Name: ______________________________

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

1. **[12 points]** Let $p = 409$ and note that p is prime. Use the fast power algorithm to compute $(219)^{81}$ in $\mathbb{F}_p$.

2. **[2 parts, 7 points each]** Let $p = 269$ and note that p is a prime.

   (a) What are the possible orders of elements in $\mathbb{F}_p$?

   (b) Suppose that g is a primitive root in $\mathbb{F}_p$ and $g^a = g^b$ for some some integers a and b. What can we conclude about a and b?

3. **[7 points]** Alice and Bob switch to the Exclusive-OR cipher with key $k = 100110$. Alice receives the ciphertext $c = 111000$. What is the corresponding plaintext?

4. **[7 points]** Let $p = 19$. Compute $\log_3(7)$.

5. **[2 parts, 6 points each]** Alice and Bob use the Diffie Hellman secret key exchange protocol. They select $p = 587$ and $g = 2$. The following table of powers in $\mathbb{F}_p$ may be helpful.

n	1	2	4	8	16	32	64	128	256	512
$(2)^n$	2	4	16	256	379	413	339	456	138	260
$(184)^n$	184	397	293	147	477	360	460	280	329	233
$(417)^n$	417	137	572	225	143	491	411	452	28	197

(a) Bob chooses private number $b = 184$. What should he send to Alice?

(b) Bob receives $A = 417$ from Alice. What is their shared secret key?

6. **[2 parts, 12 points each]** Alice and Bob use the ElGamal cipher, with $p = 227$ and $g = 5$. Alice picks $a = 28$ as her private key and in $\mathbb{F}_p$ computes $A = g^a = 49$ as her public key. Bob picks $b = 77$ as his private key and computes $B = g^b = 106$. The following table of powers in $\mathbb{F}_p$ may be helpful.

n	1	2	4	8	16	32	64	128
$(5)^n$	5	25	171	185	175	207	173	192
$(28)^n$	28	103	167	195	116	63	110	69
$(30)^n$	30	219	64	10	100	12	144	79
$(49)^n$	49	131	136	109	77	27	48	34
$(71)^n$	71	47	166	89	203	122	129	70
$(77)^n$	77	27	48	34	21	214	169	186
$(84)^n$	84	19	134	23	75	177	3	9
$(101)^n$	101	213	196	53	85	188	159	84
$(106)^n$	106	113	57	71	47	166	89	203

(a) Alice wishes to send Bob the message $m = 30$ and picks the random element $t = 84$. Using only information available to Alice, what does Alice send to Bob?

(b) Bob sends the ciphertext $(c_1, c_2) = (71, 100)$. Help Alice decrypt Bob's message.

7. Let $p = 167$ and let $g = 24$. We use Shanks's baby-step/giant-step algorithm to compute $\log_g(7)$ in $\mathbb{F}_p$. Note that g has order 83 in $\mathbb{F}_p$, and we may take $n = 1 + \lfloor\sqrt{83}\rfloor = 10$.

   (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 $\log_g(7)$.