University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Homework 6

Due at the *beginning* of class on Dec. 1

1. (Exercises 7.15/7.16) Prove formally that hardness of the DDH problem relative to $\mathcal{G}$ implies hardness of the discrete logarithm problem relative to $\mathcal{G}$.

2. Say Alice and Bob run an execution of the Diffie-Hellman key-exchange protocol. They work in the group $\mathbb{G}$ consisting of the *squares* modulo 23; the order of $\mathbb{G}$ is 11. They use generator $g = 4$.

   (a) Show that $g = 4$ does indeed generate a group of order 11.

   (b) Alice chooses private exponent $x = 6$ and Bob chooses private exponent $y = 9$. What is the transcript that results from this execution, and the shared key Alice and Bob compute?

3. (cf. Exercise 10.1) Prove that perfectly-secret public-key encryption (i.e., where security holds against an unbounded adversary) is impossible, even for 1-bit messages.

4. (Exercise 10.14) Consider a version of padded RSA encryption, where encryption of m is done by setting $\bar{m} = (0^k \| r \| 00000000 \| m)$ for random r and then computing the ciphertext $c = [\bar{m}^e \bmod N]$. Show a chosen-ciphertext attack on this scheme.