Name: ______________________________

Directions: Show all work, including fast power and extended Euclidean algorithm work, unless directed otherwise. No credit for answers without work.

1. Alice and Bob use the ElGamal cryptosystem to exchange messages with $p = 383$ and $g = 212$. Bob selects $b = 8$ as his private key and Alice publishes $A = 74$ as her public key.

   (a) **[10 points]** What is Bob's public key?

   (b) **[15 points]** Alice encrypts a message with Bob's public key and sends the ciphertext $(5, 211)$ to Bob. Find Alice's message to Bob.

2. **[5 points]** Place the following six functions in order so that if $f(x)$ proceeds $g(x)$, then $f(x) = O(g(x))$. You do not need to show your work.

$$x^2(\ln x)^5, x, e^x, x^5(\ln x)^2, \frac{1}{x}, 1$$

3. Use Shanks's Algorithm to find an x such that $2^x \equiv 120 \pmod{223}$.

   (a) **[8 points]** Compute List 1 from Shanks's Algorithm. Show details for your first two entries; no details needed for the others. Hint: the order of 2 in $\mathbb{F}_{223}$ is 37.

   (b) **[8 points]** Compute List 2 from Shanks's Algorithm. You may stop as soon as you detect a collision with List 1.

   (c) **[4 points]** Use (a) and (b) to find a solution x.

4. Let $M = 940$. Note that the prime factorization of M is $M = 2^2 \cdot 5 \cdot 47$.

   (a) **[5 points]** According to the Chinese Remainder Theorem (CRT), 812 in $\mathbb{Z}_M$ corresponds to a list (a, b, c) where $a \in \mathbb{Z}_4$, $b \in \mathbb{Z}_5$, and $c \in \mathbb{Z}_{47}$. What is this list?

   (b) **[20 points]** Solve the following system of congruences.

$$\begin{aligned} x &\equiv 2 \pmod{4} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 43 \pmod{47} \end{aligned}$$

5. **[10 points]** Let d and m be positive integers such that d divides m. Prove that if $a \equiv b \pmod{m}$, then $a \equiv b \pmod{d}$.

6. **[15 points]** Solve for x in $x^7 \equiv 2 \pmod{161}$. Hint: $161 = 7 \cdot 23$.