Math 5248 Cryptology and number theory
Fall 2005, Vic Reiner
Midterm exam 1- Due Wednesday October 12, in class

Instructions: This is an open book, open library, open notes, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult. Explain your reasoning- answers without justification or proof (where appropriate) will receive **no credit**.

1. (20 points) Solve the following simultaneous system of equations in $\mathbb{Z}/2431$ for the unknown values $a, b \in \mathbb{Z}/2431$. Show all of your work, including any steps involved in computing multiplicative inverses.

$$\overline{33}a + b = \overline{100}$$
$$\overline{2}a + b = \overline{7}.$$

2. (15 points) Assume that n, m are two positive integers, neither of which is a multiple of the other, and let $d = GCD(n, m)$. Show that there is an expression $d = xn + ym$ in which x, y are integers *with opposite signs*, that is, neither x nor y is zero, and exactly one out of the two is positive, the other negative.

3. (17 points total) The goal of this problem is to understand why one insists that $\overline{a} \in (\mathbb{Z}/26)^{\times}$ in the key (a, b) for the affine cipher. Recall that the encoding function is $E_{a,b}(x) = (ax + b)\%26$.

(a) (12 points) Show that if $\overline{a} \notin (\mathbb{Z}/26)^{\times}$, there will always exist at least two distinct elements $\overline{x}, \overline{y}$ of $\mathbb{Z}/26$ for which $E_{a,b}(x) = E_{a,b}(y)$. (Hint: If $a = 0$, can you say which x, y get mapped to the same value by $E_{a,b}$? What about if a is even? What about if $a = 13$?)

(b) (5 points) Explain why this is undesirable.

4. (15 points) How large would the keyspace be for the affine cipher if we used the Hawaiian alphabet with 13 letters, rather than the English alphabet with 26? In other words, how many diferent keys (a, b) are possible, if we insist that a, b lie in $\{0, 1, \ldots, 12\}$, that a has a multiplicative inverse mod 13, and that $(a, b) \neq (1, 0)$?

5. (18 points) The Hawaiian alphabet has the letters and (approximate) letter frequencies shown here as percentages:

a	e	i	o	u	$'$
26	7	9	11	6	7

h	k	l	m	n	p	w
4	11	4	3	8	3	1.

Assume y, y' are two strings of "Hawaiian gibberish" of the same length N, that is, they are each produced by picking letters from the Hawaiian alphabet at random, independently, with the above frequencies. What is the expected value of their *index of coincidence* $I(y, y')$?

6. (15 points) Assuming n is a positive *even* integer, compute

$$GCD(n + 2, n^2 + 4n + 6).$$

(Hint: If you've got no clue where else to start, try computing this GCD for the first few values of n, namely $n = 2, 4, 6, ...$)