MATH 3094 - PRACTICE MIDTERM 1

YOUR NAME: _____

P1	P2	P3	P4	P5	Extra	Total

Show all your work. Explain all your answers. Do not use calculator programs.

Problem 1. (20 points) For each problem below, **explain** your steps to find the answer.

(1) (5 points) *Practice the fast powering algorithm, e.g.,* find an integer between 0 and 10 that is congruent to 5^{321} mod 11.

(2) (5 points) *Practice solving Bezout's identity, e.g.,* find integers x and y such that $7x + 47y = 1$ using Euclid's algorithm.

(3) (5 points) *Practice finding multiplicative inverses, e.g.,* find the multiplicative inverse of 7 mod 47.

(4) (5 points) *Practice finding negative powers of integers in modular arithmetic, e.g.,* find an integer between 0 and 10 that is congruent to 7^{-3} mod 11.

Problem 2. (20 points)

(1) *Practice encrypting and decrypting using Caesar/shift ciphers, e.g.,* let A through Z be encoded by 0 through 25 mod 26 (so that $A \equiv 0$, $B \equiv 1$, ..., $Z \equiv 25 \bmod 26$) and encrypt "MATH" using the shift cipher $e_3(\ell) \equiv \ell + 3 \bmod 26$.

(2) *Practice encrypting and decrypting using Caesar/shift ciphers, e.g.,* the word "SOJZKXS" was encrypted using a shift cipher, and you know that O corresponds to I. Decrypt the message.

(3) *Practice working with affine ciphers, e.g.,* let $e(m) \equiv 3 \cdot m + 3 \bmod 26$. Can this function be used as an affine cipher to encrypt the alphabet? If so, what is the decryption function $d(c)$?

(4) *Practice working with affine ciphers, e.g.,* let $e(m) \equiv 4 \cdot m + 4 \bmod 26$. Can this function be used as an affine cipher to encrypt the alphabet? If so, what is the decryption function $d(c)$?

Problem 3. (20 points)

(1) *Practice working with primitive roots, e.g.,* find **all** the primitive roots modulo 11.

(2) *Practice solving the DLP, e.g.,* find x such that $2^x \equiv 5 \bmod 11$.

(3) *Practice finding multiplicative orders, e.g.,* what is the multiplicative order of 2 mod 11? How about 4 mod 11?

(4) *Practice setting up a Diffie-Hellman key exchange, e.g.,* Alice and Bob want to communicate securely and first they will use Diffie-Hellman (DH) key exchange, using $p = 11$ and $g = 4$. Alice picks $a = 3$ and Bob picks $b = 2$ for their secret keys. What is the secret key K mod 11 that the DH algorithm produces?

Problem 4. (20 points) *Practice setting up and working with an Elgamal crypto system, e.g.,* set up an Elgamal system with $p = 13$, $g = 4$, and Alice's choice $a = 3$.

(1) First compute $A \equiv g^a \bmod p$.

(2) Then, encrypt the messages $m_1 = 7$ and $m_2 = 8$ using the Elgamal system you just set up.

Problem 5. (20 points) *Practice using Shank's baby-step giant-step algorithm, e.g.,* use Shank's baby-step giant-step algorithm to find x such that

$$2^x \equiv 3 \bmod 19.$$

(1) Find the order of 2 mod 19.

(2) Compute $n = 1 + \lfloor \sqrt{18} \rfloor$.

(3) Compute List 1: $1, g, g^2, \ldots, g^n \bmod 19$.

(4) Compute $u \equiv g^{-n} \bmod 19$.

(5) Compute List 2: $h, h \cdot u, h \cdot u^2, \ldots, h \cdot u^n \bmod 19$.

(6) Use the information above to finish the baby-step giant-step algorithm and find x such that $2^x \equiv 3 \bmod 19$.