University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Homework 3

Due at the *beginning* of class on Feb. 26

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, but when it is not secure you should give a counterexample.
3. Exercise 3.9. It is enough if the output is just 1 bit long.
4. Exercise 3.10(b).
5. Exercise 3.19.