University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Homework 3

Due at the *beginning* of class on Sept. 28

All numbered exercises refer to the second edition of the book.

1. Exercise 3.3. (Note: the question is asking you to construct an encryption scheme that also hides the length of the plaintext.)

2. Exercise 3.6. When G' is secure you do not need to give a proof, though you should provide an explanation; when G' is not secure you should give a counterexample.

3. Exercise 3.8, parts (a) and (b). Part (c) is optional, and may be done for extra credit.

4. Exercise 3.10(b).

5. Exercise 3.19.