HW 4 CMSC 456. DUE Oct 8
NOTE- THE HW IS TWO PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. What is your name? Write it clearly. What is the day and time of the first midterm? Read slides on Public Key. READ ON YOUR OWN: The Euclidean Algorithm for finding inverses of numbers in a mod.

2. (30 points) Recall that $a^n \pmod{p}$ can be done in $O(\log n)$ steps. This is usually very good. But what if n is ginormous?

   (a) Give an algorithm (psuedocode) to compute $a^n \pmod{p}$ efficiently even if n is ginormous – say $n \ge 10^{10^{10^{p!}}}!$, and p is a prime. (HINT: Repeated Squaring may be part of the answer but is not, by itself, enough.)

   (b) Use your method to compute, by hand, $14^{999,999,999} \pmod{107}$. (You can use a calculator but show all steps.)

   (c) Discuss how to compute $a^n \pmod{p}$ efficiently if n is ginormous- say $n \ge 10^{10^{10^{p!}}}!$, and p is A COMPOSITE. There IS a bottleneck to doing this – what is it? Why was it NOT a problem when p is prime?

3. (20 points) Alice and Bob are going to do RSA with $p = 11$ and $q = 13$,

   (a) (1 points) What is the value of N?

   (b) (1 points) What is the value of R

   (c) (6 points) What is the least $e \ge \frac{R}{6}$ that Alice can use?

   (d) (6 points) For that e, find the correct d. (you can use a program you find on the web but you must tell us what it is.)

   (e) (6 points) Bob wants to send the message 10. What does he send? (Use repeated squaring and show all step.)

THERE IS ONE MORE PAGE!!!!!!!!!!!!!!!!!!

4. (20 points) Alice and Bob are going to do RSA with $p = 17$ and $q = 19$,

   (a) (1 points) What is the value of N?

   (b) (1 points) What is the value of R

   (c) (9 points) If Alice uses $e = 2$ then for which m is Eve EASILY able to decode the message?

   (d) (9 points) If Bob wants to send $m = 3$ then for which e is Eve EASILY able to decode the message?

5. (30 points) Suppose that Professor Cowz has a key-exchange protocol P with the following properties. There is a security parameter n. If Alice and Bob use the protocol to share a message of length n (meaning the message is n binary bits long) then the following occurs:

   - If Eve cracks it, she can use that to factor numbers of length n. (Hence we think that for n large enough Eve cannot crack it.)
   - Before the protocol Eve is looking at 2^n possible shared secret keys it could be. If she was to try to figure out which one, she would have a $\frac{1}{2^n}$ chance of getting it right. We will assume that AFTER the protocol she STILL has only a $\frac{1}{2^n}$ chance of getting it right (unless she can factor).
   - At the end of the protocol Alice and Bob share a message s of length n. They did NOT get to control the message.

   QUESTIONS:

   (a) (10 points) (Look up on the web for this one and cite your source.) Complete this sentence: If $n \geq XXX$ then Eve will not be able to find the shares secret key.

   (b) (20 points) Show how Alice and Bob can use Cowz's key-exchange protocol to create a public key cryptosystem (where they can send what they want). Its OKAY if it has a small bias in it.