University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

Homework 2

Due at the *beginning* of class on Sept. 19

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

1. Exercise 2.6.

2. Exercise 2.7.

3. Exercise 2.8.

4. The following questions concern encryptions of single-character ASCII plaintexts with the one-time pad using the *same* 8-bit key in each part. (But different parts use different keys.) You may assume that the plaintext characters are either English letters (upper- or lower-case) or the space character.

   (a) Say you see the two 8-bit ciphertexts 1011 0111 and 1110 0111. What can you say about which plaintext characters these correspond to?

   (b) Say you see the three 8-bit ciphertexts 1011 0111, 1110 0110, and 1011 0111. What can you say about the plaintext characters these correspond to?

   (c) Say you see the three 8-bit ciphertexts 0110 0110, 0011 0010, and 0010 0011. What can you say about the plaintext characters these correspond to?

5. Online are 7 ciphertexts, each of which was generated by encrypting a 31-character ASCII plaintext with the one-time pad using the *same* key. Decrypt them and recover all 7 plaintexts, each of which is a grammatically correct English sentence. Note: you can use any method you want to recover the plaintexts, as long as you do it on your own. In particular, it is fine to use a combination of automated analysis plus human insight and even occasional guessing. Hint: use what you learned in problem 4.

   Turn in the 7 plaintexts, plus any code you wrote or an explanation of how you obtained the plaintext.