HW 11 CMSC 456. Morally Due Dec 7

1. (40 points) Zelda has a secret s that she will share with $A_1, A_2, A_3, A_4, A_5, A_6$:

   If A_1 and A_2 (or any superset) get together they can learn the secret.

   If A_2 and A_3 (or any superset) get together they can learn the secret.

   If A_3 and A_4 (or any superset) get together they can learn the secret.

   If A_4 and A_5 (or any superset) get together they can learn the secret.

   If A_5 and A_6 (or any superset) get together they can learn the secret.

   If A_1 and A_3 and A_5 (or any superset) get together they can learn the secret.

   NO OTHER set of people who get together can learn anything about the secret.

   and NOW for the question:

   (a) (20 points) EXPLAIN an info-theoretic secret sharing scheme Zelda can use. Specify: (1) What Zelda gives to each person, and (2) What each group does to obtain the secret.

   (b) (20 points) Let $|s|$ be the length of the secret. For each $1 \leq i \leq 6$ tell us the length of the share that A_i gets. For each i it will be of the form $f(|s|) + O(1)$ for some f.

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

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

GOTO NEXT PAGE

2. (40 points)

   (a) (40 points) Zelda is doing info-theoretic $(3, 6)$ secret sharing with $A_1, A_2, A_3, A_4, A_5, A_6$. She is using the polynomial method with $p = 37$. She has a "brilliant" idea: Rather than share ONE secret of $\mathbb{Z}_p$, she will share two secrets! Here is her plan.

   - She wants to share $s_1, s_2 \in \mathbb{Z}_p$.
   - She picks ONE random $r \in \mathbb{Z}_p$.
   - She formulates the polynomial $f(x) = rx^2 + s_1x + s_2 \pmod{p}$
   - For $1 \leq i \leq 6$ she gives A_i the number $f(i)$.
   - If any three get together they will have three points on a degree-2 equation and hence they can find the equation $f(x)$, and hence they can find s_1, s_2.

   Show why this is a BAD idea.

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

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

   (d) (0 points) How many people came to me the DAY of the midterm needing to take it a diff day who told me *I always skip problem 1 since its just information on the HW, hence you should make that information a part of EVERY problem so people like me won't miss it again.*?

GOTO NEXT PAGE

3. (20 points) In class (the Nov 16 lecture Alice-Bob-Love-Cards) we did several protocols (using cards and other devices) such that Alice and Bob can determine if they want a second date; however, if Alice wants a second date but Bob doesn't Bob does not know that (and vice versa).

   Alice, Bob, Carol, Donna all get together for dinner. They want to see if they want to have dinner again. If ALL want to dine again, they will. If at least ONE person does not, they won't.

   Come up with a protocol so that at the end they all know if they want to have dinner together again, but if the answer is NO then the people who voted NO do not know how anyone else voted. You can use any of the devices in the talk on Alice and Bob.