Walter Unger
Sascha Geulen

WS 2012/2013
December 19, 2012

Exercise
Algorithmic Cryptography

Sheet 10

Exercise 10.1: **(4 points)**

Before Knud Knudson became a famous polar researcher (see, e.g., the historical documents of BuK WS 10/11) he discovered on one of his expeditions to the Indian Ocean the native people of the Christmas Island. Their tribal chief is elected by all citizens, but each person has a certain weight in the vote, e.g., the medicine man has a much higher influence on the vote than the ordinary people. The participation in the election is for each person compulsory. At the end of the vote, the candidate with the most votes becomes the next tribal chief (relative majority).

In an attempt to modernize the voting system, the natives want to get rid of the old ballot based system and change to a more sophisticated online election system. This system must preserve anonymity, but obviously the voters have to be counted correctly and no one must be able to cheat. Your task is now to design a system that satisfies all the requirements.

Exercise 10.2: **(4 points)**

After the discovery of the desolated New Year's Day Island, a conflict between the Christmas Island and the New Year's Eve Island began, that eventually had lead to a war between the two parties. Since one of Knud Knudson's hobbies is diplomacy, he could convince both governments of doing an election. Knud Knudson's idea is to do a hierarchical election, i.e., the citizens of the two islands first vote one of N parties and then the parties which get at least 5% of the votes do a second election, in which the new Chancellor of the New Year's Day Island is voted by an absolute majority. Each party is weighted with the result of the first election, e.g., if party `A` has got 30% of the votes in the first election, its weight in the second vote is 30. In order to achieve an absolute majority, coalitions between the parties are allowed.

Knud Knudson has suggested you for the design of the proposed election system.

Exercise 10.3: **(4 points)**

Noticing the successes of Knud Knudson's ideas for election protocols, he was invited to give the keynote talk at the respected SUPER (Symposium on Unknown Protocols for Election and Randomness) conference in Svizra. One of the talks at the conference aroused Knud Knudson's interest, an election protocol for yes/no votes where each voter can give a positive or negative vote or he can abstain. After the election only the result (yes or no) is revealed, but the number of positive and negative votes and abstentions stays secret. Unfortunately, Knud Knudson cannot remember the details of the protocol and, since he is not a computer scientist, he is not able to implement it. On the other hand, he has heard on the conference that a group of students from Aoke has studied a similar protocol in a lecture about cryptography. Can you design the protocol for Knud Knudson?

Exercise 10.4: **(4 points)**

After the conference, Knud Knudson prepares his equipment for the next expedition to the North Pole. His colleagues gave Knud Knudson for an analysis of the Ocean current a prime number p, n generators $g_1, \ldots, g_n$ of $\mathbb{Z}_p^*$, and n numbers $y_1, \ldots, y_n \in \mathbb{Z}_p^*$ with $y_i = g_i^{x_i} \bmod p$ for some x_i not known by Knud Knudson. Knud Knudson knows that if there is a pair $(y_i, y_j), i \neq j$ for that the same x was used, then the numbers will conflict with each other and cannot be used for the analysis.

Give an algorithm, that computes all pairs $(y_i, y_j), i \neq j$ such that $y_i = g_i^x \bmod p$ and $y_j = g_j^x \bmod p$ for the same x.

Merry Christmas and a Happy New Year!

Deadline: Wednesday, January 9, 2013, 15:00,
in the letterbox in front of i1.