CSCI 4331/6331

Quiz 2

Name(s):

In this quiz, you will practice proving security by reduction.

1. Let $G : \{0,1\}^n \to \{0,1\}^{n+1}$ be a PRG. Prove that

$$G'(s) = \overline{G(s)}$$

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 $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme that has indistinguishable encryptions against an eavesdropper. Prove that the following encryption scheme is also secure against an eavesdropper.

$$\mathsf{Enc}'_k(m) = \overline{\mathsf{Enc}_k(m)}$$

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) How would you decrypt?

(b) Write down the assumption you need to make to start the proof by reduction. What security game is $\mathcal{A}_c$ playing?

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

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

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

3. What would change if we defined $\mathsf{Enc}'_k(m) = \mathsf{Enc}_k(\overline{m})$