MATH/CMSC 456 (Washington) Exam 1 March 10, 2005

Use 6 pages. Do a separate problem on each page. Write your name on each page. Do not staple.

1. (25 points = 15+10) (a) In order to use extra symbols in the message, a message is encrypted using an affine cipher mod 39 with the function $y \equiv 5x + 2 \pmod{39}$. Find the decryption function.
(b) Suppose you try to use the encryption function $y \equiv 13x + 2 \pmod{39}$. Find two distinct plaintext letters x_1 and x_2 such both x_1 and x_2 encrypt to the same ciphertext letter (that is, their encryptions satisfy $y_1 = y_2$).

2. (18 points = 9+9) Suppose there is a language that has only the letters a and b. The frequency of the letter a is .1 and the frequency of b is .9. A message is encrypted using a Vigenère cipher (working mod 2 instead of mod 26). The ciphertext is BABABAAABA.
(a) Suppose you know that the key length is 1, 2, or 3. Show that the key length is probably 2.
(b) Using the information on the frequencies of the letters, determine the key and decrypt the message.

3. (12) Suppose you modify the LFSR method to work mod 5 and you use a (not quite linear) recurrence relation

$$x_{n+2} \equiv c_0 x_n + c_1 x_{n+1} + 2 \pmod{5}, \qquad x_1 = 0, x_2 = 1, x_3 = 1, x_4 = 0.$$

Find the coefficients c_0 and c_1.

4. (18 points) Let $n = 3837523$. Bob Square Messages sends and receives only messages m such that m is a square mod n and $\gcd(m, n) = 1$. It can be shown that $m^{958230} \equiv 1 \pmod{n}$ for such messages (even though $\phi(n) \neq 958230$). Bob chooses d and e satisfying $de \equiv 1 \pmod{958230}$. Show that if Alice sends Bob a ciphertext $c \equiv m^e \pmod{n}$ (where m is a square mod n, and $\gcd(m, n) = 1$), then Bob can decrypt by computing $c^d \pmod{n}$. Explain your reasoning.

5. (15 points) Suppose you want to factor an integer n. You have found some integers x_1, x_2, x_3, x_4 such that

$$x_1^2 \equiv 2 \cdot 3 \cdot 7 \pmod{n}, \qquad x_2^2 \equiv 3 \cdot 5 \cdot 7 \pmod{n}$$

$$x_3^2 \equiv 3^9 \pmod{n}, \qquad x_4^2 \equiv 2 \cdot 7 \pmod{n}.$$

Describe how you might be able to use this information to factor n? Why might the method fail?

6. (12 points) You are appearing on the Math Superstars Show and, for the final question, you are given a 500-digit number n and are asked to guess whether or not it is prime. You are told that n is either prime or the product of a 200-digit prime and a 300-digit prime.You have one minute, and fortunately you have a computer. How would you make a guess that's very probably correct? Name any theorems that you are using.