Problem 1 Secret Sharing

Problem 1 - (n, n) secret splitting.

Given a secret s and n players, the dealer generates n − 1 random strings as first n − 1 shares and last share as the bitwise XORing of s with all the other n − 1 shares. Answer the following questions in detail.

1. Can n players generate s? Why or Why not?

2. Can any n − 1 players generate s? Why or why not?

My solution:

My analysis is based on the theorem (slides of Mar 20):

According (N,T) SECRET SHARING we learned: Given a secret s and n players

a. Any t or more players can recover s

b. Less than t players have no information about s

The parameters N and T typically refer to the number of players and the minimum number of players required to reconstruct the secret, respectively, in a (T, N) threshold secret sharing scheme. The threshold T specifies the minimum number of shares required to reconstruct the secret, while the parameter N specifies the total number of shares that are generated. Hence, in the (n, n) secret splitting scheme, a secret s is split into n shares, and all n players can generate the secret s by XORing all n shares together. According to the definition, any n-1 players or fewer cannot generate the secret s because they are missing at least one share.

Hence,

1. **Can n players generate s? Why or Why not?**

   Way 1. (Based on the understanding that the secret s is given such that the value of the secret is clear. The slide P4 of March 20 says the secret s held by a "dealer", then we can consider it can be used to get the last share by XORing in this case)

   Yes, n players can generate s. Each player can XOR their share with the others to generate s. For example, if there are 3 players with shares s1, s2 and s3, then s can be generated by calculating s1 XOR s2 XOR s3. Since the last share is generated by XORing s with all the other n-1 shares, it can be represented as s XOR (s1 XOR s2 XOR ··· XOR sn-1). When all n shares are XORed together, the result is (s1 XOR s2 XOR ··· XOR sn-1) XOR (s XOR (s1 XOR s2 XOR ··· XOR sn-1)). Since any number XORed with itself is 0 and any number XORed with 0 is itself, this simplifies to just s. When all n shares are XORed together, the n-1 shares cancel out and only the secret 's' remains.

   Note: I use Way1 to solve this question based on the vague description of this question. It gave us the secret s but does not mention it's held by a dealer, we can consider the secret s is given clear. Then the last share can be calculated by XORing (n-1) shares with S. Based on the example I mentioned above, let me explain it with a numerical example.

Let's say we have a secret s = 1010 and 3 players. The dealer generates two random strings as the first two shares: 1100 and 0011. The last share is calculated as the bitwise XOR of s with the first two shares: 1010 XOR 1100 XOR 0011 = 0101. Now, if we XOR all three shares together: 1100 XOR 0011 XOR 0101 = 1010, which is the original secret s. **Hence, in this case, n players can generate s. However, if the given secret s is unknown or it cannot be used to get the last share by XORing in this question. Then the solution should be Way 2.**

Way2. (Based on the understanding regarding the vague description. Let's say the secret s is given which cannot be used to calculate the last share directly)
No, n players cannot generate s. Here is the reason: If the secret s is given but the value of the secret s is unknown or cannot be used to calculate the last share, then the dealer cannot calculate the last share as the bitwise XOR of s with all the other n − 1 shares. According to the definition, any n-1 players or fewer cannot generate the secret s because they are missing at least one share.

2. **Can any n − 1 players generate s? Why or why not?**
No, any n − 1 players cannot generate s. Because they are missing at least one share. In this scheme I explained above, all n shares are required to generate the secret s. Any n-1 players cannot generate s without the last share or the dealer's secret key. The last share is dependent on all n shares, the players cannot obtain any information about s without it.

Problem 1 - Shamir (k,n)-threshold secret sharing.

As discussed in the class, Shamir (k, n)-threshold secret sharing scheme chooses a large prime p. Then the message M is represented as a number (mod p):

$$\boldsymbol{s(x) = M + s_1 x + s_2 x^2 + \cdots + s_{k-1} x^{k-1} (mod p)}$$

1. You set up a (k, n) = (2, 30) Shamir threshold scheme, working mod the prime p =

101. Two of the shares are (1,13) and (3,12). Another person received the share (2, *). What is M? What is the value of *?

