Advanced Cryptography – Project

Electronic Voting

Instructions

1. The assignment can be performed in the same teams as the home assignments.
2. The home assignment is to be presented during the lecture hours on **29/1/2025**. All the partners must be present during the meeting. **Both partners will be graded separately for their part in their home assignment.**
3. The home assignment must be submitted until 28/1/2025, 23:55 into Moodle. Only one partner should submit the project but the names of all the partners must be included.
4. The delay can be granted **only** due to the sickness and military reservation service (miluim). The delay can be asked **only** via emails with the attachment of relevant documents.
5. Copying ANY part is strongly prohibited and will be graded by 0, all the students will stand to disciplinary committee in this case.

In the project, you are to design an **electronic voting system**.

The goal of the project is to show how basic cryptographic primitives, like ZKP and cryptographic algorithms, can be combined into a complicated application giving a real value.

Your voting system will assume that we have ***m*** voters, and there are ***n*** centers, which perform the tallying. (The use of a multitude of tallying centers is to allow voter anonymity and stop a few centers colluding to fix the vote.) There must be 3 centers with 15 voters each – 5 voters must be added during the defense and 10 voters already in the database together with their votes.

We shall assume that voters are only given a choice of one of two candidates. To avoid political discussions ☺, let's assume we have an USA political system, that is the only candidates are Democrat or Republican.

The voting system must have the following properties:

1. Only authorized voters will be able to vote.
2. No one will be able to vote more than once.
3. No stakeholder will be able to determine how someone else has voted.
4. No one can duplicate someone else's vote.
5. The final result will be correctly computed.
6. All stakeholders will be able to verify that the result was computed correctly.
7. The protocol will work even in the presence of some bad parties (third parties who might interfere in the voting processes – the BAD GUYS).

Please note that you are responsible of implementing ZKP and cryptographic algorithms from the previous assignments into the relevant and suitable parts of the requirements. The data must be encrypted using the shared key and AES algorithm. For the ZKP use isomorphic graph you developed in HW1. See where it must be implemented in the project.

To arrange office hours regarding the assignment, please write an email until Tuesday, 15:00 to get a specific time for your team.

Good luck!