Cryptography

Crypto Project

Each Project: (100 points). You need to:

3 VI (25 pts.) provide a short report describing: problem statement, description of the cryptographic building blocks and proposed solution/results. You need to look for the most recent scientific papers helping solve a given problem.

10 VI (25 pts.) present version alpha of the project (*e.g.,* TLS communication working),

23 VI (50 pts.) final presentation of the solution.

Each project can be prepared by up to 2 students.
Each project which involves communicating parties needs to use TLS protocol for providing secure communication. You need to:

- create your own certificate authority,
- issue a certificate for each participating party,
- use a client-side certificate for authentication.

List of problems:

1. Implement a social game where: a selected person formulates a question that is sent out to participants. Each participant answers yes/no ($x_i \in \{0, 1\}$, the "group answer" is defined as $\max_i\{x_i\}$. The protocol should be designed (and implemented) in such a way that each participant's input remains secret.

   See: dining-cryptographers protocol, veto network.

2. Implement a mobile app which has a functionality similar to "Tinderella" (`www.youtube.com/watch?v=bLoRPielarA`). The goal of the protocol performed between users P_i and P_2 with inputs x_1, x_2 respectively is to compute $F_i(x_i, x_2) = F_2(x_1, x_2) = b$ where $b = x_1 \wedge x_2$.

   Your app should not let anyone to learn about user's inputs (you can use Yao's garbled circuits or GSW protocol).

3. Write a mobile app which lets two users to tell if they are nearby. Implemented functionality returns 1 if two users are within a given distance and returns 0 in any other case.

4. Prepare a mobile app(s) which implements Feige-Fiat-Shamir identification protocol. Such an app can be used then as user's digital ID.

5. Implement 2-out-of-n threshold encryption for an app which stores an encrypted data backup in a cloud. In order to decrypt data one needs to use two devices (*e.g.,* PC + phone).

6. Choose an NP-hard problem and use it as a signature schme (start with finding a zero-knowledge proof for it and then apply Fiat-Shamir heuristic).