1. There is a simple way to turn a sigma protocol into a full non-interactive zero-knowledge protocol in the random oracle model by using Fiat-Shamir heuristic. It works as follows: for a statement $x$ and witness $w$, prover constructs the first message $a$ of the sigma protocol, computes challenge as $c = H(x||a)$ where $H$ is a secure hash function, and then computes the last message $z$ of the sigma protocol. Prover sends $(a, z)$ to the verifier that can recompute $c$ and then verify as usual. Implement this construction for Schnorr’s sigma protocol.

2. Is it fine to compute $c = H(a)$ in the previous construction?

3. Let $G$ be a group of order $p$ and let $g$ and $h$ be its generators. Implement full zero-knowledge construction from the lecture for the relation $R = \{(g^x, h^x) : x \in \mathbb{Z}_p\}$. (homework exercise)