CS 359C: Classics of Cryptography **Spring 2017**

Problem Set 0

Due: April 12, 2017, by 2:30pm (submit hard copy at the *beginning* of lecture)

Instructions: You will need to typeset all of your answers in LaTeX using the provided template:

`https://web.stanford.edu/class/cs359c/homework.tex`

This problem set is to ensure that you are able to work with and compile the provided LaTeX template. For your submission, you should download the above template and compile it with your name and other relevant fields filled out. Optionally, you can also include solutions to the following two exercises based on the material from the first lecture. These exercises are intended to help you think about the content, and are entirely *optional*.

Required. Submit a hard-copy of this (possibly otherwise blank) problem set using the provided template.

Optional Exercise. Show that the existence of pseudorandom generators (PRGs) with non-trivial stretch implies $\mathsf{P} \neq \mathsf{NP}$. Something to think about: why does the converse of this statement *not* hold? That is, why does $\mathsf{P} \neq \mathsf{NP}$ *not* imply the existence of PRGs?

Optional Exercise. Let $G\colon \{0,1\}^n \to \{0,1\}^{2n}$ be a secure PRG. Define the function $H\colon \{0,1\}^n \to \{0,1\}^{4n}$ where $H(s) = (G(s_0), G(s_1))$ and $(s_0, s_1) = G(s)$. (Hint: use a hybrid argument). This is the first step in the security proof of the GGM construction.