HW 3 CMSC 456. DUE Oct 1
SOLUTIONS
NOTE- THE HW IS THREE PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. READ my NOTES on ciphers- the Diffie Helman and RSA part. What is your name? Write it clearly. What is the day and time of the first midterm?

2. (10 points) Do the following using the repeated squaring method. Show your work.

   (a) $14^{26} \pmod{1000}$

   (b) $30^{14} \pmod{1000}$

   SOLUTION TO PROBLEM TWO All $\equiv$ are mod 1000.

   a)

   $14^{2^0} \equiv 14$

   $14^{2^1} \equiv ((14^{2^0})^2 \equiv 196$

   $14^{2^2} \equiv ((14^{2^1})^2 \equiv 196^2 \equiv 38416 \equiv 416$

   $14^{2^3} \equiv ((14^{2^2})^2 \equiv 416^2 \equiv 173056 \equiv 56$

   $14^{2^4} \equiv ((14^{2^3})^2 \equiv 56^2 \equiv 3136 \equiv 136$

   We write 26 as a sum of powers of 2: $26 = 2^4 + 2^3 + 2^1$.

   Hence

   $$14^{30} \equiv 14^{2^4} \times 14^{2^3} \times 14^{2^1} \equiv (136 \times 56) \times 196 \equiv 7616 \times 196 \equiv 616 \times 196 \equiv 120736 \equiv 736.$$

   b)

   $30^{2^0} \equiv 30$

   $30^{2^1} \equiv 900$

   $30^{2^2} \equiv ((30^{2^1})^2 \equiv 900^2 \equiv (-100)^2 \equiv 0$

   the remaining powers of 30 are all 0.

   so the answer is 0.

3. (30 points)

   (a) (15 points) Modify Diffie-Helman key exchange so that three people share a secret.

   (b) (15 points) State carefully exactly what function Eve needs to compute to find the shared secret, with which inputs. (HINT: Its NOT Discrete Log.)

SOLUTION TO PROBLEM THREE

We'll call the people Alice, Bob, and Carol.

a)

(a) Alice randomly obtains a prime p and a generator $g \in \{p/3, \ldots, 2p/3\}$

(b) Alice makes (p, g) public (so Bob, Carol and Eve all see it).

(c) i. Alice picks a at random and sends g^a to everyone
   ii. Bob picks b at random and sends g^b to everyone
   iii. Carol picks c at random and sends g^c to everyone.

(d) i. Alice computes $(g^b)^a = g^{ab}$ and sends it to everyone.
   ii. Bob computes $(g^c)^b = g^{bc}$ and sends it to everyone.
   iii. Carol computes $(g^a)^c = g^{ac}$ and sends it to everyone.

(e) Alice computes $(g^{bc})^a = g^{abc}$ which is the secret!

(f) Bob computes $(g^{ac})^b = g^{abc}$ which is the secret!

(g) Carol computes $(g^{ab})^c = g^{abc}$ which is the secret!

b) Eve has to be able to compute following function.

INPUT: $p, g, g^a, g^b, g^c, g^{ab}, g^{ac}, g^{bc}$

OUTPUT: g^{abc}.

THERE ARE TWO MORE PAGES!!!!!!!!!!!!!!!!!!

4. (35 points) In this problem you will be asked to write several programs and then combine them.

   (a) (9 points) Write a program POWER that will, Given g, p, n compute, $g^n \pmod{p}$. (Use repeated squaring.) Note that p need not be a prime and g need not be a generator. (As a check, not to hand in, use it to redo problem 2 above.) Use this program to compute the following:

      i. $99^{99} \pmod{1010}$
      ii. $111^{111} \pmod{1010}$
      iii. $200^{999} \pmod{1111}$

      Output the results.

   (b) (5 points) Write a program TESTPRIME that does the following: Input p test if p is prime. Use the not-quite-correct method in the slides but also make sure that p is not one of the Carmichael numbers on the first Public-Key Crypto slide-packet. Use the program to find the first 10 primes that are ≥ 1000. Output the results.

