Name: Solutions

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?

Given p, g, g^a, and g^b, compute g^{ab}.

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?

$A = g^a = 2^{14} = (2^7)^2 = (128)^2$

$= (45)^2 = 2025$

$= \boxed{33}$

   (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?

$c_1 = g^k = 2^{10} = 1024 = 28$

$c_2 = m(B^k) = 70 \cdot (55)^{10}$.

$(55)^2 = 37$; $(55)^4 = (37)^2 = 41$ $(55)^5 = 55 \cdot 41 = 14$

$(55)^{10} = 14 \cdot 14 = 196 = 30$

$c_2 = 70 \cdot 30 = 2100 = 25$. So ciphertext is $\boxed{(28, 25)}$

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 $\log_g(407)$.

   (a) **[2 points]** Compute List 1 in Shanks's algorithm.

$n = \lceil \sqrt{N} \rceil = 8$; $g^n = 4^8 = 2^{16} = (2^8)^2 = (256)^2 = 442$

i	0	1	2	3	4	5	6	7	8
g^{8i}	1	442	82	271	443	524	353	143	396

   (b) **[2 points]** Compute List 2 in Shanks's algorithm. You may stop after finding a collision with list 1.

j	0	1	2	3	4	5	6	7
hg^j	407	486	231	353	270	509	323	150

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

We see $g^{8\cdot 6} = 353 = hg^3$, so

$h = g^{8\cdot 6 - 3} = g^{45}$. Therefore $\log_g(407) = \boxed{45}$.