Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. [JJJ 2.8] Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications using the ElGamal public key cryptosystem.

   (a) Alice chooses $a = 947$ as her private key. What is the value of her public key?

   (b) Bob chooses $b = 716$ as his private key, so his public key is $B = 2^{716} = 469$. Alice encrypts the message $m = 583$ using the ephemeral key $k = 887$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?

   (c) Alice decides to choose a new private key $a = 299$ with associated public key $A = 2^{299} = 34$. Bob encrypts a message using Alice's public key and sends her the ciphertext $(661, 1325)$. Decrypt the message.

   (d) Now Bob chooses a new private key and publishes the associated public key $B = 893$. Alice encrypts a message using this public key and sends the ciphertext $(693, 793)$ to Bob. Eve intercepts the transmission. Help Eve by solving the discrete logarithm problem $2^b \equiv 893 \pmod{1373}$ and use the value of b to decrypt the message.

2. In this problem, we modify the ElGamal public key cryptosystem to create a new cryptosystem called ElGamalAdd. Instead of multiplying the message m by the shared secret, this system adds m to the shared secret. Specifically, we publish a large prime p and a primitive root g in $\mathbb{F}_p$ of large prime order. The key space consists of all pairs $(k_{\text{priv}}, k_{\text{pub}})$ of the form (a, g^a) where $a \in \mathbb{F}_p^*$. The encryption function follows.

$e_{k_{\text{pub}}}(m)$, where k_{pub} has the form g^a:
Choose an ephemeral key k in $\mathbb{F}_p$ at random.
Compute $c_1 = g^k$ and $c_2 = m + (g^a)^k$.
Return (c_1, c_2)

   (a) What is the associated decryption function?

   (b) If Eve wishes to decrypt messages sent with the ElGamalAdd cryptosystem, she may want to solve the corresponding ElGamalAdd Problem, or EGAP. The EGAP problem is to compute m given the information $p, g, g^a, g^k, m + g^{ak}$ that is available to Eve. Prove that EGAP and the Diffie–Hellman Problem (DHP) have the same level of difficulty. **Note:** this means you must show (1) how a black box solution to DHP can be used to solve EGAP efficiently, and (2) how a black box solution to EGAP can be used to solve DHP efficiently.

   (c) In light of the result in part (b), discuss the relative strengths of the ElGamal and ElGamalAdd cryptosystems.

3. [JJJ 2.16] Decide whether each of the following are true or false.

   (a) $x^2 + \sqrt{x} \in O(x^2)$.

   (b) $k^{300} \in O(2^k)$.

   (c) $2^k \in O(e^k)$.

   (d) $e^k \in O(2^k)$.

   (e) $k^r \in O(e^{\sqrt{k}})$ for each positive real number r.

(f) $e^{\sqrt{k}} \in O(e^{rk})$ for each positive real number r.

4. Shanks's Algorithm. Let $p = 211$ and let $g = 8$.

   (a) Find the order N of g in $\mathbb{F}_p$.

   (b) Compute List 1 in Shanks's Algorithm for computing $\log_g(h)$.

   (c) Use Shanks's Algorithm to find each of the following discrete logarithms. In each case, explicitly give List 2.

      i. $\log_g(122)$

      ii. $\log_g(150)$

      iii. $\log_g(200)$