MAT 302 Mid-term Checklist

♦ Do you know:

1. [**Groups**]: Groups $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$, and how to compute the Euler Totient Function $\phi(N)$, given the factorization of $N$?

2. [**Algorithms**]:
   - Euclid and Extended Euclid, application to computing inverses in $\mathbb{Z}_N^*$.
   - Exponentiation: how to compute $b^a \pmod{N}$ given $b, a$ and $N$? The “square and multiply” algorithm for exponentiation.
   - Finding Roots: how to find $b$ such that $b^a = c \pmod{N}$ given $a, c$ and $N$? How to find roots for prime and composite $N$.
   - Discrete Log: how to find $a$ such that $b^a = c \pmod{N}$ given $b, c$ and $N$? The baby step giant step algorithm and its complexity.
   - Primality Testing: The Fermat test, Carmichael Numbers and the Miller-Rabin test. The notions of Fermat witnesses and liars, and the proof that there aren’t too many Fermat liars mod $N$ where $N$ is composite and not Carmichael.
   - Finding generators for $\mathbb{Z}_p^*$.

3. [**Number Theory**]: Fermat’s Little theorem, Euler’s theorem, Lagrange’s theorem, Chinese Remainder theorem, $\mathbb{Z}_p^*$ is a cyclic group, the number of elements of order $d$ in $\mathbb{Z}_p^*$.

4. [**Cryptography**]:
   - Caesar cipher and the One-time pad.
   - Diffie-Hellman key exchange and El Gamal encryption.
   - RSA public-key encryption.

♦ You will have 100 minutes to solve about five problems.

♦ Most of the material is from the first three chapters of the book (until Sec. 3.4).

♦ Make sure to go over the problem sets and the midterm practice test. Do not hesitate to e-mail me if you have any questions.

♦ Most problems can be solved easily with a thorough understanding of the material presented in class. One of the problems will involve some amount of creativity and original problem solving.