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

Exercise (Random self-reducibility of Subgroup Hiding). *Let* $\mathbb{G}_1 = \langle g_1 \rangle$ *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* $\mathcal{A}$

$$\mathsf{Adv}^{\mathsf{sgh}}_{\mathbb{G}}(\mathcal{A}) = |\Pr[x \xleftarrow[u]{} \mathbb{G} : \mathcal{A}(x) = 1] - \Pr[x \xleftarrow[u]{} \mathbb{G}_1 : \mathcal{A}(x) = 1]| \leq \varepsilon \ .$$

Show that if $\mathbb{G}$ *is a cyclic subgroup of* n *elements then* $\mathbb{G}_1$ *cannot be indistinguishable form* $\mathbb{G}$*. As a consequence, there must exist a base set* $\{g_1, \ldots, g_\ell\}$ *such that any element of* $\mathbb{G}$ *is uniquely representable as* $g_1^{\alpha_1} \cdots g_\ell^{\alpha_\ell}$ *for* $\alpha_1, \ldots, \alpha_\ell \in \mathbb{Z}_q$*. Show that under this assumption subgroup hiding is randomly self-reducible. For that, define an algorithm* $\mathcal{B}$ *such that*

$$|\Pr[\mathcal{B}(x) = 1] - \Pr[\mathcal{B}(y) = 1]| = \mathsf{Adv}^{\mathsf{sgh}}_{\mathbb{G}}(\mathcal{A})$$

for any $x \in \mathbb{G}_1$ *and for any* $y \in \mathbb{G} \setminus \mathbb{G}_*$*. What is the additional requirement to* q *and what happens if this assumption is not satisfied? How one can define subgroup hiding for cyclic groups?*

Solution. Hint: Let g be the generator of $\mathbb{G}$ how g_* looks like and what can you tell about the structure of $\mathbb{G}_*$ in terms of powers of g. **Clarification:** Last question can be neglected.