My solution:
Note: In a Shamir threshold scheme, the degree of the polynomial is k-1. The coefficients of the polynomial used to represent the secret message are chosen randomly from the prime field.
Substituting the two shares (1, 13) and (3, 12) into the polynomial s(x):
(1) s(1) = M + s_1 = 13 (mod 101)
(2) s(3) = M + 3s_1 = 12 (mod 101)

Hence, s(3) - s(1) = 2s1 = -1 (mod 101) = 100. Hence, s1 = $\frac{100}{2}$ (mod 101) = 50

Note: Quotient × Divisor + Remainder = Dividend → -1 × 101 + 100 = -1

Substituting s1 = 50 in s(1) = M + s_1 = 13 (mod 101)→ M + 50 = 13 (mod 101)
→ M = 13 -50 (mod 101)
→ M = -37 (mod 101)
→ M = 64

Note: -37 (mod 101), since the prime is 101, to get the smallest non-negative integer: -37 + prime = -37+101=64.

Hence, M = 64.

Since s(x) = M + s_1 * x (mod p) → s(x) = 64 + 50 * x (mod 101),
Substituting the share (2, *): s(2) = 64 + 50 * 2 (mod101)
= 64 + 100 (mod101)
= 164 (mod101) = 63.

Hence, the value of * is 63.

2. In a (3, 5) Shamir secret sharing scheme with modulus p = 17, the following were given to Alice, Bob, Charles: (1, 8), (3, 10), (5, 11). Calculate the corresponding Lagrange interpolating polynomial, and identify the secret M.

My solution:

(3, 5) means a secret M is shared by dividing it into 5 shares (also called shadows), in such a way that the secret can only be reconstructed if at least k of the n shares are combined.

Given (x_i, y_i) are the points corresponding to Alice, Bob, and Charles:
Alice: (x_0, y_0) = (1, 8),
Bob: (x_1, y_1) = (3, 10),
Charles: (x_2, y_2) = (5, 11)

According to LAGRANGE INTERPOLATING POLYNOMIALS:

$$P_n(x)=\sum_{k=0}^{n} y_k L_{n,k}(x) \equiv \sum_{k=0}^{n} y_k\left[\prod_{i=0,i\neq k}^{n}\frac{x-x_i}{x_k-x_i}\right] \bmod p$$

Here is the process to calculate the corresponding Lagrange interpolating polynomial.

Alice: (x_0, y_0) = (1, 8), Bob: (x_1, y_1) = (3, 10), Charles: (x_2, y_2) = (5, 11)

Substituting above sharing:

$$L_0(x) = \frac{(x-x1)(x-x2)}{(x0-x1)(x0-x2)} = \frac{(x-3)(x-5)}{(1-3)(1-5)} = \boldsymbol{\frac{(x-3)(x-5)}{8}}$$

$$L_1(x) = \frac{(x-x0)(x-x2)}{(x1-x0)(x1-x2)} = \frac{(x-1)(x-5)}{(3-1)(3-5)} = -\boldsymbol{\frac{(x-1)(x-5)}{-4}}$$

$$L_2(x) = \frac{(x-x0)(x-x1)}{(x2-x0)(x2-x1)} = \frac{(x-1)(x-3)}{(5-1)(5-3)} = \frac{(x-1)(x-3)}{8}$$

Correspondingly,

$$y_0L_0(x) = y_0 * \frac{(x-x1)(x-x2)}{(x0-x1)(x0-x2)} = 8 * \frac{(x-3)(x-5)}{(1-3)(1-5)} = (x-3)(x-5) = \boldsymbol{x^2-8x+15}$$

