HW 11 CMSC 389. DUE Jan 20
REMINDER- OPTIONAL PROJECT DUE JAN 20
SOLUTIONS
THIS HW IS TWO PAGES LONG

1. (0 points) READ my NOTES SECRET SHARING- PARTICULARLY VERIFIABLE.

2. (30 points) Zelda wants to share a secret with A_1, A_2, A_3, A_4 so that if 3 of them get together they can find out the secret but any 2 cannot. She uses the mod field 11. Assume that A_1 gets 6, A_2 gets 9 and A_3 gets 1. (I am not telling you A_4's share.) For each of the following either solve it OR tell me why it can't be solved.

   (a) A_1, A_2, A_3 all get together. Can they find out the secret? If so then find it out and tell me. If not then tell me why not.

   (b) A_1, A_2, A_3 all get together. Can they find out what A_4's share was? If so then find it out and tell me. If not then tell me why not.

   (c) A_1, A_2 all get together. Can they find out the secret? If so then find it out and tell me. If not then tell me why not.

   (d) A_1, A_2 all get together. Can they find out what A_4's share was? If so then find it out and tell me.

   SOLUTION TO PROBLEM 2

   2a) YES. We know that $f(1) = 6$, $f(2) = 9$, and $f(3) = 1$ and that f is a quadratic. After either setting up three linear equations in three variables OR doing the h_i method in the note you arrive at

   $f(x) = 3x + 3$

   Hence the secret is 3.

   2b) YES. As above A_1, A_2, A_3 find out that $f(x) = 3x + 3$. They know that A_4 gets $f(4) = 4$.

   2c,2d) If A_1 and A_2 get together they have two points on a quadratic. From this they learn NOTHING. In particular for ANY $c \in \{0, 1, \ldots, 10\}$ there is a quadratic f such that $f(1) = 6$, $f(2) = 9$, and the constant term is c. Hence they have NO INFO on what s is. Similar for figuring out $f(4)$.

3. (30 points) Zelda wants to do VERIFIABLE Secret Sharing with A_1, A_2, A_3, A_4 so that if 2 of them get together they can find out the secret but any 1 cannot. She uses the mod field p where p is large. But alas, A_4 has a computer that can solve Discrete Log problems mod p. Alice gives out the shares and the appropriate powers of g. For each of the following statements state TRUE or FALSE and EXPLAIN your answer.

   (a) A_4 can learn the secret.

   (b) A_4 can learn A_1's share.

   (c) A_4 can give a false value of $f(4)$ and have the other players not realize this.

SOLUTION TO PROBLEM 3

Recall that Zelda will

- Pick random a_1.
- Form $f(x) = a_1 x + s$.
- Give A_1 $f(1)$, A_2 $f(2)$, A_3 $f(3)$, and A_4 $f(4)$.
- Give EVERYONE g^{a_1}, g^s, and g.

3a) YES. Since A_4 has g^s and can compute Discrete Log, he can get s.

3b) YES. Since A_4 has g^s and g^{a_1} and can compute Discrete Log, he can get a_1 and s. Hence he can compute $f(1)$ and learn A_1's share.

3c) NO. The Verifiable part of Verifiable Secret Sharing still works. Assume that A_4 gives a value $f(4)' \neq f(4)$. We show he gets caught. EVERYONE has g^{a_1} and g^s, so EVERYONE can compute $(g^{a_1})^4 \times g^s = g^{4a_1+s} = g^{f(4)}$. Once A_4 reveals his (false) value $f(4)'$, EVERYONE will compute $g^{f(4)'}$ and they will find out its NOT $g^{f(4)}$.

THERE IS A SECOND PAGE

4. (40 points) (Read the notes on non-threshold secret sharing) Zelda wants to share a secret with A_1, A_2, A_3, A_4 so that if A_1 AND any two of A_2, A_3, A_4 want to find the secret they can, but (1) any set that does not include A_1 CANNOT get the secret, (2) Any set that is A_1 and just ONE of $\{A_2, A_3, A_4\}$ CANNOT get the secret. Show how Zelda CAN do this with shares of size $|s|$. Make up a HW problem on this that I can give to my next Winters class and also provide the solution. Make it so that next years class will see a clean problem and a clean solution. The kind you would want to see.

SOLUTION TO PROBLEM 4

(a) Zelda has secret s. She generates RANDOM s'. She lets $s_1 = s'$ and $s_2 = s \oplus s_1$.

(b) Give A_1 s_1.

(c) Do standard poly secret sharing with A_2, A_3, A_4 where they need for ANY two of them to get the secret, with secret s_2.

(d) IF A_1 and any two of A_2, A_3, A_4 get together then the two of $\{A_2, A_3, A_4\}$ can find s_2. A_1 has s_1. So they computer $s_1 \oplus s_2 = s$.

PROBLEM for Next Years class:

Zelda works over mod 11. We view all of the elements of $\{0, 1, \ldots, 10\}$ as a sequence of 4 bits (e.g., 0 is 0000, 1 is 0001, ..., 10 is 1010). Zelda wants to make sure that if A_1 and any two of A_2, A_3, A_4 can find the secret, but no other set can.

The secret is 7=0111. DO an example where YOU pick the random strings or numbers needed.

ANSWER:

(a) Zelda picks random string $s_1 = 0001$. Zelda then makes $s_2 = 0111 \oplus 0001 = 0110$.

(b) Zelda gives A_1 0001.

(c) Zelda wants to secret share 0110 (which is 6) the number in the standard way to A_2, A_3, A_4 so that any 2 can get the secret. Zelda needs two pick TWO random numbers in $\{0, 1, 2, \ldots, 10\}$. We'll say they are $a_2 = 4$ and $a_1 = 8$. Let

$f(x) = 4x^2 + 8x + 6$ (all mod 11)
Give A_2 $f(2) = 4 * 4 + 8 * 4 + 6 = 5 - 1 + 6 = 10$.
Give A_3 $f(3) = 4 * 3^2 + 8 * 3 + 6 = 4 * (-2) + 24 + 6 = 3 + 2 + 6 = 0$
Give A_4 $f(4) = 4 * 4^2 + 8 * 4 + 6 = 4 * 5 - 1 + 6 = 25 = 3$.