Theoretical Foundations of Cryptography
Assignment 3

Instructor: Bhavana Kanukurthi

This problem set is due on Tuesday, October 17th, 11:59P.M. via email. The email needs have the subject "Assignment 3". The filename has to have the format firstname2.pdf where "firstname" is your First Name.

Collaboration Policy

- At most two students may collaborate on the assignment. If you choose to do so, both students need to acknowledge the same in their write-ups.
- Collobaration must be restricted to discussions. Each student must write-up their solutions independently.
- If you choose to consult any other source, you must credit that source as well.

Problem 1 (5+5 Points)**.** Let $G : \{0,1\}^{n_1} \to \{0,1\}^{n_2}$ be a pseudorandom generator. Let $h_1 : \{0,1\}^{n_1} \to \{0,1\}^{n_1}$ and $h_2 : \{0,1\}^{n_2} \to \{0,1\}^{n_2}$ be polynomial time computable permutations. Prove that G_1 and G_2 defined by $G_1(s) \stackrel{\mathsf{def}}{=} G(h_1(s))$ and $G_2(s) \stackrel{\mathsf{def}}{=} h_2(G(s))$ are both pseudorandom generators.

Problem 2 (10 Points)**.** Recall that in a standard definition of a PRF, the adversary is allowed to query the PRF on inputs, polynomially many times. He is allowed to make these queries adaptively: namely, he can send a query after receiving the responses (i.e., output of the PRF) to his previous queries. Now, unlike in a standard (or adaptive) PRF, a non-adaptive PRF is only secure if an adversary specifies all his queries $x_1, x_2, \ldots, x_{\mathsf{poly}()}$ at the same time. In other words, he can't wait to receive $F_k(x_i)$ before specifying his next query, x_{i+1}.

Given any (standard) PRF, build a "weak" form of a PRF which has the following properties:

- It needs to be completely insecure against adaptive queries.
- If the queries are non-adaptive, the PRF outputs will remain hard-to-predict.