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

Exercise (Fixed domain CBC is PRF). *Let $\mathcal{M}$ is an Abelian group and let $\mathcal{F}_{all}$ be a family of all functions of type $f : \mathcal{M} \to \mathcal{M}$. Show that functions*

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

are pseudorandom functions. Explain why these functions are easily distinguishable from random if you can query two functions simultaneously, i.e., evaluate CBC construction on different input sizes.

Solution. Recall that $\mathcal{F}$ is (t, q, ε)-pseudorandom function family if any t-time adversary $\mathcal{A}$ that makes at most q oracle queries finds ....

Simplified problem. Let us prove the pseudorandomness of g_2. .... For clarity let $(x_1, y_1) \ldots, (x_q, y_q)$ be the queries to the oracle $g_2(\cdot, \cdot)$. Let $z_i = f(x_i)$ and $w_i = z_i + y_i$. Now for a moment assume that all x_i are different. Then by the definition of $\mathcal{F}_{all}$, we get ...and thus we can replace g_2 with a random function...

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 ...