HW 09 CMSC/MATH/ENEE 456. Morally DUE NOV 23
DEAD CAT DAY extended to Nov 30

1. (0 points but you MUST DO IT)

   (a) What DAY and TIME are the TIMED FINAL?

   (b) IF that DAY/TIME is not good for you then EMAIL ME.

   (c) We are NOT meeting the Tuesday of Thanksgiving. When is the make-up lecture?

   THROUGHOUT THIS HW $\frac{a}{b}$ MEANS $\lfloor \frac{a}{b} \rfloor$.

GOTO NEXT PAGE

2. (40 points) Alice and Bob are going to do PRIVATE-LWE with parameters:

   $\vec{k} = (11, 100, 39, 4)$.

   $p = 1009$.

   $\gamma = 2$.

   (a) (13 points) Alice wants to send the bit 1. The random vector she picks is $(1, 2, 3, 4)$. The e she picks at random is 2. What does she send Bob? Show your work, though you may use a calculator.

   (b) (13 points) Alice wants to send the bit 0. The random vector she picks is $(5, 10, 41, 3)$. The e she picks at random is -1. What does she send Bob? Show your work though you may use a calculator.

   (c) (14 points) Bob receives from Alice $(12, 39, 44, 19; 779)$. What bit did Alice send? Show your work though you may use a calculator.

   (d) (0 points) How many students did not now when the midterm was and commented that they always skip the first question, and then suggested that I make this information part of all of the second question?

   (e) (0 points) What DAY and TIME are the TIMED FINAL?

   (f) (0 points) IF that DAY/TIME is not good for you then EMAIL ME.

GOTO NEXT PAGE

3. (30 points) Alice and Bob are going to do PRIVATE-LWE with parameters:

   $\vec{k} = (10, 201, 89, 8)$.

   $p = 2003$.

   $\gamma = 4$.

   Alice and Bob think that Eve might be intercepting their messages and tampering with them!

   (a) (15 points) Give an algorithm so that, if Bob gets $(r_1, r_2, r_3, r_4; D)$, he will output one of the following

   - Alice probably sent a 0.
   - Alice probably sent a 1.
   - Eve definitely tampered with the message.

   (b) (15 points) Use your technique in the part 1 on the following inputs. Show your work and state your conclusion. (You may use a calculator.)

   i. Bob gets $(1, 2, 3, 4; 5)$.

   ii. Bob gets $(11, 40, 99, 101; 245)$.

GOTO NEXT PAGE

4. (30 points) Alice and Bob are going to do PRIVATE-LWE with parameters:

   $\vec{k} = (11, 100, 39, 4)$. (RECALL- this is private)

   $p = 1009$. (RECALL- this is public)

   $\gamma = 2$. (RECALL- this is public)

   Eve sees Alice send

   $$(7, 13, 22, 100; 618).$$

   She later finds out that this decoded to 0.

   Write down what she knows about k_1, k_2, k_3, k_4.