HW 4 CMSC 456. DUE Oct 8
SOLUTIONS
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 $n \geq 10^{10^{10^{p!}}}$!, 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 $n \geq 10^{10^{10^{p!}}}$!, 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?

SOLUTION TO PROBLEM TWO

a) Recall that $a^n \pmod p \equiv a^{n \pmod{p-1}} \pmod p$.

   (a) Input(a, n, p)

   (b) Divide n by $p-1$ and let n' be the remainder. NOTE: $0 \leq n' \leq p-2$, so n' is SMALL

   (c) Compute $a^{n'} \pmod p$ using repeated squaring.

b) When you divide 999,999,999 by 106 you get remainder 27.

So we now do $14^{27} \pmod{107}$.

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

$14^{2^1} \equiv ((14^{2^0})^2 \equiv 196 \equiv 89$

$14^{2^2} \equiv ((14^{2^1})^2 \equiv 89^2 \equiv 7921 \equiv 3$

$14^{2^3} \equiv ((14^{2^2})^2 \equiv 3^2 \equiv 9$

$14^{2^4} \equiv ((14^{2^3})^2 \equiv 9^2 \equiv 81$

We write 27 as a sum of powers of 2: $27 = 2^4 + 2^3 + 2^1 + 2^0$.

Hence

$$14^{27} \equiv 14^{2^4} \times 14^{2^3} \times 14^{2^1} \times 14^{2^0} \equiv 81 \times 9 \times 89 \times 14$$

$$(81 \times 9) \times (89 \times 14) \equiv 87 \times 69 \equiv 11$$

c) We can use that $a^n \pmod p \equiv a^{n \pmod{\phi(p)}} \pmod p$.

PRO- $n \mod \phi(p)$ will be smaller than p, so small.

CON- computing $\phi(p)$ might be hard. For p prime it was easy.

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 $e \geq \frac{R}{6}$ 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.)

SOLUTION TO PROBLEM THREE

a) $N = pq = 11 \times 13 = 143$

b) $R = (p-1)(q-1) = 10 \times 12 = 120$

c) $R/6$ is 20. We need to pick the least $e \geq 20$ such that e is rel prime to 120. $e = 23$ works.

d) Need d such that $ed \equiv 1 \pmod{120}$.

I used the program at `https://planetcalc.com/3311/`

The answer was 47.

e) To send 10 Bob must send

$10^{23} \pmod{143}$. We omit the solution.

$10^{2^0} \equiv 10$

$10^{2^1} \equiv 100$

$10^{2^2} \equiv 100 \times 100 \equiv (-43)(-43) \equiv 1849 \equiv 133$

$10^{2^3} \equiv 133 \times 133 \equiv (-10)(-10) \equiv 100$

$10^{2^4} \equiv 100 \times 100 \equiv 133$

So

$$10^{23} \equiv 10^{16} \times 10^4 \times 10^2 \times 10^1 \times 10^0 \equiv 133 \times 133 \times 100 \times 10 \times$$

$$\equiv 133 \times 133 \times 100 \times 10 \times \equiv (-10)(-10)(100)(10) \equiv$$

$$(100)(100)(10) \equiv 133 \times 10 \equiv -10 \times 10 \equiv -100 \equiv 33.$$

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?

   SOLUTION TO PROBLEM FOUR

   a) $N = pq = 17 * 19 = 323$

   b) $R = (p-1)(q-1) = 288$

   c) If Bob wants to send m then he sends $m^e \pmod N$ so $m^2 \pmod{323}$.

   For m small it will $m^2 \pmod{323}$ will be the ordinary m^2, and then Eve can take a square root (easy in the normal numbers, hard in mod 323) and get the answer.

   So long as $m^2 < 323$, it will be easy to determine m. That occurs when $m \leq 17$.

   d) If Bob wants to send m then he sends $m^e \pmod N$ so $3^e \pmod{323}$.

   For e small it will $3^e \pmod{323}$ will be the ordinary 3^e, and then Eve can take a log base 3 (easy in the normal numbers, hard in mod 323) and get the answer.

   So long as $3^e < 323$, it will be easy to determine m. That occurs when $m \leq 5$.

   END OF SOLUTION TO PROBLEM FOUR

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.

1) According to `http://mathworld.wolfram.com/RSANumber.html` The RSA challenge has challenged people to factor larger and larger numbers. The current winners is 232 DECIMAL digits so around 700 bits. We'll make it an even 1000 bits just to be sure.

2) Alice wants to send Bob m of length n. They first do the key-exchange protocol. They both now have a string s of length n. Eve has NO IDEA what s is. Alice then sends Bob $m \oplus s$.