Walter Unger
Sascha Geulen

WS 2012/2013
November 28, 2012

Exercise
Algorithmic Cryptography

Sheet 7

Exercise 7.1: **(4 points)**

Construct a Zero-Knowledge-Proof based on the following problem:

`VERTEX COVER`
Input: Graph $G = (V, E)$ and $k \in \mathbb{N}$.
Question: Is there a vertex cover of size at most k for G, i.e., a subset $C \subseteq V$ with $|C| \leq k$ such that for each edge $\{u, v\} \in E$ at least one of u and v belongs to C?

Exercise 7.2: **(4 points)**

Construct a Zero-Knowledge-Proof based on the following problem:

`SET COVER`
Input: A set U, n subsets $S_i \subseteq U$, and $k \in \mathbb{N}$.
Question: Is there a subset of at most k subsets S_i such that their union is U?

Exercise 7.3: **(4 points)**

Construct a Non-Interactive Zero-Knowledge-Proof based on the following problem:

`DISCRETE LOGARITHM`
Input: Prime number p, generator g of $\mathbb{Z}_p^*$, and $y \in \mathbb{Z}_p^*$.
Question: What is the $x \in \{1, \ldots, p-1\}$ with $y \equiv g^x \bmod p$?

Definition: In a Non-Interactive Zero-Knowledge-Proof, the challenge is chosen by the Prover.

Exercise 7.4: **(4 points)**

Construct a protocol for the following problem:

`A` and `B` want to interchange two equally long binary information, i.e., `A` wants to send the information $I_{\texttt{A}}$ to `B` and `B` wants to send $I_{\texttt{B}}$ to `A`, with $|I_{\texttt{A}}| = |I_{\texttt{B}}|$. If one of the participants aborts the protocol, the other participant shall have at most twice the work to determine the desired information.

Deadline: Wednesday, December 5, 2012, 15:00,
in the lecture or in the letterbox in front of i1.