HW I (due February 20th, before tutorial)

1. Suppose that for an application, the attacker has access to an encryption of the key with itself, i.e., $E(k,k)$ (for this we assume that our cipher is such that $\mathcal{K} \subseteq \mathcal{M}$). To define security, we slightly modify the semantic security game: after choosing the key k at random, the challenger starts by sending $E(k,k)$ to the adversary then the game continues as before. Show an example of a semantically secure cipher (E, D) that stays secure even if an encryption of the key is revealed, and another semantically secure cipher (E', D') that becomes completely insecure if an encryption of the key is revealed.

2. Assume $G_1, G_2 : \{0,1\}^\ell \to \{0,1\}^L$ are pseudo-random generators. Assume moreover that one of them is secure, but we do not know which one. Propose a construction of a secure PRG $G : \{0,1\}^{2\ell} \to \{0,1\}^L$ and prove its security.

3. Let $f : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a pseudo-random function. We define a pseudo-random permutation $F : (\mathcal{K} \times \mathcal{K}) \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ obtained by applying a two-round Feistel construction. More precisely, we define $F(k_1 \| k_2, u_0 \| v_0) = u_2 \| v_2$ where $u_1 = v_0, v_1 = u_0 \oplus f(k_1, v_0)$ and $u_2 = v_1, v_2 = u_1 \oplus f(k_2, v_1)$. Show that for any choice of f, F is a pseudo-random permutation, but that it is never a secure pseudo-random permutation. In contrast, one can show that a 3-round Feistel network is a secure PRP provided f is a secure PRF (you are not asked to prove this).