Name:_____

Introduction to Cryptography
Diffie-Hellman Key Exchange

(1) Suppose we know integers a, c, and n satisfying $c \equiv a^b \mod n$ for some unknown integer exponent b. Finding the value of b is known as the **Discrete Logarithm**. Use Python to find b in each of the following equations. Record the run-time for each of the computations.
   (a) $7 \equiv 5^b \mod 37$
   (b) $7 \equiv 5^b \mod 157$
   (c) $7 \equiv 5^b \mod 1607$
   (d) $7 \equiv 5^b \mod 15287$
   (e) $7 \equiv 5^b \mod 150053$
   (f) $7 \equiv 5^b \mod 1500043$

(2) Use Desmos or a calculator to plot the computation time as a function of the answer b that you found in each part of the previous problem. Using an appropriate regression line, approximate how long it would take to solve $7 \equiv 5^b \mod n$ if $b < n$ and b had 100 digits.

(3) Suppose Alice and Bob want to use Diffie-Hellman to agree upon a key which will be used to encode a secret message. Suppose they (publicly) agree to use the prime 1500043 and the primitive root 5.
   (a) Verify that 5 is indeed a primitive root of 1500043.
   (b) If Alice uses the exponent $a = 1234567$, what is the public key they send to Bob?
   (c) If Bob uses the exponent $b = 1010101$, what is the public key they send to Alice?
   (d) Using what is known to Alice, compute the secret key.
   (e) Using what is known to Bob, compute the secret key.

(4) Suppose Alice and Bob want to use Diffie-Hellman to agree upon a key which will be used to encode a secret message. Suppose they (publicly) agree to use the prime p and the primitive root a. Suppose also that Alice's public key and Bob's public key are intercepted by Eve the eavesdropper. If Eve now pretends to be Bob when communicating with Alice, and Eve pretends to be Alice when communicating with Bob, how can Eve ensure that they can decrypt the secret messages between Alice and Bob without either Alice or Bob knowing? This is called the **Man-in-the-Middle attack**.

(5) Suppose three individuals want to use Diffie-Hellman to agree upon a key which will be used to encode secret messages. Suppose they (publicly) agree to use the prime p and the primitive root a. If each individual chooses their own secret exponent, explain how to modify Diffie-Hellman so that they all can agree on a secret key.