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

Exercise (PRG from PRP). *Let $\mathcal{F}$ be a (q,t,ε)-secure pseudorandom permutation family defined by a deterministic function $f:\mathcal{K}\times\mathcal{M}\to\mathcal{M}$ such that all functions $f_k(m):=f(k,m)$ are different. Show that functions $g_m:\mathcal{K}\to\mathcal{M}^n$ defined through the following iteration algorithm*

$$
\begin{array}{l}
g_m(k)\\
\left[\begin{array}{l}
c_1 \leftarrow f(k,m)\\
c_2 \leftarrow f(k,c_1)\\
\cdots\\
c_n \leftarrow f(k,c_{n-1})\\
\textbf{\textit{return}}\ c_1,c_2,\ldots,c_n
\end{array}\right.
\end{array}
$$

are pseudorandom generators for any $m\in\mathcal{M}$ for small enough n.

Solution.
SUBPROOF. Let us prove the claim under the assumption that we can replace all function invocations by random samplings from $\mathcal{M}$.

SUBPROOF. Define the collision event and analyse what is the probability that such event occurs under the assumption that function family is the set of all functions $\mathcal{F}_{\text{ALL}}(\mathcal{M}\to\mathcal{M})$. Conclude that the construction is pseudorandom generator under this assumption.

SUBPROOF. Use PRP/PRF switchng lemma to complete the proof