Math 3375 Final Exam 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 final exam. You should use the previous handout from the midterm to help you with the material from Chapters 1 and 2.

Exam Information. The final exam will be on **WEDNESDAY, DECEMBER 11, 2013** from **1:00PM-4:00PM** in **RYAN BUILDING 2047**. You will *not* be allowed to bring in any notes, use the text book, or use a calculator. You will be expected to do all calculations by hand (I will use numbers for which this is possible). The information on the next page will be included with the exam. You must bring your **Student Card**.

Material Covered. All the material discussed in class may appear on the final. The material that we covered was Chapters 1 through 4. See the midterm review sheet for the breakdown of Chapters 1 and 2. Below, I have given a breakdown of what you will need to know from Chapters 3 and 4.

> **Section 3.1** Know what a polygraphic substitution cipher is, and how it differs from the ciphers of Chapter 1. Also know how to use a Playfair Square to encrypt and decrypt a message.
> **Section 3.2** Know how to find the inverse of a 2×2 matrix (mod 26, or modulo some other number). Know the basic matrix operations. Know how to solve a linear system of equations (also modulo 26, or modulo some other number). You do not need to know about the connection to geometrical transformations.
> **Section 3.3** Know Hill's encryption system. In particular, you should know how to encrypt and decrypt a message using this system. You should also know what keys are valid for Hill's encryption system.
> **Section 4.1** Know Euler's ϕ function. Of special importance is Lemma 4.7 and Euler's Theorem. Be able to compute $\phi(n)$ for a given integer. You should also know Fermat's Little Theorem and Euler's Corollary.
> **Section 4.2** You should know what a public-key encryption system is, and how it differs from a private-key encryption system. You should know the details of the RSA encryption system. In particular, given two primes p and q, you should be able to create a public-key and private-key from this information. You should also know how we compute numbers of the form $m^c \mod n$.
> **Section 4.3** You don't need to know the material of this section, i.e., you don't need to know the computer syntax. However, you should know how to set up the appropriate equations.
> **Section 4.4** From this section, you only need to know how signature authentication works, and how the Diffie-Hellman key exchange process works.

Exam Format. The exam will be out of 90 points (it is 10 pages long). The type of questions will be similar to the midterm. You will also be given some choice for some questions.

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

The following information will be included as part of the exam:

1. Numerical position of letters

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

2. Inverses modulo 26

$$
\begin{aligned}
1 \cdot 1 &\equiv 1 \pmod{26} & \qquad 3 \cdot 9 &\equiv 1 \pmod{26} \\
5 \cdot 21 &\equiv 1 \pmod{26} & \qquad 7 \cdot 15 &\equiv 1 \pmod{26} \\
9 \cdot 3 &\equiv 1 \pmod{26} & \qquad 11 \cdot 19 &\equiv 1 \pmod{26} \\
15 \cdot 7 &\equiv 1 \pmod{26} & \qquad 17 \cdot 23 &\equiv 1 \pmod{26} \\
19 \cdot 11 &\equiv 1 \pmod{26} & \qquad 21 \cdot 5 &\equiv 1 \pmod{26} \\
23 \cdot 17 &\equiv 1 \pmod{26} & \qquad 25 \cdot 25 &\equiv 1 \pmod{26}
\end{aligned}
$$