1. (0 points) What is your name? Write it clearly. STAPLE your HW.

2. (10 points) Describe how you would find a generator mod 31.

3. (20 points) Alice and Bob are going to do the Diffie Helman protocol with \( p = 47 \) and \( g = 2 \).
   
   (a) If Alice picks \( a = 4 \) and Bob picks \( b = 7 \) then what is the shared secret key that Alice and Bob will share?
   
   (b) If Alice picks \( a = 7 \) and Bob picks \( b = 4 \) then what is the shared secret key that Alice and Bob will share?
   
   (c) The answers to the last two problems are the same. Explain why this is so.
   
   (d) If Alice picks \( a = 4 \) and Bob picks \( b = 7 \) then Eve CAN find the shared secret key EASILY (very easily, not just because 47 is so small). Explain why. Give some good advice for people using prime \( p \) and generator \( g \) to avoid this problem pointed out in part d.

4. (20 points) Assume you have a quick test for telling if a number is prime. Write down an algorithm that will, given \( n \), find a prime between \( n \) and \( 2n \) by picking numbers at random that are NOT divisible by 2, 3, OR 5 and testing them. (SEE handout on the course website about finding primes.)
5. (30 points) For this problem express the answers in terms of factorials. If your answer is (say) $\frac{19!}{10!9!}$ DO NOT reduce it- leave it in those terms.

(a) I have 5 $a$’s and 8 $b$’s. How many different words can I spell? (They need not be, and won’t be real words. For example $aaaaabbbbbbb$ and $abababababbb$ are both words.) HINT: Think of a word as a 13-long sequence of characters. You are CHOOSING 5 positions to put the $a$’s into. Note that once this is done the places to put $b$’s are determined.

(b) I have 5 $a$’s and 8 $b$’s and 6 $c$’s. How many different words can I spell? HINT: Think of a word as a 19-long sequence of characters. You are CHOOSING 5 positions to put the $a$’s into. You THEN have 13 left. You are CHOOSING 8 positions to put $b$’s into. Note that once this is done the places to put $c$’s are determined.

(c) I have $n_1$ $a$’s and $n_2$ $b$’s and $n_3$ $c$’s. How many different words can I spell?

6. (20 points) What is the coefficient of $x^{10}y^4z^6$ in $(x + y + z)^{20}$? Explain your answer.