HW 5 CMSC 389. DUE Jan 10

DO NOT USE A CALCULATOR. ON THE MIDTERM YOU WILL NOT BE ALLOWED ONE

1. (0 points) READ my NOTES on Diffie-Helman in ciphers.pdf.
2. (30 points) Compute the following using the repeated squaring method.
   (a) $2^{20} \pmod{17}$
   (b) $3^{40} \pmod{47}$
   (c) $4^{10} \pmod{59}$
   (d) $5^5 \pmod{101}$
   (e) $6^{16} \pmod{91}$
3. (40 points) Alice and Bob are going to do Diffie Helman with $p = 29$ and $g = 2$.
   (a) Assume that Alice's picks $a = 10$. What does Alice send Bob? Show your work.
   (b) Assume that Bob's picks $b = 8$. What does Bob send Alice? Show your work.
   (c) What is the shared secret key? Show your work. Express both as a number in $\{0, \ldots, 28\}$ and as a sequence of bits in binary. Show your work.
   (d) If Alice uses a and Bob uses b then let the shared secret key be $s(a, b)$. Find pairs (a_1, b_1) and (a_2, b_2) so that $a_1 \neq a_2$ and $b_1 \neq b_2$ and $s(a_1, b_1) = s(a_2.b_2)$.
4. (30 points) Alice and Bob are doing Diffie Helman with prime $p = 6299$ and generator $g = 2$. Alice sends 64. Bob sends 65.
   (a) Find the shared secret key. Show your work. FOR THIS ONE YOU CAN use a calculator, but you will also need to think- brute force will not work.
   (b) Give Alice and Bob advice on how they can prevent Eve from using your method, even if $p = 6299$.