Introduction to Cryptology ENEE459E/CMSC498R: Homework 9

Due by *midnight* on 5/1/2018.

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. Determine the points on the elliptic curve $E : y^2 = x^3 + 2x + 1$ over Z_{11}. How many points are on this curve?

4. 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.