Math 3375 Midterm Info Sheet

The purpose of this handout is to help you study by listing the concepts, definitions, and results you will need to know for the midterm.

Midterm Information. The midterm will be on Thursday Oct. 17, 2013 at 8:30AM. The midterm will take place in our regular class room and will be 75 minutes long. You will *not* be allowed to bring in any notes, use the text book, or use a calculator. Please bring your **Student Card**.

Material Covered. All the material discussed in class may appear on the midterm. The material that we covered was Chapters 1 and 2. Below, I have given a breakdown of what you will need to know from each section.

Section 1.1 You will need to know how to do a proof by induction. Also, know the well-ordering axiom.
Section 1.2 Know what it means for one number to divide another, and know the basic properties of division. Know what a prime number is. Know the division algorithm. Be able to use the Euclidean algorithm to find the greatest common divisor of two numbers. Also, know how to find x and y such such that $\gcd(a, b) = ax + by$.
Section 1.3 Know what it means for two numbers to be relatively prime, and know the Fundamental Theorem of Arithmetic.
Section 1.4 Know how to do computations involving modular arithmetic.
Section 1.5 Know the four basic mono-alphabetic substitution ciphers: additive, multiplicative, affine, and keyword. Be able to encrypt and decrypt a given message if you are given a suitable key.
Section 1.6 Know the various strategies for breaking mono-alphabetic substitution ciphers.
Section 2.1 You will need to know the multiplication principle.
Section 2.2 Know the difference between permutation and combination, and know their formulas.
Section 2.3 Know the basics of probability: experiment, sample space, event. Know how to determine the probability of an event, and know the properties of probability.
Section 2.4 Know what it means for two events to be independent and how to compute the expected number.
Section 2.5 You should know what is meant by a poly-alphabetic substitution cipher. You should know the two different methods discussed in class (changing letters to numbers, and the Vigenère Square). Be able to encrypt and decrypt using the Vigenère Square. Know how to apply the Kasiski Test. Know the formula for the Index of Coincidence (you don't need to know the formula for the length of the keyword). You should know what the value of the Index of Coincidence can tell you (e.g. see bottom of page 96).

If you have questions, please feel free to email me. Good luck!