Problem 1 (30 Points): Secret Sharing

(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. **5 Points.** Can n players generate s? Why or Why not?
2. **5 Points.** Can any $n-1$ players generate s? Why or why not?

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):

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

1. **10 Points.** 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 (3 points)? What is the value of * (3 points)?
2. **10 Points.** 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.

Problem 2 (30 Points): 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.
Rethinking The Ali Baba Cave. Are the following solutions satisfying the ZKP property?

1. **5 Points.** 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?
2. **5 Points.** 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?

The Sudoku Game (20 Points). 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/`.

Problem 3 (40 Points): Private Information Retrieval

In the slides, we talked about using homomorphic encryption to perform private information retrieval (PIR). Specifically, suppose the server holds a dataset $\mathcal{D}$ of n integers $\mathbf{d} = [d_1, d_2, \cdots, d_n]$ encrypted under the client's key. For the server to select an element, e.g., d_i, obliviously, the client sends an encrypted selection binary vector $\mathbf{s}$ of length n containing 0s everywhere except for a 1 in the position i of the element to be selected. The server then computes the dot product of $\mathbf{d}$ and $\mathbf{s}$ using the homomorphism, with the encrypted result $r = \sum_{j=1}^{n} d_j s_j$, and sends it to the client, who can decrypt it.

1. **Protocol design (15 Points).** Please design a protocol based on (somewhat/fully) homomorphic encryption to achieve the goal.
2. **Implementation (25 Points).** This simple dot-product protocol for a database of a specific size can be run by the the SHEEP platform: `https://github.com/alan-turing-institute/SHEEP`.

   SHEEP supports a number of fully homomorphic encryption libraries (inlcuding HElib, SEAL TFHE, and libpallier). Please use the SHEEP platform to realize the PIR, where the server holds $\mathbf{d} = [2, 4, 6, 8, 10, 1, 3]$ and the client wants to retrieve each element.

   Submission requirement: (1) screenshots of the major steps of your answer, and (2) source code files – all named with the prefix "hw4-3-".