HW 4 CMSC 389. DUE Jan 11
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) $2^{1000} \pmod{17}$.

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 $3^{100,000,000,000,001} \pmod{7}$.

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?

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.