HW 10 CMSC 456. MORALLY DUE Nov 26
NOTE- THE HW IS ONE PAGE LONG!!!!!!!

1. (0 points) READ the syllabus- Content and Policy. What is your name? Write it clearly. What is the day of the final? READ the slides and notes on Secret Sharing.

2. (30 points) Let $1 \leq t \leq L$. Show that there CANNOT be a (t, L) VSS scheme if all the players are all powerful and they want information-theoretic security. The players shares can be of any finite length. (WARNING- DO NOT prove that the VSS scheme WE gave in class would not work. You need to show that NO VSS scheme works.)

3. (30 points)

   (a) (20 points) In class we showed how to use the Paillier Public Key Crypto System and Secret Sharing to hold an election where there are TWO candidates. Find a way to hold an election with THREE candidates and V voters. You are GIVEN V and need to put conditions on N so that your scheme works.

   (b) (10 points) If 1,000,000 people want to vote then how large does N have to be?

4. (20 points) Zelda wants to do $(3, 3)$ secret sharing with polynomials. The secret is 1001 which is 9 in base 2, so she uses mod 11. Zelda picks out $r_2 = 3$ and $r_1 = 7$. What shares does she give out? Give the ACTUAL NUMBER, do not just say, for example $f(1)$. (NOTE- this was an issue on the midterm when some people for Diffie Helman wrote that Alice sends $2^4 \pmod{11}$. I am asking this question now so that you DO NOT make the same MISTAKE on the FINAL.)

5. (20 points) In the last problem Zelda had secret 9 and used mod 11. The players DO know the length of the secret (that is not considered a leak of info). The players DO know that they work mod 11. Does the choice of 11 leak any information? Explain your answer.