Theoretical Foundations of Cryptography E0 248
Problem Set 1

Instructor: Bhavana Kanukurthi

This problem set is due on Monday, August 28th, 5:00PM.

Problem 1. Suppose $\varepsilon : \mathbb{N} \to [0,1]$ is not a negligible function. Consider this statement: *There exists some polynomial $p()$ (where $p(k) > 0, \forall k > 0$) and some $k_0 > 0$ such that $\varepsilon(k) > 1/p(k)$ for all $k > k_0$?*
Either disprove it with a counter-example or prove it.

Problem 2. [1]

(a) Show that the existence of one-way functions implies $\mathsf{P} \neq \mathsf{NP}$.

(b) Suppose that one-way functions exist. Does there exist a one-way function $f : \{0,1\}^n \to \{0,1\}^n$ with a fixed point, i.e. $f(0^n) = 0^n$?

Problem 3. Suppose $f, g : \{0,1\}^{2n} \to \{0,1\}^m$ are one-way functions. For $x \in \{0,1\}^{2n}$, let x_1 and x_2 denote the first and second halves of x, respectively. Furthermore, $(\cdot,\cdot)$ is the concatenation operator for bit-strings and $\oplus$ is the bit-wise exclusive or operator. Prove that in general:

(a) $f_a(x_1, x_2) := (f(x_1, x_2), x_1)$ is not a one-way function.
Hint: Can we have one-way functions which *do not* depend on the entire input?

(b) $f_b(x_1, x_2) := (f(x_1, x_2), x_1 \oplus x_2)$ is not a one-way function.

(c) $f_c(x_1, x_2) := (f(x_1), g(x_2))$ is a one-way function.

(d) $f_d(x) := (f(x), g(x))$ is not a one-way function.

Problem 4. Show that one-way functions cannot have polynomial size ranges. Prove that this is true even for a weak one-way function.

Problem 5. Consider the following conjecture: *For every length preserving[2] one-way function, the function $f'(x) = f(x) \oplus x$ is also one-way.* Refute it.

[1] Unless otherwise mentioned, when we say one-way functions we mean strong OWFs, in this and all subsequent problems.

[2] A function f is length preserving if the output length is the same as the input length (for all inputs).