Homework 2

(Due Date: Oct 19, 2015)

1. (5 points) Let G_1 and G_2 be two PRGs. Let G be such that $G(s) = G_1(s) \| G_2(s)$. Is G a PRG?

2. (5+5 points)

   (a) Suppose that we reverse the role of the key s and the input x in the GGM construction of PRF. Is this new construction a PRF?

   (b) Given a PRF family $\left\{ f_s : \{0,1\}^{n+\log n} \rightarrow \{0,1\} \right\}$, construct a new PRF family $\{f'_s : \{0,1\}^n \rightarrow \{0,1\}^n\}$.

3. (10 points) Alice and Bob have never met before. Alice wants to send a sequence of private messages (each of ℓ bits) to Bob. Alice has heard of public-key encryption (PKE) but she does not want to use it to transmit all her messages because PKE requires a lot of computational resources and she only has an old cell phone. She has also heard of secret-key encryption (SKE) as being much more efficient, but she does not know how to transmit her messages to Bob using SKE since she has no a priori shared key with him.

   Alice decides that she is willing to use public-key encryption for sending *one* message (of ℓ bits), and no more. How can she still send all of her messages privately to Bob?

4. (5+5 points) We want to design a sealed-bid auction scheme. Assume that the seller is honest and that the buyers make their bids in some pre-determined ordered fashion (e.g., the lexicographical ordering of their names). A natural security requirement from a sealed-bid auction scheme is that buyer i should not be able to choose his bid based on the bid of buyers $j < i$, since otherwise the former can always outbid the latter.

   Now consider the following two proposals to perform a sealed-bid auction among n buyers:

(a) The seller publishes a public key pk for the IND-CPA secure encryption scheme based on trapdoor permutations discussed in class. Each buyer sends the encryption $Enc(pk, x)$ of its bid x, and then the seller decrypts all of these and awards the product to the highest bidder.

(b) Each buyer commits to her bid using the commitment scheme based on one-way permutations discussed in class. Once all the commitments are finished, each buyer reveals her bid by opening the commitment. The seller awards the product to the highest bidder.

Do either of these proposals satisfy the security requirement of sealed bid auction?

5. (15 points) Consider the language:

$$L = \{(G_0, G_1), (H_0, H_1) \mid \textsf{either } G_0 \sim G_1 \textsf{ or } H_0 \sim H_1\}$$

That is, an instance $x = (G_0, G_1), (H_0, H_1)$ is in the language L if either G_0 and G_1 are isomorphic or H_0 and H_1 are isomorphic.

Construct a zero-knowledge interactive proof system for L.

6. (Extra Credit) Using a commitment scheme, design a three-message protocol that allows two mutually distrusting parties to toss a coin such that even if either of the parties is adversarial, the outcome of the protocol looks indistinguishable from the uniform distribution. (The parties are assumed to always finish the protocol.)