HW 6 CMSC 389. DUE Jan 13

1. (0 points) READ my NOTES on line. (Still the notes on ciphers, though they have been updated.) What is your name? Write it clearly. IMPORTANT- READ the notes on the repeated squaring method to make calculation of a^n mod p EASY. You will need it for this HW, the last problem.

2. (25 points) Alice and Bob are going to use a Faux-1-time-pad. They are going to agree on a fraction that is < 1, expand it out in decimal as $0.d_1d_2d_3\ldots$ and then let $b_i = d_i \pmod 2$. Then $b_1b_2\cdots$ will be their key. For example, if the fraction is $1/3 = 0.33333\ldots$. then their key is $1111\ldots$. Another example: if the fraction is $1/4 = 0.2500000\ldots$ then their key is $01000000000\ldots$.

   (a) If Alice and Bob use 1/6 for their fraction then How would they encode 11010101000010101?

   (b) If Alice and Bob use 1/7 for their fraction then How would they encode 11010101000010101?

   (c) Which Faux-1-time-pad is better to use?

3. (25 points) Dr. Dogz is looking at the following problem: given n, find a prime in $[n, 2n]$. He wants to cut down the search by NOT looking at candidates that are divisible by 2 OR 3 OR 5 OR 7. Write down an algorithm that does this (you can assume that there already is an algorithm for testing primality).

4. (25 points) Dr. Dogz is looking at the following problem: given n, find is a SAFE prime in $[n, 2n]$. (That is, a prime p such that $\frac{p1}{2}$ is prime.) He wants to speed it up be only looking at p such that (1) p is is not divisibley by 2 OR 3 AND (2) $\frac{p-1}{2}$ is not divisible by 2 OR 3. write down an algorithm that does this (you can assume that there already is an algorithm for testing primality).

5. (25 points) Note that 47 is a safe primes since $\frac{47-1}{2} = 23$ which is prime. Test $2, 3, 4, 5, 6$ to see if they are generators. Show all work. (HINT- you will need to be able to take powers of numbers fast, so use the repeated squaring method.)