HW 4 CMSC 389. DUE Jan 11
SOLUTIONS
WARNING- THE HW IS ONE PAGES LONG!!!!!!!!!!!!!

1. (0 points) Write your name! READ cipher and english.

2. (22 points) Compute each of the following using the repeated squaring method. Show all work.

   (a) $2^{100} \pmod{17}$

   (b) $2^{1000} \pmod{17}$.

   SOLUTION TO PROBLEM TWO

   Omitted

   END OF SOLUTION TO PROBLEM TWO

3. (24 points) In this problem we guide you to a technique to find $3^{100,000,000,000,000} \pmod{7}$ in reasonable time. Realize that repeated squaring won't be fast enough. All math in this problem is mod 7.

   (a) Compute 3^0, 3^1, 3^2, ..., 3^{10} all mod 7.

   (b) From the above try to find a pattern and a formula for 3^n.

   (c) Use the formula to find $3^{100,000,000,000,001} \pmod{7}$.

   SOLUTION TO PROBLEM THREE

   1)

   $3^0 \equiv 1$

   $3^1 \equiv 3 \times 1 \equiv 3$

   $3^2 \equiv 3 \equiv 3 \equiv 9 \equiv 2$

   $3^3 \equiv 3 \times 2 \equiv 6$

   $3^4 \equiv 3 \times 6 \equiv 3 \times -1 \equiv -3 \equiv 4$

   $3^5 \equiv 3 \times 4 \equiv 12 \equiv 5$

   $3^6 \equiv 3 \times 5 \equiv 15 \equiv 1.$

   $3^7 \equiv 3 \equiv 1 \equiv 3$

   $3^8 \equiv 2$

$3^9 \equiv 3 \equiv 2 \equiv 6$

$2^{10}3 \equiv 6 \equiv 4$

2)

AH- the pattern seems to be $1, 3, 2, 6, 4, 5$ then REPEAT SO

If $n \equiv 0 \pmod 6$ then $3^n \equiv 1$

If $n \equiv 1 \pmod 6$ then $3^n \equiv 3$

If $n \equiv 2 \pmod 6$ then $3^n \equiv 2$

If $n \equiv 3 \pmod 6$ then $3^n \equiv 6$

If $n \equiv 4 \pmod 6$ then $3^n \equiv 4$

If $n \equiv 5 \pmod 6$ then $3^n \equiv 5$

3)

$3^{100,000,000,000,000} \pmod 7$.

Need to know $100,000,000,000,001 \pmod 6$.

$100,000,000,000,001$ is odd so $\equiv 1$ OR 3 OR 5 mod 6.

$100,000,000,000,001 \equiv 2 \pmod 3$ so $\equiv 2$ or 5 mod 6.

Hence $100,000,000,000,000 \equiv 5 \pmod 6$.

Hence $2^{100,000,000,000,000} \equiv 5 \pmod 7$.

END OF SOLUTION TO PROBLEM THREE

4. (27 points)

   (a) Alice and Bob do Diffie Helman with $p = 53$, $g = 4$, $a = 5$, $b = 6$ What does Alice send? What does Bob send? What is the shared secret key?

   (b) Alice and Bob do Diffie Helman with $p = 53$, $g = 4$, $a = 6$, $b = 5$. What does Alice send? What does Bob send? What is the shared secret key?

   (c) If you did the problems above correctly then they had the same answer. Is this a coincidence or is there a reason for it?

SOLUTION TO PROBLEM FOUR

a) All equations are mod 53

Alice sends $g^a = 4^5$

$4^2 = 16$

$4^4 = 16^2 = 256 = 44$

$4^5 = 4^4 \times 4 = 44 * 4 = 17$

Alice sends 17

Bob sends- we omit that

Secret is $17^6 = 44$

b) Omitted

c) If Alice sends a and Bob b sends be then secret is g^{ab}.

If Alice sends b and Bob sends a then secret is gab

So not a coincidence.

END OF SOLUTION TO PROBLEM FOUR

5. (27 points) Alex wants to use the prime 101 for Diffie Helman.

   (a) In order to determine if a number, g, is a generator, what does Alex have to do?

   (b) Is picking 101 a bad idea?

   (c) Give a prime between 100 and 200 that would be a good one to use.

SOLUTION TO PROBLEM FIVE

The nontrivial factors of 100 are 2,5,10,20,25,50. Alex needs to raise g to all of these powers. If any are 1 then g is NOT a geneator, else it is.

101 is a bad idea since the number of divisor is large

Lets look at primes over 100 until we find a safe one.

101: 101-1=100=2*50. 50 is NOT PRIME so NO

103: 103-1=102=2*51. 51 is NOT PRIME so NO

107: 107-1=106=2*53. 53 IS PRIMES so

answer is 107.

END OF SOLUTION TO PROBLEM FIVE