Name:		
i tallic.		

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

1. [1 point] Describe the Diffie-Hellman Problem (DHP). What are the inputs to DHP? What is the output to be computed?

- 2. [2 parts, 2 points each] Alice and Bob use ElGamal with p = 83 and g = 2.
 - (a) Alice wishes to generate a private/public key pair. She selects a=14 as her private key. What is her public key?

(b) Bob publishes B=55 as his public key. Alice wishes to send the message m=70 to Alice. She picks the ephemeral key k=10. What ciphertext should she send to Bob?

- 3. Let p=571 and g=4. Note that the order N of g in \mathbb{F}_{571} satisfies N=57. We wish to compute $\log_q(407)$.
 - (a) [2 points] Compute List 1 in Shanks's algorithm.

(b) [2 points] Compute List 2 in Shanks's algorithm. You may stop as soon as you detect a collision with List 1.

(c) [1 point] Use (a) and (b) to find $\log_g(407)$.