HW 11 CMSC 456. Morally DUE Nov 25
DEAD CAT DAY IS NOV 27
THIS HW IS TWO PAGES LONG

1. (0 points) What is Day/Time of Final? **READ MID SOLUTIONS! Even for the problems you got right!!!!!!!!!!!!!!**

2. (30 points) Zelda wants to do $(7, 14)$ information-theoretic secret sharing. The players are $A_1, \ldots, A_{14}$. The secret string is 1001.

   (a) (15 points) Zelda wants to use the random string method. How many strings does A_1 get? (Give an actual number, not something like *the 9th JUSTIN Composite*.) How long are the strings A_1 gets?

   (b) (15 points) Zelda wants to use the polynomial method. What is the smallest prime Zelda can use? What is the degree of the polynomial that Zelda uses? How many strings does A_1 get? How long are they?

3. (30 points)

   (a) (20 points) DESCRIBE the random-string $(3, 9)$ secret sharing scheme. You must describe both what Zelda gives out, and how any three people can determine the secret. KEY: Explain it so that someone who has never seen secret sharing can understand it. This is NOT hypothetical. A TA who does not know secret sharing is grading this problem and will learn the protocol from you! How many strings does each person get? (Give an actual number, NOT something like *the 17th MARINA number*.)

   (b) (10 points) DO AN EXAMPLE of your method.

MORE HW ON THE NEXT PAGE

4. (40 points)

   (a) (30 points) DESCRIBE the polynomial $(4, 7)$ secret sharing scheme. You must describe both what Zelda gives out, and how any four people can determine the secret. How many strings does each person get? (Give an actual number, NOT something like *the Ninth Nathan Natural Number*.) KEY: Explain it so that someone who has never seen secret sharing can understand it. This is NOT hypothetical. A TA who does not know secret sharing is grading this problem and will learn the protocol from you!

   (b) (10 points) DO AN EXAMPLE of your method.