The art of cryptography, summer 2016

MICHAEL NÜSKEN

13. Exercise sheet
Hand in solutions until Monday, 18 July 2016, 11:59

Exercise 13.1 (Civitas). (0 points)

Study the Civitas election scheme as embedded in the course' notes.

Exercise 13.2 (dudle). (0+16 points)

Having public polls and scheduling parties are processed similar to elections. A common tool for this is `http://www.doodle.com/`. A project at TU Dresden aims at generating a "privacy-enhanced" version of doodle, see `http://dudle.inf.tu-dresden.de/`.

(i) Find the documentation Kellermann and Böhme (2009) and name the problems they address. +3

(ii) There are four steps in the scheme. Name them and present their content in pseudo-code. +6

(iii) Comment on the designer's claims concerning +4

- verifiability,
- privacy,
- usability, and
- computational complexity.

(iv) Find newer reports and discuss improvements. +3

Exercise 13.3 (Voting). (10 points)

Two fundamental steps in voting are

election process getting the voters' opinion (assuming they have one),

tallying process transforming the voters' opinion into a final result.

The party pooper for the second point is ARROW's theorem. In this exercise we deal with the first point. The bad news here is reality. The US Presidential Election in 2000 had several problem's with the first step.

(i) List three of these problems as precisely as possible (give your sources). 3

(ii) Has something similar happened in Germany or in your home country (take your state, if you are German)? 4

(iii) Derive general principles for the election process. 3