Begin each problem on a separate page.

**Problem 1 Oblivious Transfer**

Recall that in the 1-out-of-2 oblivious transfer functionality, the sender has two bits $m_0$ and $m_1$, and the receiver has a bit $b$. At the end of the protocol, the receiver is able to compute $m_b$, but learn nothing about $m_{1-b}$. Meanwhile, the sender learns nothing about the receiver’s choice $b$. In class, we constructed a protocol for 1-out-of-2 oblivious transfer that is secure against honest-but-curious adversaries.

Imagine that there is a physical device that implements 1-out-of-2 oblivious transfer for malicious adversaries. Show how to use this physical mechanism to achieve 1-out-of-3 oblivious transfer against malicious adversaries. You do not have to provide a formal definitions or proofs, but have to argue that:

(a) Your construction computes 1-out-of-3 oblivious transfer correctly.
(b) The sender does not learn the choice of the receiver.
(c) The receiver learns only one out of the 3 bits.

Hint: You might need to use the 1-out-of-2 device more than once.

**Problem 2 Secure 3-Party Computation**

In class we saw Yao’s construction of secure 2-party computation protocols, assuming honest but curious adversaries. Give a similar, constant-round protocol for secure 3-party computation. Informally (but convincingly) justify that your protocol is secure and correct.

**Problem 3 Combining ZK proofs**

Construct a ZK proof with soundness $1/2$ for the language $L = \{(G,H) \mid G$ or $H$ has a Hamiltonian path$\}$. Do not transform the input instance (e.g., using Cook’s reduction or some gadget, into a regular graph Hamiltonicity instance). Instead, construct a protocol based on Blum’s Hamiltonicity protocol. Your techniques should apply analogously for the graph isomorphism protocol. Show that your protocol is complete, sound, and zero knowledge. Hints:

- What would you do if $L$ requires both $G$ and $H$ to have Hamiltonian paths?
- In fact, the same techniques can give a ZK protocol for the language $L = \{(G,H_1,H_2) \mid G$ has a Hamiltonian path, or $H_1$ is isomorphic to $H_2\}$.

Identify a general class of ZK protocols that can be combined using your techniques.