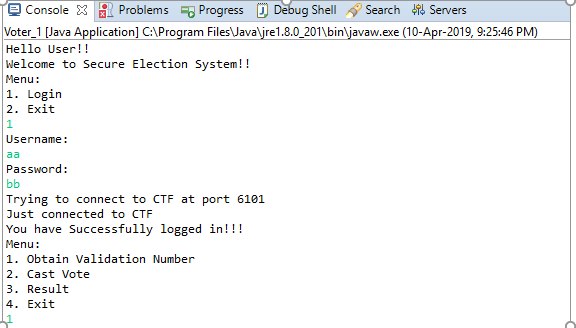
Updates on ctf server console:

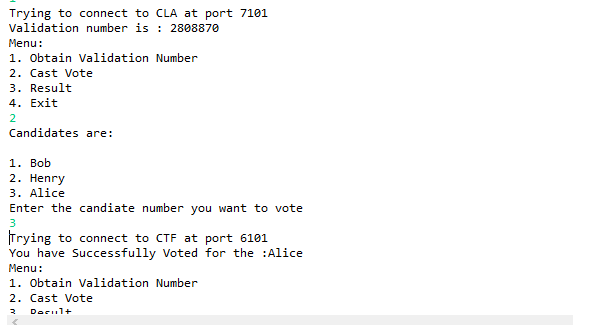


1. Run Voter\_1.java
2. Login:

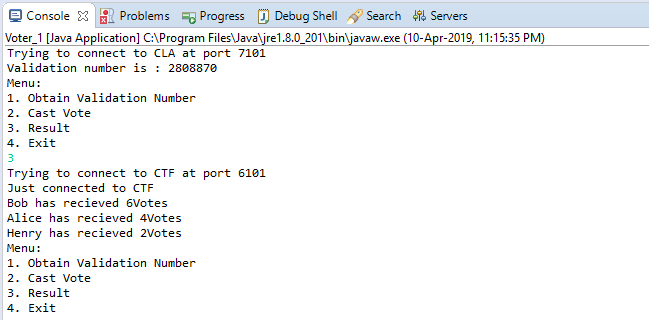


1. Login, getting validation no and casting vote:





1. Show result:



**Contribution:**

We equally contributed on this project together. Riddhi designed the project and Smit coded the module, helped each other debugging and solving errors.