$y_1L_1(x) = y_1 * \frac{(x-x0)(x-x2)}{(x1-x0)(x1-x2)} = 10 * \frac{(x-1)(x-5)}{(3-1)(3-5)} = -\frac{5}{2}(x\text{-}1)(x\text{-}5) = -\frac{5}{2}(x^2\text{-}6x\text{+}5) = \boldsymbol{-\frac{5}{2}x^2+15x-\frac{50}{2}}$

$y_2L_2(x) = y_2 * \frac{(x-x0)(x-x1)}{(x2-x0)(x2-x1)} = 11 * \frac{(x-1)(x-3)}{(5-1)(5-3)} = \frac{11}{8}(x-1)(x-3) = \boldsymbol{\frac{11}{8}x^2 - \frac{11}{2}x + \frac{33}{8}}$

We got the Lagrange interpolating polynomial $P_n(x_i)=y_i$, 0≤i≤n below:

$P_n(x) = \sum_{k=0}^{n} y_k L_{n,k}(x) = y_0 L_{n,k}(0) + y_1 L_{n,k}(1) + y_2 L_{n,k}(2)$

$\equiv [\, (x^2 - \frac{5}{2}x^2 + \frac{11}{8}x^2) - 8x + 15x - \frac{11}{2}x + (15 - \frac{50}{2} + \frac{33}{8})\,]$ mod17

$= [\frac{-1}{8}\, x^2 + \frac{3}{2}x + \frac{-47}{8})]$ mod17

Based on Lagrange interpolation polynomial, choose a large prime p, the message M is represented as a number (mod p):

SHAMIR THRESHOLD SCHEME: Given k points on the plane (x_1 , y_1), . . . , (x_k , y_k), all x_i distinct, there exists a unique polynomial f of degree ⩽ k − 1, s.t. f (x_i) = y_i for all i. Hence, the degree of the polynomial f in this question is k-1=3-1=2.

Hence, in this question, each share is represented by a point on a polynomial of degree 2 over a finite field of modulus p=17.

$s(x) \equiv M + s_1x + s_2x^2 + \cdots + s_{k-1}x^{k-1}(mod p)$

$(x_i, y_i), i = 1,2,\ldots,n; y_i \equiv s(x_i)(mod p)$

Hence, the polynomial is: $\boldsymbol{s(x) \equiv M + s_1x + s_2x^2(mod p)}$

Substituting sharing: Alice: (x_1, y_1) = (1, 8), Bob: (x_2, y_2) = (3, 10), Charles: (x_3, y_3) = (5, 11)

$s(1) = 8 \equiv M + s_1 + s_2(mod 17)$

$s(3) = 10 \equiv M + 3s_1 + 9s_2(mod 17)$

$s(5) = 11 \equiv M + 5s_1 + 25s_2(mod 17)$

A. s(3) – s(1) = $2s_1 + 8s_2$ = 2 (mod17)

B. s(5) – s(3) = $2s_1 + 16s_2$ = 1 (mod17)

B-A = $8s_2$ = -1 (mod17) → $s_2 = \frac{16}{8}$ (mod17) = 2 (mod17) = 2

Note: -1 (mod17) = 16

Substituting s_2 =2 into $2s_1 + 8s_2$ = 2 (mod17) → $2s_1$ + 8*2 = 2 (mod17)

→ $2s_1$ =-14 (mod17)

→ s_1 =-7(mod17) = 10

Substituting s_1 = 10, s_2 = 2 into $s(1) = 8 \equiv M + s_1 + s_2(mod 17)$

M + 10 + 2 (mod17) = 8

M = 8-10-2 (mod17) = -4 (mod17) = 13

Hence, M = 13.

Problem 2 Zero Knowledge Proof (ZKP)

Recall that a ZKP protocol is a protocol that involves a prover and a verifier that enables the prover to prove to a verifier without revealing any information other than the statement itself and to any other parties.

Problem 2 - Rethinking The Ali Baba Cave.

