Problem Set #6

CMSC/Math 456
Instructor: Daniel Gottesman

Due on Gradscope, Thursday, Oct. 12, noon (before start of class)

General instructions: If you collaborate or use any outside resources, remember to cite them in your solutions.

Problem #1. Breaking Diffie Hellman (40 points)

For this problem, you are Eve and are faced with Alice and Bob who are running Diffie-Hellman with $p = 67$ and $g = 28$.

When you show your work in this problem, count a single modular exponentiation or a single modular addition, subtraction, multiplication, or division as a single step. E.g., writing $28^6 = 40 \bmod 67$ is one step. While the numbers in this problem are small, any algorithm you use should be reasonably scalable to much larger sizes.

a) (20 points) What is the order of g in $\mathbb{Z}_p^*$? Show what calculations you did to conclude this result. You should solve this by calculating at most 8 modular exponentiations. (You can do it in fewer than this.)

b) (20 points) Alice announces $A = g^a = 46 \bmod p$ and Bob announces $B = g^b = 22 \bmod p$. What is their final key $k = A^b = B^a \bmod p$? Show your work.

Problem #2. Oracle for Discrete Log (80 points)

For this problem, imagine you have access to an oracle $\mathcal{O}$, a black box, that takes input (N, g, y) and outputs x. The output $x = \mathcal{O}(N, g, y)$ satisfies $g^x = y \bmod N$. (If there is no such x, the box outputs "error.") However, each time you use the box, it costs \$1,000, so you want to minimize the number of times you use the oracle. Assume you may also do polynomial-time computations with no cost if they do not use the oracle. (As usual, polynomial-time means polynomial in the length of the input to the computation.)

In each part of the problem, you are asked to give an algorithm to do something, minimizing uses of $\mathcal{O}$. Give your answers in words or pseudocode.

a) (20 points) Given 3 possible input-output pairs from the box $((N_1, g_1, y_1), x_1)$, $((N_2, g_2, y_2), x_2)$, and $((N_3, g_3, y_3), x_3)$, give an algorithm (minimizing uses of $\mathcal{O}$), to determine if indeed $g_i^{x_i} = y_i \bmod N_i$ for all i. How many times did you use $\mathcal{O}$?

b) (20 points) You witness Alice and Bob use Diffie-Hellman once, using p as the modulus and g as the base, with Alice announcing $A = g^a \bmod p$ and Bob announcing $B = g^b \bmod p$. Give an algorithm (minimizing uses of $\mathcal{O}$) to find $k = A^b = B^a \bmod p$. How many times did you use $\mathcal{O}$?

c) (20 points) You are given $(N, g, a, b, \{c_i\}, \{d_i\})$ with $g, a, b \in \mathbb{Z}_N^*$, $c_i, d_i < N$, and i ranging from 1 to 10. g is a generator of $\mathbb{Z}_N^*$. That is, there are 10 pairs (c_i, d_i) but the same (N, g, a, b) for all pairs. Give an algorithm (minimizing uses of $\mathcal{O}$) to find integers $\{x_i\}$ for all i such that $g^{x_i} = a^{c_i} b^{d_i} \bmod N$. How many times did you use $\mathcal{O}$?

d) (20 points) You are given (N, g, r, y, y') with $r = \mathrm{ord}(g)$ odd. Give an algorithm (minimizing uses of $\mathcal{O}$) to find integer x such that $y = g^{x+x'} \bmod N$ and $y' = g^{x-x'} \bmod N$. How many times did you use $\mathcal{O}$? What happens if r is even? Can you get the algorithm to work then?