University of Maryland
CMSC456—Introduction to Cryptography
Professor Jonathan Katz

# Homework 8

**Due at the *beginning* of class on May 6**

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

1. The following questions concern the group $\mathbb{Z}_{55}^*$.
   (a) How many elements are in this group?
   (b) Define $f_3 : \mathbb{Z}_{55}^* \to \mathbb{Z}_{55}^*$ by $f_3(x) = [x^3 \bmod 55]$. Compute $f_3(6)$.
   (c) What function computes the inverse of $f_3$?
   (d) Find $x$ such that $f_3(x) = 2$.
2. The following questions concern the group $\mathbb{Z}_{19}^*$.
   (a) How many elements are in this group?
   (b) Find a generator of this group.
   (c) Find an element of this group (besides the identity) that is not a generator.
   (d) Two parties run the Diffie-Hellman protocol using this group and $g = 4$. Say Alice chooses $x = 10$ and Bob chooses $y = 6$. What are the messages sent in this execution of the protocol, and what is the key that the parties compute?
3. Exercise 10.4.
4. Exercise 11.4.
5. Exercise 11.5.
6. Exercise 11.8.