Are the following solutions satisfying the ZKP property?
1. Assuming Victor is wearing a camera that records the whole transaction between Peggy and Victor. The only thing the camera will record is Victor shouting "A!" (or "B!") and Peggy appearing at A or (B). Is this a ZKP protocol? Why or why not?

My solution:
No, it does not satisfy the ZKP property.
Here is the reason:
According to the definition of Zero-Knowledge Proof (ZKP) protocol on the slides (P3), the protocol involves a prover and a verifier that enables the prover to prove to a verifier without revealing any other information. In the original case, Peggy is the prover and Victor is the verifier. In this case, Peggy as the prover is clear. However, the verifier in this case does not satisfy the definition. In this case, the verifier could be either the camera or Victor. If the camera as the verifier, it only records the scenario but it does not verify Peggy knows the secret word without revealing it. If Victor is the verifier wearing a camera that records the whole transaction, the camera is superfluous. Because the protocol should only establish connection between Peggy and Victor. A ZKP protocol allows one party (the prover) to prove to another party (the verifier) that they possess certain knowledge without revealing the knowledge itself.

2. Another way is that: Peggy could prove to Victor that she knows the magic word, without revealing it to him, in a single trial. Specifically, both Victor and Peggy go to the entrance of the cave, then Victor can watch Peggy go in through the path A and come out through the path B. Is this a ZKP protocol? Why or why not?

My solution:
No, it does not satisfy the ZKP property.
Here is the reason:
In this scenario: it is a single trial. The protocol in this scenario cannot succeed with overwhelming probability in a single trial. This scenario does not satisfy the completeness property of a zero-knowledge proof (ZKP) protocol. Completeness of ZKP requires that if the statement is true, an honest prover can convince an honest verifier of its truth with overwhelming probability. In the single trial, if Peggy goes in through the path A and come out through the path B successfully. It does satisfy "Everything that is true has a proof" or

"Everything that is provable is true". However, it does not satisfy "Given honest prover and honest verifier, the protocol succeeds with overwhelming probability". This scenario lacks completeness.

Problem 2 - The Sudoku Game

Alice wants to prove to Bob that she has solved a Sudoku puzzle that no one else has ever solved, but does not want her solution known to anyone. Can you help her design a solution based on the ZKP (using non-crypto language)? Prove the completeness, soundness, and zero-knowledge. More information about the sudoku game can be seen in https://sudoku.com/.

My solution:

We can try to use a Zero-Knowledge Proof (ZKP) protocol based on graph isomorphism.

Step 1. Alice constructs a graph that represents her Sudoku solution. Each vertex in the graph represents a cell in the Sudoku puzzle, and each edge represents a constraint between two cells (e.g., two cells in the same row, column, or region must have different values).

Step 2. Alice constructs another graph that is isomorphic to the first graph (i.e., it has the same structure but the vertices are labeled differently). She sends this second graph to Bob as her commitment.

Step 3. Bob then challenges Alice by asking her to either reveal the mapping between the two graphs (i.e., show how the vertices in the first graph correspond to the vertices in the second graph) or to construct a third graph that is isomorphic to one of the first two graphs but not the other.

Step 4. If Alice can successfully respond to Bob's challenge, she has proven that she knows a valid solution to the Sudoku puzzle without revealing her solution.

This protocol satisfies the properties of completeness, soundness, and zero-knowledge:

- **Completeness:** If Alice knows a valid solution to the Sudoku puzzle, she can always construct the required graphs and respond to Bob's challenge correctly. If Alice knows a valid solution to the Sudoku puzzle, it can be considered "Everything that is true has a proof". Bob and Alice can perform many experiments base on this solution to ensure the protocol succeeds with overwhelming probability.
- **Soundness**: If Alice does not know a valid solution to the Sudoku puzzle, she cannot construct the required graphs or respond to Bob's challenge correctly with non-negligible probability.
- **Zero-knowledge:** Bob learns nothing about Alice's solution to the Sudoku puzzle. Only Alice herself knows a valid solution and her proof does not leak any additional information.