hw10 Solutions

hw10 Problem 2: No VSS with All Powerful Players

Problem 2

Let $1 \leq t \leq L$. 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.

Problem 2 SOLUTION

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

$w_1, w_2, \ldots$ be $\{0, 1\}^*$ in lex order.
For $i = 1$ to ∞:
$A_1, \ldots, A_{t-1}$ 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.

hw10 Problem 3: Voting with 3 Candidates

Problem 3

a) 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) If 1,000,000 people want to vote then how large does N have to be?

Problem 3: Solution One

Set up three votes:

1. Vote for Alice (1) or NOT Alice (0), using what I did in class.
2. Vote for Bob (1) or NOT Bob (0), using what I did in class.
3. Vote for Carol (1) or NOT Carol (0), using what I did in class.

Can find all of the totals.
Since the math is all mod N^2 need

$$1,000,000 < N^2$$

So can take $N = 1000$.

Caveat: Someone can vote for Alice AND Bob. Is that bad?
Bonus: works for approval voting!

Problem 3: Solution Two. Example

V is given. We determine N^2 and b later.
EXAMPLE:
If there were 9 voters then do the following:
The three candidates are X_0, X_1, X_2.
To vote for X_0 vote use $10^0 = 1$
To vote for X_1 vote use $10^1 = 10$
To vote for X_2 vote use $10^2 = 100$

Lets say:
X_0 gets 3 votes, contributes $3 \times 10^0 = 3$.
X_1 gets 2, votes, contributes $2 \times 10^1 = 20$
X_2 gets 4, votes, contributes $4 \times 10^2 = 400$
If you add these together you get 423.
Note: The digits ARE the number of votes!
Important: Could add without carries since 9 people and base 10.

Problem 3: Solution Two. General

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

1. Alice picks $N = pq$, b, broacasts N, b.
2. Voter V_i votes X_0 by $c_i = ENC(1)$ to Bob.
3. Voter V_i votes X_1 by $c_i = ENC(b)$ to Bob.
4. Voter V_i votes X_2 by $c_i = ENC(b^2)$ to Bob.
5. Bob computes $c = c_1 \cdots c_V \pmod{N^2}$. $c = d_2 d_1 d_0$ in base b.
6. Let i be such that $d_i = \max\{d_0, d_1, d_2\}$. The winner is X_i.

Take $b \le V + 1$ to avoid overflows from one digit to the next.
Max the sum could be is all vote for X_2. Sum is Vb^2. Need:
$Vb^2 < N^2$ so $\sqrt{V}b < N$. We take $b = V + 1$, so $\sqrt{V}(V + 1) < N$.

If $V = 1,000,000$ then $\sqrt{V}(V + 1) = 1,000,001,000$, so thats N.

Problem 4

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 isredDO NOT make the same MISTAKE on the FINAL.

Problem 4. Solution

All math is mod 11.
$f(x) = 3x^2 + 7x + 9$

Give A_1 $f(1) = 8$
Give A_2 $f(2) = 2$
Give A_3 $f(3) = 2$

Note: Is it OKAY that $f(2) = f(3)$. YES. Nobody knows this until $f(2)$ and $f(3)$ are in the same 3-set. So does not leak anything. Usual reasons for why secret sharing works still work.

Problem 5

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.

Problem 5. Solution

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!