Walter Unger
Sascha Geulen

WS 2012/2013
December 12, 2012

Exercise
Algorithmic Cryptography

Sheet 9

Exercise 9.1: **(4 points)**

Construct an election protocol for the following problem:

Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_m\}$ be two groups of voters, and $\mathtt{K}_1$ and $\mathtt{K}_2$ be two candidates. One of the candidates is to be elected. A candidate wins the election if he gets at least 50% of the votes (absolute majority) and if he gets at least 10% of each group (veto of group A or B). It is not allowed to use a trusted center.

Exercise 9.2: **(4 points)**

Construct an election protocol for the following problem:

Let $\mathtt{K}_1$, $\mathtt{K}_2$, and $\mathtt{K}_3$ be three candidates. Each voter can vote for one of the candidates or can do an invalid vote. The election is only valid and the result may only be revealed if at least 50% of the votes are valid. Then the candidate with the most votes wins (relative majority). It is not allowed to use a trusted center.

Exercise 9.3: **(4 points)**

Construct an election protocol for the following problem:

Let $\mathtt{K}_1$ and $\mathtt{K}_2$ be two candidates. The candidate with the most votes wins (absolute majority). The result of the vote must not be revealed, but it must be possible for the winner that he can convince the voters of being elected. It is not allowed to use a trusted center.

Exercise 9.4: **(4 points)**

Construct a protocol for the following problem:

A donor `D` wants to donate a given amount of money to *one* of two donees `A` or `B`. `D` shall be able to check whether the amount was received by `A` or `B`, but he must not determine who got the amount. It is not allowed to use a trusted center.

Deadline: Wednesday, December 19, 2012, 15:00,
in the lecture or in the letterbox in front of i1.