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

**Exercise (Security of hash ElGamal implies Decisional Diffie Hellman).** *Show that ElGamal cryptosystem is $(t, \varepsilon)$-IND-CPA secure only if the underlying group $\mathbb{G}$ is Decisional Diffie Hellman group.*

**Solution.**