Math 124 Winter 2009
Assignment #6

This assignment is due at the beginning of class on Tuesday, April 7, 2009. Late assignments will not be accepted. You must submit solutions to all problems.

YOUR ASSIGNMENT MUST BE STAPLED AND PROBLEM NUMBERS CLEARLY LABELLED. UNSTAPLED ASSIGNMENTS WILL NOT BE ACCEPTED! DO NOT CROWD YOUR WORK. DO NOT WRITE IN MULTIPLE COLUMNS.

1. Find the greatest common divisor of 4961 and 4235.

2. The number 1074967 is a product of two distinct primes. At most, how many trial divisions by primes will be required to find these primes? (Consult the primes table to answer this question.)

3. Use Fermat's Little Theorem/Euler's Theorem to help to compute 3^{147} MOD 95.

4. Suppose that Alicia is implementing RSA with primes $p = 53$, $q = 31$, and public exponent $e = 17$.

(a) Explain what she does to set up for receiving encrypted messages and calculate all of the numbers that she will use with these choices of p, q, and e.

(b) If Roberto wants to send Alicia the message $x = 224$ encrypted using her public key, determine the ciphertext he produces.

(c) Suppose Alicia receives the encrypted message $y = 775$. Write down the expression that she will need to evaluate in order to decrypt. (Do not actually evaluate this expression.)

(d) Use an online calculator to compute the answer to **(c)**.

5. OMIT.

6.

(a) Find the base ten representation of the number with base two representation 101001000.

(b) Find the base two representation of 83 (base ten).

(c) Find the base ten representation of the number with base twenty-six representation ZAP.

(d) Write the base twenty-six representations for the five numbers following the number with base twenty-six representation NIGHT.

(e) How many digits are in the base two representation of the number 25^{3829}?

(f) Find the base ten representation of the number with base eight representation 76341.

7. 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`).

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

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

10. The two ciphertexts

```
HSZIR MTRHH LNVGR NVHNL IVWVN ZMWRM 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 transposition. Explain which is which. Find the plaintext.

11. 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.

12. (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 $a \equiv b \pmod{mp}$.