MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Pseudorandom generator from Subgroup Hiding). *Let $\mathbb{G}_* = \langle g_* \rangle$ be a q-element subgroup of a finite group $\mathbb{G}$. We say that $\mathbb{G}_*$ is (t, ε)-indistinguishable from $\mathbb{G}$ if for any t-time adversary $\mathcal{A}$*

$$\mathsf{Adv}^{\mathsf{sgh}}_{\mathbb{G}}(\mathcal{A}) = |\Pr[x \leftarrow_u \mathbb{G} : \mathcal{A}(x) = 1] - \Pr[x \leftarrow_u \mathbb{G}_* : \mathcal{A}(x) = 1]| \leq \varepsilon \ .$$

Define a function $f : \mathbb{Z}_q \to \mathbb{G}$ that is a pseudorandom generator whenever (t, ε)-indistinguishable from $\mathbb{G}$. Describe a naive distinguishing strategy for the subgroup hiding and compute the corresponding time-success bound.

Solution. Hint: The most simple function works **Hint:** How are discrete logarithm and group membership related?