HW 11 CMSC 389. DUE Jan 20
REMINDER- OPTIONAL PROJECT DUE JAN 20
THIS HW IS TWO PAGES LONG

1. (0 points) READ my NOTES SECRET SHARING- PARTICULARLY VERIFIABLE.

2. (30 points) Zelda wants to share a secret with A_1, A_2, A_3, A_4 so that if 3 of them get together they can find out the secret but any 2 cannot. She uses the mod field 11. Assume that A_1 gets 6, A_2 gets 9 and A_3 gets 1. (I am not telling you A_4's share.) For each of the following either solve it OR tell me why it can't be solved.

   (a) A_1, A_2, A_3 all get together. Can they find out the secret? If so then find it out and tell me. If not then tell me why not.

   (b) A_1, A_2, A_3 all get together. Can they find out what A_4's share was? If so then find it out and tell me. If not then tell me why not.

   (c) A_1, A_2 all get together. Can they find out the secret? If so then find it out and tell me. If not then tell me why not.

   (d) A_1, A_2 all get together. Can they find out what A_4's share was? If so then find it out and tell me.

3. (30 points) Zelda wants to do VERIFIABLE Secret Sharing with A_1, A_2, A_3, A_4 so that if 2 of them get together they can find out the secret but any 1 cannot. She uses the mod field p where p is large. But alas, A_4 has a computer that can solve Discrete Log problems mod p. Alice gives out the shares and the appropriate powers of g. For each of the following statements state TRUE or FALSE and EXPLAIN your answer.

   (a) A_4 learn the secret.

   (b) A_4 learn A_1's share.

   (c) A_4 give a false value of $f(4)$ and have the other players not realize this.

THERE IS A SECOND PAGE

4. (40 points) (Read the notes on non-threshold secret sharing) Zelda wants to share a secret with A_1, A_2, A_3, A_4 so that if A_1 AND any two of A_2, A_3, A_4 want to find the secret they can, but (1) any set that does not include A_1 CANNOT get the secret, (2) Any set that is A_1 and just ONE of $\{A_2, A_3, A_4\}$ CANNOT get the secret. Show how Zelda CAN do this with shares of size $|s|$. Make up a HW problem on this that I can give to my next Winters class and also provide the solution. Make it so that next years class will see a clean problem and a clean solution. The kind you would want to see.