

### HW 5 CMSC 389. DUE Jan 10

1. (0 points) What is your name? Write it clearly. Staple your HW. What is the day and time of the second midterm? Are you free then? (if not then SEE ME IMMEDIATELY) When is the final? Are you free then? (if not then SEE ME IMMEDIATELY)
  
2. (50 points) (NOTE- you may want to write a program to do this one for you. Read the entire question first so you can do this. It can be done by hand- your choice.) In this problem we work mod 31.
  - (a) Find the least number  $g \geq 4$  such that  $g$  is a generator mod 31.
  - (b) If Alice and Bob do Diffie-Helman, Alice uses  $a = 17$ , and Bob uses  $a = 9$ , then what is their shared secret key?
  
3. (50 points) Alice wants to use a linear cipher to send messages to Bob. For some reason she wants to send  $a$  to  $p$  and  $c$  to  $x$ .  
This is possible. Explain how it is possible. Use indexing starting at  $a = 0$ .