6. Exercise sheet
Hand in solutions until Friday, 9 December 2016, 12:00 (noon)

Exercise 6.1 (PRF ⇒ PRG). (6 points)
Let $F : \{0,1\}^\kappa \rightarrow \{0,1\}^\kappa$, $k \mapsto F_k$ be a pseudorandom function. Fix $w_0, w_1, w_2 \in \{0,1\}^\kappa$, all different. Define $G(s) := F_s(w_0) | F_s(w_1) | F_s(w_2)$.
Prove that $G$ is a pseudorandom generator.

Exercise 6.2 (IND-CPA?). (12 points)
Let $F$ be a pseudorandom function and $G$ a pseudorandom generator with expansion factor $\ell(\kappa) = \kappa + 1$. For each of the following encryption schemes, classify the scheme as insecure, IND-POA secure (but not IND-CPA) or IND-CPA secure. In each case, the shared key $k$ is chosen uniformly random, $k \in \{0,1\}^\kappa$.

(i) To encrypt $m \in \{0,1\}^{2\kappa+2}$ send $m \oplus (G(k) | G(k + 1))$. (3 points)
(ii) To encrypt $m \in \{0,1\}^{\kappa+1}$ choose a random $r \xleftarrow{} \{0,1\}^\kappa$ and send $[r, G(r) \oplus m]$. (3 points)
(iii) To encrypt $m \in \{0,1\}^\kappa$ send $m \oplus F_k(0^\kappa)$. (3 points)
(iv) To encrypt $m \in \{0,1\}^{2\kappa}$ choose a random $r \xleftarrow{} \{0,1\}^\kappa$ and send $[r, m \oplus (F_k(r) | F_k(r + 1))]$. (3 points)

Even if not mentioned explicitly: any statement needs a proof.

Exercise 6.3 (CTR mode). (0+8 points)
Prove this:

**Theorem.** If $F$ is a pseudorandom function then CTR mode with $F_k$ using a randomly chosen initial value $\text{ctr}$ on $\ell$ blocks is IND-CPA secure.

**Hint:** First, consider $\ell = 2$. 
