Name: ______________________________

Directions: Show all work. No credit for answers without work.

1. **[10 points]** Find a primitive root modulo 7. Show work that verifies your selection is a primitive root.

2. **[5 points]** Let m and n be large integers. Suppose that $2^{m-1} \equiv 1 \pmod{m}$ and $2^{n-1} \equiv 4 \pmod{n}$. What, if anything, can you conclude about whether m and/or n is prime, and why?

3. **[3 parts, 4 points each]** Short Answer (no need to show work on this problem). Let p be an odd prime and let g be a primitive root in $\mathbb{F}_p$.

   (a) How many primitive roots are there in $\mathbb{F}_p$?

   (b) What is the order of g in $\mathbb{F}_p$?

   (c) What is the order of g^2 in $\mathbb{F}_p$?

4. Alice and Bob use the multiplication symmetric cipher with prime $p = 421$ and $\mathcal{K} = \mathcal{M} = \mathcal{C} = \mathbb{F}_p^*$. Recall that the encryption function is given by $e_k(m) = km$. They choose the key $k = 182$.

   (a) [**5 points**] Alice wishes to send the message $m = 282$ to Bob. What is the corresponding cipher text?

   (b) [**10 points**] Alice receives the ciphertext $c = 296$ in response. What is the corresponding plaintext message?

   (c) [**5 points**] How many plaintext/ciphertext pairs does Eve need to compute the shared key? Explain.

5. [**5 points**] Alice and Bob switch to the Exclusive-OR cipher with key $k = 01100101$. Alice receives the ciphertext $c = 00101110$. What is the corresponding plaintext?

6. **[2 parts, 12 points each]** Alice and Bob use the ElGamal cipher, with $p = 59$ and $g = 11$.

   (a) Alice picks $a = 17$ as her private key and in $\mathbb{F}_p$ computes $A = g^a = (11)^{17} = 14$ as her public key. Bob wishes to send to Alice the message $m = 40$ and picks the random element 8. What does Bob send to Alice?

   (b) Bob sends a second encrypted message to Alice with ciphertext $(c_1, c_2) = (39, 5)$. Help Alice decrypt Bob's message.

7. Let $p = 179$ and let $g = 3$. We use Shanks's baby-step/giant-step algorithm to compute $\log_g(4)$ in $\mathbb{F}_p$. Note that g has order 89 in $\mathbb{F}_p$, and we may take $n = 1 + \lfloor\sqrt{89}\rfloor = 10$.

   (a) [**8 points**] Compute List 1 (the baby-steps).

   (b) [**12 points**] Compute List 2 (the giant-steps).

   (c) [**4 points**] If it exists, find $\log_g(4)$.