   (c) (5 points) write a program TESTSAFEPRIMES that does the following: Input p test if p is a SAFE prime. (Use TESTPRIME as a subroutine.) Use the program to find the first 10 safe primes that are ≥ 1000. Output the results. Call them $p_1, \ldots, p_{10}$ for later reference.

   (d) (5 points) Given a Safe prime p and a number $g \in \{1, \ldots, p-1\}$ test if g is a generator. (This will use the program POWER.) Use the program to find, for each p_i from the last problem, the smallest generator mod p_i.

   (e) (11 points) I had said in class that *about half of the numbers in* $\{1, \ldots, p-1\}$ *are generators.* Lets get some empirical evidence on this! For all the p_i in Part c, for EVERY $g \in \{1, \ldots, p_i\}$. test if g is a generator. DO NOT output the generators, just output the number of generators. Also output what fraction of the numbers in $\{1, \ldots, p_i - 1\}$ are generators.

SOLUTION TO PROBLEM FOUR

Omitted

THERE IS ONE MORE PAGES!!!!!!!!!!!!!!!!!

5. (10 points) Professor Dogz has an idea! Rather than look at a random prime by picking an n-bit number he will pick an n-bit number of the form $30k+1$. This way he already knows its not divisible by 2,3, or 5.

   (a) Write psuedocode that will create a random number with ROUGHLY n bits (could be off by a constant) of the form $30k+1$.

   (b) Discuss PROS and CONS of picking random primes in this manner. (You can be informal.)

   SOLUTION TO PROBLEM FIVE

   a) The idea is to pick a random k of length m (we determine m later) and then look at $30k+1$. So we need m so that $30k+1$ is n bits. 30 is approximately 32. Hence $32k$ is around $m+5$ long. Hence we pick $m=n-5$.

   (a) Input n

   (b) Pick a random $n-6$ bit string k'.

   (c) Let $k=1k'$ (in binary).

   (d) Output $30k+1$.

   b)

   PRO- by only looking at such numbers you will find a prime faster since none of the numbers are divisible by 2,3,5. How much faster? There are 2^n n-bit numbers. Hence the search space is usually 2^n (though one finds a prime fairly fast). Now the search space is only $\frac{2^n}{30}$.

   CON- If Eve knows your prime will be of that form perhaps she can use some clever number theory or programming to take advantage of that.

6. (15 points) Alice and Bob do the Diffie-Helman Key Exchange with $p=107$ and $g=15$. Alice picks $a=20$ and Bob picks $b=9$. (You can use your program or Wolfram Alpha or some program on the web. Tell us which you used.)

   (a) (3 points) What does Alice send Bob? Show how she calculates it. For example (And this is NOT the right answer!):
   Alice sends Bob $g^{a^2} \pmod{107^2} = 15^{400} \pmod{107^2} = 8237$.

(b) (3 points) What does Bob send Alice? Show how he calculates it

(c) (3 points) Describe how Alice calculates the shared secret. Carry out that calculation and give the result.

(d) (3 points) Describe how Bob calculates the shared secret. Carry out that calculation and give the result. (This should be the same as the last answer.)

(e) (3 points) What is the secret written in binary? Use 8 bits since $2^7 < 107 < 2^8$. There can be leading 0's.

(f) (0 points) Why might Alice and Bob use the answer in binary?

SOLUTION TO PROBLEM SIX

I used wolfram alpha

All arithmetic is mod 107.

a) Alice sends $g^a = 15^{20} = 42$

b) Bob sends $g^b = 15^9 = 51$

c) Alice finds the shared secret by $(g^b)^a = 51^{20} = 12$

d) Bob finds the shares secret by $(g^a)^b = 42^9 = 12$

e) 12 in binary is 00001100

f) Alice and Bob end up with a fairly random sequence of 0's and 1's. They can use this for a 1-time pad.