Cryptography: Homework 7
(Deadline: Nov 15, 2018)

1. (15 points) Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a PRG with expansion factor $l(n) > n$. Let $\mathrm{Im}(G) = \{G(k) : k \in \{0,1\}^n\}$ be the image of G. For any $m \in \{0,1\}^{l(n)}$, define $m \oplus \mathrm{Im}(G) = \{m \oplus s : s \in \mathrm{Im}(G)\}$. Show that there exist $m_0, m_1 \in \{0,1\}^{l(n)}$ such that $m_1 \oplus \mathrm{Im}(G) \not\subseteq m_0 \oplus \mathrm{Im}(G)$.

2. (15 points) Show that the fixed-length encryption from PRG (page 6, lecture 10) is not perfectly secret. (hint: use the result of Question 1)