HW 10 CMSC 456. MORALLY DUE Nov 26
SOLUTIONS
NOTE- THE HW IS ONE PAGE LONG!!!!!!!

1. (0 points) READ the syllabus- Content and Policy. What is your name? Write it clearly. What is the day of the final? READ the slides and notes on Secret Sharing.

2. (30 points) Let $1 \le t \le L$. Show that there CANNOT be a (t, L) VSS scheme if all the players are all powerful and they want information-theoretic security. The players shares can be of any finite length. (WARNING- DO NOT prove that the VSS scheme WE gave in class would not work. You need to show that NO VSS scheme works.)

   SOLUTION TO PROBLEM TWO

   Assume there is a (t, L) VSS scheme for Zelda to share a secret with $A_1, \ldots, A_L$. We show that $t-1$ of them can learn the secret!

   $A_1, \ldots, A_{t-1}$ get together. They do not know how long A_t's share is, but they know that A_t HAS a share. Let

   $$w_1, w_2, \ldots w_n$$

   be a list of ALL possible shares in lexicographic order.

   For $i = 1$ to n:

   $A_1, \ldots, A_{t-1}$ assume w_i is A_t's share. They use this to find the secret (which may be wrong) and they try to VERIFY w_i is the share. If they succeed in verifying that w_i IS the share then GREAT – that IS the share, and the secret they got with it is correct (and they stop). This WILL happen with the correct share, but not any others.

3. (30 points)

   (a) (20 points) In class we showed how to use the Paillier Public Key Crypto System and Secret Sharing to hold an election where there are TWO candidates. Find a way to hold an election with THREE candidates and V voters. You are GIVEN V and need to put conditions on N so that your scheme works.

(b) (10 points) If 1,000,000 people want to vote then how large does N have to be?

SOLUTION TO PROBLEM THREE

a)

V is given. We determine N^2 and b later.

Begin Intuition:

The three candidates are X_0, X_1, X_2.

We want to write every element in $\mathbb{Z}_M$ in a base where there are only three digits. We call the digits 0th, 1st, 2nd where 0th is the rightmost, 1st is the middle, 2nd is the leftmost.

If you want to vote for X_0 then you send a number to increase the 0th digit by 1 and leave everything else unchanged.

If you want to vote for X_1 then you send a number to increase the 1st digit by 1 and leave everything else unchanged.

If you want to vote for X_2 then you send a number to increase the 2nd digit by 1 and leave everything else unchanged.

Important Issue: We need to avoid the following – so many people vote for a candidate that her digit goes back to 0.

End Intuition

The base will be b which we determine later.

To vote for X_0 send 1 which is 001. To avoid having the 0th place get to b we need $V < b$.

To vote for X_1 send b which is 010. To avoid having the 1st place get to b^2 we need $V < b$.

To vote for X_2 send b^2 which is 100. To avoid having the 2nd place get to b^3 we need $V < b$.

From the above we will take $b = 2V$ ($V + 1$ would suffice but makes the math below messier).

All of the arithmetic is taking place in mod N^2. Hence we need that the largest possible number is $< N^2$. If all V voters vote for the 2nd candidate then the number will be: Vb^2.

$Vb^2 < N^2$

$V \times (2V)^2 < N^2$

$4V^3 < N^2$

So we take $N \geq \lceil 2V^{3/2} \rceil$.

Formally:

(a) V is given.

(b) Alice picks primes p, q, such that $N = pq \geq \lceil 2V^{3/2} \rceil$, and broadcast N. Let $b = 2V$ and broadcast this also.

(c) For voter V_i to vote X, send $c_i = ENC(1)$ to Bob.

(d) For voter V_i to vote Y, send $c_i = ENC(b)$ to Bob.

(e) For voter V_i to vote Z, send $c_i = ENC(b^2)$ to Bob.

(f) Bob computes the product of all the c_i. Call this c.

(g) Alice does (t, t) VSS secret p with $Q_1, \ldots, Q_t$.

(h) $Q_1, \ldots, Q_t$ know p hence q, so the can $DEC(c)$ to find a three-digit (in base b) number $d_2 d_1 d_0$. Let i be such that $d_i = \max\{d_0, d_1, d_2\}$. The winner is X_i.

b) If $V = 1,000,000$ then we need to take $N \geq \lceil 2V^{3/2} \rceil = \lceil 2(10^6)^{3/2} \rceil = \lceil 2 \times 10^9 \rceil = 2,000,000,000$.

END OF SOLUTION TO PROBLEM THREE

4. (20 points) Zelda wants to do $(3, 3)$ secret sharing with polynomials. The secret is 1001 which is 9 in base 2, so she uses mod 11. Zelda picks out $r_2 = 3$ and $r_1 = 7$. What shares does she give out? Give the ACTUAL NUMBER, do not just say, for example $f(1)$. (NOTE- this was an issue on the midterm when some people for Diffie Helman wrote that Alice sends $2^4 \pmod{11}$. I am asking this question now so that you DO NOT make the same MISTAKE on the FINAL.)

SOLUTION TO PROBLEM FOUR

All math is mod 11.

$f(x) = 3x^2 + 7x + 9$

Give A_1 $f(1) = 3 + 7 + 9 = 10 + 9 = -1 + 9 = 8$

Give A_2 $f(2) = 3 \times 4 + 7 \times 2 + 9 = 12 + 14 + 9 = 1 + 3 - 2 = 2$

Give A_3 $f(3) = 3 \times 9 + 7 \times 3 + 9 = 3 \times -2 + 21 - 2 = -6 + 10 - 2 = 2$

END OF SOLUTION TO PROBLEM FOUR

5. (20 points) In the last problem Zelda had secret 9 and used mod 11. The players DO know the length of the secret (that is not considered a leak of info). The players DO know that they work mod 11. Does the choice of 11 leak any information? Explain your answer.

   SOLUTION TO PROBLEM FIVE

   YES INFORMATION IS LEAKED! Once they know the secret is length 4 there are 16 possibilities for it. But once they know they are working mod 11 they know the secret is one of

   0000,0001,0010,0011,0100,0101,0110,0111,1000,1001,1010.

   Thats only 11 possibilities. So they know five strings the secret is NOT. Thats information!

   END OF SOLUTION TO PROBLEM FIVE