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

Exercise (Almost regular hash function as pseudorandom generator). *Let $h : \mathcal{X} \to \mathcal{Y}$ be an almost regular hash function, i.e. the distribution $h(x)$ for $x \xleftarrow{u} \mathcal{X}$ is statistically ε-close to the uniform distribution over the set $h(\mathcal{X})$. Show that h is a pseudorandom generator provided that $|h(\mathcal{X})| \approx \mathcal{Y}$. Analyse how the distinguishing advantage depends on $|h(\mathcal{X})|$.*

Solution.