1. Use the Miller-Rabin test to determine if the following values are prime or composite. How confident are you in your answers?

   (a) $n = 2^{1341} - 19$ (b) $n = 2^{1279} - 1$

2. Your goal is to find a 20-bit pseudoprime number n
   (a) How many 20-bit numbers do you expect that you will need to pick, on average, before finding a prime?
   Hint: Remember the Prime Number Theorem?
   (b) Find a 20-bit pseudoprime.
   How confident are you that your n is a pseudoprime?

   You may use Mathematica's RandomInteger[ ] command, but NOT the RandomPrime[ ] command. That would be cheesy.

3. Generate a desirable pair (p, α) for use with Diffie-Hellman Key Exchange where p is a 20-bit prime. Repeat where p is a 200-bit prime.