Exercise Algorithmic Cryptography Sheet 7

Exercise 7.1 (4 points)
Construct a protocol for the following problem:
A and B want to exchange two equally long binary messages, i.e., A wants to send the information $I_A$ to B and B wants to send $I_B$ to A, with $|I_A| = |I_B|$. If one of the participants aborts the protocol, the other participant has at most twice the work to determine the desired information. Do not use a trusted center.

Exercise 7.2 (4 points)
Construct a protocol for the following problem:
A, B and C want to play skat. For this, 32 cards must be dealt out such that each player gets ten cards and two cards—the skat—are put aside. It must be impossible that any player can influence the cards dealt out for any player or can see which cards were given which player. Do not use a trusted center.

Exercise 7.3 (4 points)
Construct a protocol for the following problem:
A, B and C want to determine who has the most money, but none of them wants to say how much money he has actually. Furthermore, no other information except who has the most money must be revealed; in particular, it must not be revealed who has the least money. The number of communication rounds must be independent of the capital. Do not use a trusted center.

Hint: Assume that the money of A, B and C is less than 100,000 €.

Exercise 7.4 (4 points)
Construct a protocol for the following problem:
A, B and C want to elect one of them randomly. It must be possible that two people cooperate in order to manipulate the election arbitrarily. If this happens, the third person must not discover it. Do not use a trusted center.

Deadline: Thursday, December 12, 2013, 10:15 a.m., in the lecture or in the letterbox in front of i1.
Please fill in your name and your student number and mark the exercises that you can present. Then staple this page in front of your solution sheet.

<table>
<thead>
<tr>
<th>Name</th>
<th>Student Number</th>
<th>E 7.1</th>
<th>E 7.2</th>
<th>E 7.3</th>
<th>E 7.4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>