CSCI 4331/6331

Quiz 3

Name(s):

1. In this problem, you will prove the following statement:
   Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. Prove that

   $$G(s) = F_s(0^n)||F_s(1^n)$$

   is a PRG.

   The following questions are meant to guide you through the proof. If you feel that you do not need them, you can just provide the full proof at the end.

   (a) Write down the assumption you need to make to start the proof by reduction. (What do you need to assume about the adversary $\mathcal{A}_c$?)

   (b) In order to prove security by a reduction, what is the adversary $\mathcal{A}_r$ that you need to construct?

   (c) How would you construct $\mathcal{A}_r$ using $\mathcal{A}_c$?

   (d) Argue that $\mathcal{A}_r$ succeeds if $\mathcal{A}_c$ succeeds.

2. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF.
   Is $F'_k(x) = F_k(x)||F_k(\overline{x})$ necessarily a PRF?

   (a) What do you get when you query F'_k on input $x = 0^n$?

   (b) Can you find two queries x, y such that $F'_k(x)$ and $F'_k(y)$ are correlated?

   (c) How does this help you distinguish F'_k from a random function?