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

Exercise (Separation between one-wayness and collision-resistance). *Let $\mathcal{H}$ be (t, ε)-oneway function family with an input domain $\mathcal{X}$ and output range $\mathcal{Y}$. Define a new hash function family $\mathcal{H}^*$ with the input domain $\mathcal{X} \cup \{x_0, x_1\}$ and output range $\mathcal{Y} \cup \{y_0\}$ such that the function family is still one-way but is not collision resistant.*

Solution. Let x_0, x_1 be outside of the range $\mathcal{X}$ and y_0 outside the range. Then we can inplant a known collision to each hash function $h^* \in \mathcal{H}^*$ by defining ...