Theoretical Foundations of Cryptography E0 248
Problem Set 2

Instructor: Bhavana Kanukurthi

This problem set is due on Friday, September 15th, 5:00P.M via email. The email needs have the subject "Assignment 2". 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 (10 Points)**.** Given a strong (resp., weak) one-way function, prove that there exists a length-preserving strong (resp., weak) one-way function.

Problem 2 (10 Points)**.** Let $f : \{0,1\}^n \to \{0,1\}^n$ be a strong one way function. Then consider the function $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined as following: $g(p,x) = (p, f(x))$ if p starts with $\log(n)$ zeroes and $g(p,x) = (p,x)$, otherwise, where $|p| = |x|$. Then prove that g is a weak one-way function. Now, let f be a weak one way function and prove that g (defined as before) is a weak one-way function.

Notation For any function h, we denote by h^T the function which composes h itself T times. In other words, $h^T(x) = \underbrace{h(h(\ldots(h(x))))}_{T \text{ times}}$.

Problem 3 (20 Points)**.** Let f be a one-way permutation (i.e., a one-way function which is also a permutation). Given $k > 0$, use f to build a one-way function g such that g^k is a secure one-way function but g^{k+1} is insecure.

Problem 4 (20 Points)**.** Let $f : \{0,1\}^n \to \{0,1\}^n$ be a weak one-way permutation. Here is a suggestion for building a strong one-way function g from it: For all x, simply let $g(x) = f^T(x)$ where T is a polynomial in n. Is g necessarily one-way? Prove or disprove.