COMS W6261: Advanced Cryptography: Minimalist Cryptography
Instructor: Tal Malkin

Problem Set 2

Do by: Tuesday 2/23/2016

1. (**Required**) Please read (or brush up on) the definitions for pseudorandom generator (PRG) and pseudorandom function (PRF). [Katz-Lindell 3.3.1, 3.5.1]

2. (**Recommended**) Read how to construct a PRG from a one-way permuation + hard-core bit. [Katz-Lindell 7.4.1, 7.4.2]

3. (**Recommended**) Read how to construct a PRF from a PRG (GGM construction). [Katz-Lindell 7.5]