1. (10 points) Let $F$ be a keyed length preserving function. We proved in class that if $F$ is a PRF, then defining $\text{PRG}(s) := F_s(0^n) \parallel F_s(1^n)$ is indeed a PRG. In this problem you’ll show that switching the roles of the key and input does not work. Specifically, define 

$$G(s) := F_{0^n}(s) \parallel F_{1^n}(s).$$

Prove that $G$ is not necessarily pseudorandom.

Guidelines: You need to prove that if any PRF $F'$ exists, then there’s another PRF $F$ that when plugged into $G$ results in a construction that is not a PRG. This means you need to show (1) a construction of $F$ out of $F'$, (2) a proof that your constructed $F$ is a PRF (show a reduction, using the fact that $F'$ is a PRF), and (3) $G$ is not a PRG (show a distinguisher).

As a hint towards constructing $F$: Define $\forall x \in \{0, 1\}^n, F_{0^n}(x) = F_{1^n}(x) = 0^n$, and $F_k(x) = F'_k(x)$ for all $k \notin \{0^n, 1^n\}$.

2. (10 points) Let $F$ be a PRF. We saw that the encryption scheme outputing $\text{Enc}_k(m) = (r, F_k(r \oplus m))$ (where $r$ is chosen at random) is CPA secure but not CCA secure (note: by default, “CCA” means “CCA2”).

Prove that the scheme is CCA1 secure.

As a reminder, the CCA1 (“lunch time attack”) security definition allows the adversary to access the decryption oracle only before seeing the challenge ciphertext, but not afterwards (while the encryption oracle can be accessed both before and after).

3. (20 points) Let $F$ be a strong PRP. For each of the following schemes, determine whether they are CPA secure, and whether they are CCA secure. Prove your answers by describing the reduction (if secure) or the attacker (if not secure). However, you do not need to provide a full formal analysis of the success probability of your reduction or attacker — an informal argument is sufficient.

(a) $\text{Enc}'_k(m) = (r, F_k(r \oplus m))$ for a random $r$.
(b) $\text{Enc}''_k(m) = F_k(r \parallel m)$ for a random $r$.

4. (12 points) What is the effect of a dropped ciphertext block (e.g., if the ciphertext $c_1, c_2, c_3, \ldots$ is received as $c_1, c_3, \ldots$) when using the CBC, and when using the Counter modes of operation?

5. (10 points) Consider a stateful variant of CBC-mode encryption, where the sender simply increments IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA secure.

As an aside, making the same change to Counter-mode encryption does preserve CPA security, and that is indeed one way to use block-ciphers in stream-cipher mode.
6. **Extra Credit:** Let $P$ be a PRP, and define $P'_k(x) = P^{-1}_k(x)$. Prove or disprove: $P'$ is also a PRP.

Note: on the midterm you were asked to prove this for *strong* PRP, while here the question is about a PRP. As a reminder, the difference in the definitions is in the pseudorandomness condition: for strong PRP the distinguisher is given access to both the permutation and its inverse, while for PRP the distinguisher only has access to the permutation.