Cryptography ENEE/CMSC/MATH 456: Homework 8

Due by 2pm on 5/3/2023.

1. The public exponent e in RSA can be chosen arbitrarily, subject to $gcd(e, \phi(N)) = 1$. Popular choices of e include $e = 3$ and $e = 2^{16} + 1$. Explain why such e are preferable to a random value of the same length.
   Hint: Look at the algorithm for modular exponentiation given in the lecture notes.

2. Prove formally that the hardness of the CDH problem relative to G implies the hardness of the discrete logarithm problem relative to G.

3. Can the following problem be solved in polynomial time? Given a prime p, a value $x \in Z_{p-1}^*$ and $y := g^x \mod p$ (where g is a uniform value in Z_p^*), find g, i.e., compute $y^{1/x} \mod p$. If your answer is "yes," give a polynomial-time algorithm. If your answer is "no," show a reduction to one of the assumptions introduced in this chapter.

4. Describe in detail a man-in-the-middle attack on the Diffie-Hellman key-exchange protocol whereby the adversary ends up sharing a key k_A with Alice and a different key k_B with Bob, and Alice and Bob cannot detect that anything has gone wrong.

   What happens if Alice and Bob try to detect the presence of a man-in-the-middle adversary by sending each other (encrypted) questions that only the other party would know how to answer?

5. Consider the following key-exchange protocol:

   Common input: The security parameter 1^n.
   (a) Alice runs $\mathcal{G}(1^n)$ to obtain (G, q, g).
   (b) Alice chooses $x_1, x_2 \leftarrow Z_q$ and sends $\alpha = x_1 + x_2$ to Bob.
   (c) Bob chooses $x_3 \leftarrow Z_q$ and sends $h_2 = g^{x_3}$ to Alice.
   (d) Alice sends $h_3 = g^{x_2 \cdot x_3}$ to Bob.
   (e) Alice outputs $h_2^{x_1}$. Bob outputs $(g^\alpha)^{x_3} \cdot (h_3)^{-1}$.
   Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).