University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Problem Set 2

This is an ungraded homework, intended to make you think further about some of the concepts covered in class.

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

1. Exercise 2.3.
2. Exercise 2.6.
3. Exercise 2.7.
4. Exercise 2.8. (I strongly suggest you do this problem.)
5. Exercise 2.9.
6. Exercise 2.13(a).
7. Exercise 3.2.
8. Exercise 3.3. (This requires some thought beyond what we have covered in class.)
9. Define the function G as $G(x) = x \| x$ (where "$\|$" denotes string concatenation). Describe and analyze an attack showing that G is not a pseudorandom generator.