Midterm for MAT 708 Cryptography

There are 5 problems on the take-home portion of the midterm. You are to work on these by yourself - no collaboration of any kind is allowed. I am the only person you may ask for help. You may use notes or your text if you would like, but that is all.

I understand that I am not allowed to either give nor receive any unauthorized aid on this exam.

Signature _____

1. Find the discrete logarithm of 3 base 2 mod 125.
2. Users A and B use the Diffie-Hellman key exchange technique with a common prime $p = 71$ and primitive root $\alpha = 7$.
   (a) If user A has private key $X_A = 5$, what is A's public key Y_A?
   (b) If user B has private key $X_B = 12$, what is B's public key Y_B?
   (c) What is the shared secret key?
3. Consider an ElGamal scheme with a common prime $p = 71$ and a primitive root $\alpha = 7$.
   (a) If B has public key $Y_B = 3$ and A chose the random integer $k = 2$, what is the ciphertext of $M = 30$?
   (b) Now if A chooses a different value of k so that the encoding of $M = 30$ is $C = (59, C_2)$, what is the integer C_2?
4. An RSA cipher is set up with modulus 12091 and encryption key 3. The ciphertext is '9812'. Decrypt it (just as an integer, which we presume is encoded from text in some unknown and irrelevant manner).
5. It has been claimed that there is a "short cut" to finding the multiplicative inverse of $x \pmod n$ (when x and n are relatively prime). Let $\phi(n)$ denote the Euler's totient function (which equals the number of positive integers less than n that are relatively prime to n), then the multiplicative inverse to $x \pmod n$ is just $x^{(\phi(n)-1)} \pmod n$.
   (a) Calculate $\phi(26)$.
   (b) What are the multiplicative inverses of 3, 7 and 19 (*mod* 26) (just list them)?
   (c) Show that the formula above, $x^{-1} \pmod n \equiv x^{(\phi(n)-1)} \pmod n$, works for a = 3, 7, and 19 when $n = 26$.
   (d) Use the formula for $\phi(n)$ (based on the prime factorization of n) to calculate $\phi(100000)$.
   (e) Working mod 100000, and using your result from part (d), find the multiplicative inverse of 7(*mod* 100000).

The prime factorization formula for Euler's totient function is

$$\phi(n) = (p_1 - 1)p_1^{k_1-1} \times (p_2 - 1)p_2^{k_2-1} \times \cdots \times (p_r - 1)p_r^{k_r-1}$$

where

$$n = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_r^{k_r}.$$

This portion of the midterm is worth 75% of the grade for this exam. The other 25% you already earned when you found this portion of the midterm.

This set of problems is due by the beginning of class on Monday, June 10^{th}.