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

Exercise (Collision-resistance is closed under iterative hashing). *Let $\mathcal{H}$ be (t, ε)-collision resistant hash function family defined by a single function $h : \mathcal{S} \times \mathcal{M} \to \mathcal{S}$. Show that function families defined by the construction*

$$\begin{aligned} g_1(s, m_1) &= h(s, m_1) \enspace , \\ g_2(s, m_1, m_2) &= h(g_1(s, m_1), m_2) \enspace , \\ g_3(s, m_1, m_2, m_3) &= h(g_2(s, m_1, m_2), m_3) \enspace , \\ &\ldots \end{aligned}$$

are also collision resistant function families also indexed by s.

Solution.

Simplified problem. Let us prove the collision resistance of g_2. Let there be a collision, i.e., ... Then ...

General solution. The analysis done above is suitable for any i. Indeed, let g_{i-1} be ....

Qualitative analysis. Note that the success bound grows ...