Math 135 (Summer 2006)
Review for Prelim #1

Chapter 1 Topics

- Know the historical contexts of the specific ciphers discussed in Chapter 1, with a special emphasis on the cryptosystems covered in class.
- Be able to encrypt and decrypt plaintext using any of the cryptosystems covered in class.
- Be able to distinguish among the categories of ciphers: simple substitution, transposition, monoalphabetic substitution, polyalphabetic substitution, steganography, symmetric, asymmetric, etc.
- Be able to use function notation to evaluate a function from a table of values, a verbal (or written) description, or a formula. Be able to compute compositions and inverses.

Chapter 2 Topics

- Understand the meaning of the notations $a \equiv b \pmod{m}$, $a = b \,\mathrm{MOD}\, m$, and $a = b \,\mathrm{DIV}\, m$.
- Be able to solve (for the smallest non-negative x) congruences such as $x \equiv -543 \pmod{67}$, $8x \equiv 6 \pmod{21}$ and $11x + 5 \equiv 11 \pmod{20}$.
- Be able to solve (for the smallest non-negative a and b) systems of equations such as

$$a + b \equiv 2 \pmod{36}$$

$$6a + b \equiv 3 \pmod{36}.$$

- Be able to encipher and decipher using modular arithmetic with affine ciphers (including the special cases of a shift cipher and a decimation cipher).
- Be able to encipher and decipher using a substitution alphabet mixed via a keyword, and using a substitution mixed via a columnar transposition. (That is, a monoalphabetic substitution where the cipher alphabet is generated by a keyword or a keyword columnar transposition.)
- Be able to encipher and decipher using a columnar transposition, or a keyword columnar transposition.
- Be able to apply the theorem on the existence of multiplicative inverses, and find multiplicative inverses for small moduli.
- Be able to perform a small-scale cryptanalysis on a substitution or transposition using frequency analysis (frequency charts provided) and/or a few hints.

Selected Review Problems

1. Encipher GEOMETRY using **(a)** a Caesar (+3) shift, **(b)** the Wheatstone-Playfair cipher on page 16, and **(c)** the ADFGVX cipher on page 21 (with the keyword MATH).

2. Use the Vigenère cipher to **(a)** encipher GEOMETRY using the keyword ANGLE, and **(b)** decipher WUXAYERTH using the keyword PUMPKIN.

3. Let $f(x) = (3x+5) \bmod 26$ and let $g(x) = (5x+1) \bmod 26$. Determine **(a)** $f^{-1}(x)$, and **(b)** $f(g(x))$.

4. Without actually determining the solution, explain why the congruence $7x \equiv 1 \pmod{481}$ must have a solution.

5. Let $P(x)$ be the function that assigns to a given letter in a string x the pair of letters determined by the following table:

	V	W	X	Y	Z
V	E	S	P	Q	R
W	D	F	M	N	O
X	C	T	G	K	L
Y	B	U	V	H	Z
Z	A	W	X	Y	I

(Regard any J in a string as an I.) For example, $P(\texttt{M}) = \texttt{WX}$ and $P(\texttt{PHONE}) = \texttt{VX YY WZ WY VV}$. **(a)** What is the domain of the function P? **(c)** What is the range of the function P? **(d)** Is the function P one-to-one? **(e)** If P is one-to-one, describe its inverse P^{-1} and evaluate $P^{-1}(\texttt{ZZ WY XW VV VZ WY VV XW})$. If P is not one-to-one, give an example to show this.

6. The two ciphertexts

HSZIR MTRHH LNVGR NVHNL IVWVN TGSZM TRERM T

and

SISEE RMIHI GHNST SEANA VAGOI MDNGN IRIMM OEDTG N

came from the same plaintexts. One of the ciphertexts came from a monoalphabetic substitution, and the other came from a simple columnar substitution. Explain which is which. Find the plaintext.

7. The string SUCCESS was part of the plaintext that produced the ciphertext

TSEKC OGEIC HUDEE NNCLU SICSS S

using a keyword columnar transposition. Find the plaintext.

8. (Bonus) Suppose that m and p are distinct prime numbers. (That is, m and p are each prime, and $m \neq p$.) Suppose further that $a \equiv b \pmod{m}$ and that $a \equiv b \pmod{p}$. Prove that $a \equiv b \pmod{mp}$.