HW 12 CMSC 456. Morally DUE Dec 2
THIS HW IS TWO PAGES LONG
SOLUTIONS

1. (0 points) What is day/time of final? **READ MID SOLUTIONS! Even for the problems you got right!!!!!!!!!!!!!!**

2. (30 points) Zelda does (3,5) secret sharing. The secret is of length 2, so they use the prime 5. Zelda gives out the following numbers:

   A_1 gets 3

   A_2 gets 3

   A_3 gets 3

   A_4 gets 3

   A_5 gets 3

   (a) (15 points) A_1 and A_2 get together. Show that for $c = 0, 1, 2$, there is a quadratic polynomial over $\mathbb{Z}_5$ where ALL of the following hold:

   i. $f(1) = 3$
   ii. $f(2) = 3$
   iii. The constant term is c (which is equivalent to $f(0) = c$).

   (NOTE: it's also true for $c = 3, 4$ but I want to spare you the work. This is important because, if you did the problem with $c = 0, 1, 2, 3, 4$ you would show that A_1 and A_2 have learned NOTHING since all secrets are still possible.) **Show your work.**

   ANSWER

   ALL $\equiv$ are mod 5.

   $c = 0$: $f(x) \equiv r_2x^2 + r_1x + 0$. Need r_1, r_2 so that $f(1) \equiv 3$ and $f(2) \equiv 3$.

   $f(1) = 3$: $r_2 + r_1 + 0 \equiv 3$, so $r_2 + r_1 \equiv 3$.

   $f(2) = 3$: $4r_2 + 2r_1 + 0 \equiv 3$, so $4r_2 + 2r_1 \equiv 3$.

   Sub $r_1 \equiv 3 - r_2$ into the second equation:

$$4r_2 + 2(3 - r_2) \equiv 3$$

$$2r_2 + 6 \equiv 3$$

$$2r_2 + 1 \equiv 3$$

$$2r_2 \equiv 3 - 1 \equiv 2.$$

We can easily see from this that $r_2 \equiv 1$.

We have $r_2 \equiv 1$. So $r_1 \equiv 3 - r_2 \equiv 3 - 1 \equiv 2$.

So we have

$f(x) \equiv x^2 + 2x$.

Lets CHECK:

$f(1) \equiv 1 + 2 \times 1 \equiv 3$. YES

$f(2) \equiv 4 + 2 \times 2 \equiv 4 + 4 \equiv 8 \equiv 3$. YES.

$c = 1$: Omitted.

$c = 2$: Omitted.

END OF ANSWER

(b) (15 points) What is the secret? **Show your work.**

ANSWER

ALL $\equiv$ are mod 5.

$f(x) \equiv r_2x^2 + r_1x + s$

$f(1) \equiv 3$ so $r_2 + r_1 + s \equiv 3$

$f(2) \equiv 3$ so $4r_2 + 2r_1 + s \equiv 3$

$f(3) \equiv 3$ so $9r_2 + 3r_1 + s \equiv 3$, so $4r_2 + 3r_1 + s \equiv 3$.

From the last two equations we get $r_1 \equiv 0$.

Sub this into the first two equations to get

$r_2 + s \equiv 3$

$4r_2 + s \equiv 3$

From this we get $3r_2 \equiv 0$ so $r_2 \equiv 0$. (Note that we needed that 5 was prime).

So $r_2 = 0$.

From the first equation we get $s = 3$.

END OF ANSWER

3. (40 points) Show that there is NO way to do (t, m) Verifiable Secret Sharing in a way that is information-theoretic secure.

(*WARNING:* The scheme I showed in class for VSS was comp-secure. This has NO bearing on our problem. Just because there IS a comp-secure scheme does not mean that there is not an info-secure scheme. DO NOT MAKE THIS MISTAKE!!!!!!!!)

ANSWER

Assume that there is a (t, m)-VSS scheme. We show that if the players have unlimited computational power then $t-1$ can crack the secret. (In fact, 1 can crack the secret but we leave that for you to figure out.)

$A_1, \ldots, A_{t-1}$ get together. They reveal their shares $s_1, \ldots, s_{t-1}$. They can find the share of A_t as follows:

They know the share is of string in $\{0,1\}^*$. Let $\{0,1\}^*$ be, in lex order, $u_1, u_2, u_3, \ldots$.

$A_1, \ldots, A_{t-1}$ try to verify that A_t's share is u_1. If they fail they try to verify u_2. Etc. Eventually they will find the share and verify it. They then have A_t's share so can crack the secret.

END OF ANSWER

GOTO NEXT PAGE

4. (30 points) Professor Gasarch is grading this one and actually wants ideas on how to improve the course. Make your answers short and coherent. You can only get this one wrong if you leave it out or say something incoherent.

   (a) (10 points) What was your favorite topic in the course? Why?

   (b) (10 points) What was your least favorite topic in the course? Why?

   (c) (10 points) What is your opinion of the dead cat policy? Why?

   (d) (0 points, but answer if you have an answer.) Name something to IMPROVE the course aside from removing your least favorite topic.)

5. (0 points but you should do it) Alice, Bob, and Carol 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 dispencers). Alice has a bit a, Bob has a bit b, Carol has a bit c. They want to compute $a \wedge b \wedge c$ such that

   (a) At the end they ALL know $a \wedge b \wedge c$.

   (b) At the end Alice only knows a or course, and $a \wedge b \wedge c$, and whatever can be deduced from these. So

      i. If $a = 0$ and $a \wedge b \wedge c = 0$ then Alice knows nothing about b, c.

      ii. If $a = 0$ and $a \wedge b \wedge c = 1$ then THIS CANNOT HAPPEN.

      iii. If $a = 1$ and $a \wedge b \wedge c = 0$ then Alice knows that $b \wedge c = 0$, so at least one of b, c is 1.

      iv. If $a = 1$ and $a \wedge b \wedge c = 1$ then Alice knows that $b \wedge c = 1$, so $b = c = 1$.

   (c) Similar for Bob and Carol.

   Hint: Use a variant of what we did in the Alice-Bob-Cards-dating lecture