HW 5 CMSC 456. Morally DUE Oct 7
NOTE- THE HW IS FOUR PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. What is your name? What is the day and time of the midterm?

2. (20 points)

   (a) (20 points) Alice wants to find safe primes. She will, as usual, pick a random string of bits and test. She wants to make sure that if she tests p, then p is NOT even but ALSO $\frac{p-1}{2}$ is NOT even. How can she do this? Give pseudocode that will, given L, generate an arbitrary L bit number (it can be off by 1) such that if the number is p then both p and $\frac{p-1}{2}$ are odd.

   (b) (0 points) Think about how Alice can also make sure that p and $\frac{p-1}{2}$ are not divisible by 3.

3. (20 points)

   (a) (20 points) A *Saadiq Prime* is a prime p such that either $p-1 = 2q$ where q is a prime OR $p - 1 = 6q$ where q is a prime. Give psuedocode for an EFFICIENT algorithm for the following: given a prime that you are promised is a Saadiq prime, find a generator for $\mathbb{Z}_p^*$.

   (b) (0 points) Think about: Usually we look for a safe prime, and once we have it, we look for a generator. What is a PRO of instead looking for a Saadiq prime and then looking for a generator? What is a CON of doing so?

   (c) (0 points) Think about how we may generalize the notion of Saadiq prime and how useful that would be.

GOTO NEXT PAGE FOR NEXT PROBLEM

4. (20 points)

   For each $x \geq 1$,

   - Let $f(x)$ denote the number of primes $\leq x$
   - Let $g(x)$ denote the number of safe primes $\leq x$.
   - Let $h(x)$ denote the number of Saadiq primes $\leq x$.

   And now for the actual problem

   (a) (5 points) Give a table of the values $f(x)$, $g(x)$, and $h(x)$ for $x = 1000, 2000, \ldots, 10000$. Your data does not need to be 100% correct, but should be very close. (*Hint*: consider modifying your code from the previous programming assignment.)

   (b) (5 points) Find A, B so that $f(x) \approx \frac{Ax}{\ln x} + B$ fits the data pretty well. Sample x at every multiple of 100 up to 10000. (Recall that $\ln x$ is the natural log of x.)

   (c) (5 points) Find A, B so that $g(x) \approx \frac{Ax}{\ln x} + B$ fits the data pretty well. Sample x at every multiple of 100 up to 10000.

   (d) (5 points) Find A, B so that $h(x) \approx \frac{Ax}{\ln x} + B$ fits the data pretty well. Sample x at every multiple of 100 up to 10000.

GOTO NEXT PAGE

5. (25 points) Alice and Bob are going to do El Gamal with $p = 89$ and $g = 30$.

   (a) (5 points) Alice picks $a = 3$ and Bob picks $b = 6$. What is the shared secret key s that they need to begin doing El Gamal?

   (b) (5 points) Alice wants to send the message 43. What does she send? We will call what she sends c_{43} for later.

   (c) (5 points) Alice wants to send the message 26. What does she send? We will call what she sends c_{26} for later.

   (d) (5 points) Alice wants to send the message 69. What does she send? We will call what she sends c_{69} for later.

   (e) (5 points) If you did the problems above correctly then you will note that $c_{43} + c_{26} \equiv c_{69} \pmod{89}$. Also note that $43 + 26 = 69$. Is this a coincidence? Explain.

GOTO NEXT PAGE

6. (15 points) Compute the following and show your work. (You may use a calculator for simple operations such as multiplication.)

   (a) (5 points) $7^{999,999,999,999,999} \pmod{100}$

   (b) (5 points) $7^{999,999,999,999,999} \pmod{101}$

   (c) (5 points) $7^{999,999,999,999,999} \pmod{102}$