CS 435: Introduction to Cryptography **Fall 2016-17**

Homework 3

Professor Somesh Jha **Due:** October 29

1. Let G and F be PRGs. Prove that $F \circ G$ (where $\circ$ is function composition) is also a PRG. Follow the proof structure provided in the note which is sent by email.

2. Let G and F be PRGs. Is (F, G) a PRG? Note that $(F, G)(s)$ is $(F(s), G(s))$. Please justify your answer.

3. Let G be a pseudorandom generator and define $G'(s)$ to be the output of G truncated to n bits (where $|s| = n$). Prove that the function $F_k(x) = G'(k) \oplus x$ is not pseudorandom.

4. (**Exercise 3.14**) Prove that if F is a length-preserving pseudorandom function, then $G(s) \stackrel{\text{def}}{=} F_s(1) \| F_s(2) \| \ldots \| F_s(\ell)$ is a pseudorandom generator with expansion factor $\ell \cdot n$.