HW 10 CMSC 456. Morally DUE Nov 30

1. (25 points) (You might want to write a program on your own for this problem, but not for autograding.) Alice and Bob are doing LWE-private key over mod 101. They agree on secret key $(2, 3, 5, 7)$. We give the random numbers Alice picks, the bit she wants to send, and the value of e she picks. YOU will supply what she sends Bob.

Rand Numb	bit	e	What Alice Sends Bob
(1,8,7,90)	1	0	
(1,8,7,90)	0	1	
(1,8,7,90)	1	-1	
(1,8,7,90)	0	0	
(10,81,71,91)	1	1	
(10,81,71,91)	0	-1	
(10,81,71,91)	1	0	
(10,81,71,91)	0	1	

2. (25 points) Alice and Bob do LWE-private with $p = 1001$, vectors of length 3. (1001 is not a prime but one can still do LWE-private using it.)

   (a) (25 points) Describe a variant of LWE-private where Alice can send Bob one of THREE possibilities, which we will call $0, 1, 2$.

   (b) (0 points) DO NOT HAND IN- do this for your own enlightenment. Describe a variant of LWE-private where Alice can send Bob one of FOUR possibilities, which we will call $0, 1, 2, 4$.

   (c) (0 points) Do parts 1 and 2 of this question with a general p. The key is to find γ that works.

3. (25 points) A1, A2, A3, A4 have cards similar to those used in the Alice-Bob-Cards-Dating lecture. (e.g., hearts, spades, uparrows, make them clear, make them opaque, make them fit into pez dispensers). A1 has a bit a_1, A2 has a bit a_2, A3 has a bit a_3, A4 has a bit a_4. They want to compute $a_1 \wedge a_2 \wedge a_3 \wedge a_4$ such that

   (a) At the end they ALL know $a_1 \wedge a_2 \wedge a_3 \wedge a_4$.

   (b) At the end A1 only knows a_1 (of course), $a_1 \wedge a_2 \wedge a_3 \wedge a_4$, and what can be deduced from these. So

      i. If $a_1 = 0$ and $a_1 \wedge a_2 \wedge a_3 \wedge a_4 = 0$ then A1 knows nothing about a_2 or a_3 or a_4.

      ii. If $a_1 = 0$ and $a_1 \wedge a_2 \wedge a_3 \wedge a_4 = 1$ THIS CANNOT HAPPEN.

      iii. If $a_1 = 1$ and $a_1 \wedge a_2 \wedge a_3 \wedge a_4 = 0$ then A1 knows $a_2 = 0$ or $a_3 = 0$ or $a_4 = 0$, but does not know which of those happens. a_1 DOES NOT even know how many of a_2, a_3, a_4 said 0.

      iv. If $a_1 = 1$ and $a_1 \wedge a_2 \wedge a_3 \wedge a_4 = 1$ then A1 knows $a_2 = 1$ and $a_3 = 1$ and $a_4 = 1$.

   (c) Similar for a_2, a_3, a_4.

   And now **finally** the problem: Give a protocol for A_1, A_2, A_3, A_4 to use that achieves the above conditions. Recall that they can use cards.

   Hint: Use a variant of one of the schemes discussed in the Alice-Bob-Cards-dating lecture

4. (25 points) In this problem we only deal with messages that are strings of bits. DO NOT do just part b and say is applies to Part a- just do two different methods for Part a and Part b.

   In this problem when I ask for an error-detection or error-correction code I mean you have to tell me:

   If Alice wants to send $m_1 \cdots m_L$, what does she send?

   When Bob gets $b_1 \cdots b_n$ what does he do to detect or correct?

   (a) (15 points) Give an error-detecting code such that the following happens.

   - If there are 0 errors, Bob is confident there are 0 errors.
   - If there is 1 error, Bob is confident there is 1 error.
   - If there are 2 errors, Bob is confident there are 2 error.
   - If there are ≥ 3 errors then Bob is confident of something but he is wrong.

   (Hint: Use a variant of the Parity Check.)

   (b) (10 point) Give an error-correcting code such that the following happens (note also that there is a question on the fourth point).

   - If there are 0 errors, Bob is confident there are 0 errors.
   - If there is 1 error, Bob is confident there is 1 error and he knows where it is so he can correct it.
   - If there are 2 errors, Bob is confident there are 2 errors and he knows where it is so he can correct them.
   - If there are ≥ 3 errors then Bob is confident of something but he MIGHT BE wrong. Give an example where there are 3 errors but Bob is right. Give an example where there are 3 errors but Bob is wrong.

   (Hint: Use a variant of the repetition code.)