HW 5 CMSC 456. Morally DUE Oct 7
SOLUTIONS
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.

SOLUTION TO PROBLEM TWO

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 arbitrary an 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.

ANSWER:

We want to know when $\frac{p-1}{2}$ is odd. Hence we need to know when there exists x such that $\frac{p-1}{2} = 2x + 1$. Simple Algebra reveals $p = 4x + 3$.

We now give two ways to do this.

Method One: Similar to What We've done in Class:

(a) Input L.

(b) Generate y, a string of length $L - 3$.

(c) Let $x = 1y$ (append 1 to the beginning of y). Note that x is $L-2$ bits.

(d) Output $4x + 3$. Note that since x is $L - 2$ bits, $4x$ is L bits, so $4x + 3$ is L bits also.

Another way to write this (which TA Justin came up with). A number is of the form $4x + 3$ iff the last two bits in binary are 1.

Method Two: Justin's Method

(a) Input L.

(b) Generate y, a string of length $L - 3$.

(c) Let $x = 1y11$

(d) Output x.

END OF SOLUTION TO PROBLEM TWO

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.

SOLUTION TO PROBLEM THREE

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 $\mathbb{Z}_p^*$.

ANSWER: Recall that g is not a gen if there exists a positive factor f of $p-1$, $f \neq p-1$, such that $g^f \equiv 1 \pmod{p}$. If $p-1 = 6q$ there just are not that many factors.

(a) Input p. We know that either $p-1 = 2q$ where q is prime or $p-1 = 6q$ where q is prime.

(b) Factor $p-1$. This is EASY: divide $p-1$ by 2 to get $p-1 = 2r$. Then try to divide r by 3. You will succeed or not, but that's it! Let F be the set of all positive factors of $p-1$ (except $p-1$ and 1). Note that F will have ≤ 6 elements.

(c) For $g = 2$ to $p-2$ do the following:

   i. For all $f \in F$ compute $g^f \pmod{p}$.

   ii. If any of them =1 then goto the next g.

   iii. If none of them =1 then output g and halt.

END OF SOLUTION TO PROBLEM THREE

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.

SOLUTION TO PROBLEM FOUR

Omitted

END OF SOLUTION TO PROBLEM FOUR

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.

SOLUTION TO PROBLEM FIVE

All arithmetic is mod 89.

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

ANSWER: $30^{3\times 6} \equiv 5$. So the secret key is 5. Gee, not much of a secret if I know it :-)

(b) Alice wants to send the message 43. What does she send?

ANSWER: Alice sends $43 \times 5 \equiv 37$.

(c) Alice wants to send the message 26. What does she send?

ANSWER: Alice sends $26 \times 5 \equiv 41$.

(d) Alice wants to send the message 69. What does she send?

ANSWER: Alice sends $69 \times 5 \equiv 78$

(e) Omitted.

END OF SOLUTION TO PROBLEM FIVE

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) $7^{999,999,999,999,999} \pmod{102}$

SOLUTION TO PROBLEM SIX

We just do the first one completely. The other two we just begin.

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

ANSWER: We need $\phi(100)$. This is

$$\phi(100) = \phi(2^2 \times 5^2) = \phi(2^2)\phi(5^2) = (2^2-2)(5^2-5) = 2 \times 20 = 40$$

$$7^{999,999,999,999,999} \equiv 7^{999,999,999,999 \bmod 40} \pmod{100} \equiv 7^{39} \pmod{100}$$

We need 39 as a sum of powers of 2.
The highest power of 2 that is not > 39 is $2^5 = 32$

$$39 = 2^5 + 7$$

The highest power of 2 that is not > 7 is $2^2 = 4$

$$39 = 2^5 + 2^2 + 3$$

The highest power of 2 that is not > 3 is $2^1 = 2$

$$39 = 2^5 + 2^2 + 2^1 + 1$$

The highest power of 2 that is not > 1 is $2^0 = 1$. OH, we're done!

$$39 = 2^5 + 2^2 + 2^1 + 2^0$$

All $\equiv$ are mod 100.
$7^0 \equiv 1$
$7^{2^0} \equiv 7$
$7^{2^1} \equiv (7^{2^0})^2 \equiv 7^2 \equiv 49$
$7^{2^2} \equiv (7^{2^1})^2 \equiv 49^2 \equiv 1$
$7^{2^3} \equiv (7^{2^2})^2 \equiv 1^2 \equiv 1$
$7^{2^4} \equiv (7^{2^3})^2 \equiv 1^2 \equiv 1$
$7^{2^5} \equiv (7^{2^4})^2 \equiv 1^2 \equiv 1$

$$7^{39} \equiv 7^{2^5} \times 7^{2^2} \times 7^{2^1} \times 7^{2^0} \equiv 1 \times 49 \times 7 \equiv 43$$

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

Use $\phi(101) = 100$.

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

Use $\phi(102) = \phi(2 \times 3 \times 17) = 1 \times 2 \times 16 = 32$.

END OF SOLUTION TO PROBLEM SIX