Homework 2

Please submit your solutions to the email address 7ccsmsen at gmail dot com. Please submit only ASCII text or PDFs. Every solution should be preceded by the corresponding question, like:

Qn:	**…a difficult question from me…**
A:	**…an answer from you …**
Q$n+1$	**…another difficult question…**
A:	**…another brilliant answer from you…**

Solutions will only be accepted until 30th December!

1. Often problems in e-voting are due to difficulties with authentication. Keep this in mind for what could go wrong with the following discount offered by an insurance company: John Hancock Insurance is partnering with Vitality, which you might know as one of those work-related wellness programmes. The programme is available in 30 US states. If you sign up for this, John Hancock will send you a free Fitbit monitor. That's a tiny, pill-shaped device that some people wear in sleek-looking bracelets to track how far they walk/run, the calories burned, and the quality of sleep. That means the insurance company would know exactly when a customer does a sit-up, how far she runs – or when he or she has skipped the gym for a few days. For 'good' customers there will be a discount in their premiums. Why is this a problem?

2. Voice voting is the method of casting a vote in the 'open air' for everyone present to hear. Which of the following security requirements do paper ballots satisfy **better** than voice voting? Check all that apply and give a brief explanation for your decision.

   - ☐ Integrity
   - ☐ Enfranchisement
   - ☐ Ballot secrecy
   - ☐ Voter authentication
   - ☐ Availability

3. Explain how an attacker can use chain voting in order to influence the outcome of a poll using paper ballots.

4. Which of the following mechanisms help with defending against chain voting? Check all that apply. Give a brief reason for each defence that mitigates chain voting attacks.

   - ☐ Using a glass ballot box to make it clear there are no ballots in the box before the start of the election.

- ☐ Distributing ballots publicly before the election.
- ☐ Checking that a voter's ID (drivers license, passport) matches the voter.
- ☐ Each ballot has a unique ID. When a voter is given a ballot, the ID is recorded. When the voter submits his or her ballot, this ID is checked against the record.

5. In the Estonian general election, votes can be cast via Internet some time before the election day. These votes cast via Internet can be changed an unlimited amount of times, the last vote is tabulated. You can even change your vote on the polling day in person. Which security requirement does this procedure address?

6. What is the main difference between online banking and e-voting? (Hint: Why is the latter so hard to get secure?)

7. Imagine, hypothetically, you have a perfectly secure Internet voting system, by which I mean nobody can tamper with or steal votes between your browser and the central server responsible for vote tallying. What can still go wrong with such a perfectly secure voting system, which is prevented in traditional elections with paper-based ballots?