Interactive Protocol

A₁

A₅ A₂

A₄ A₃

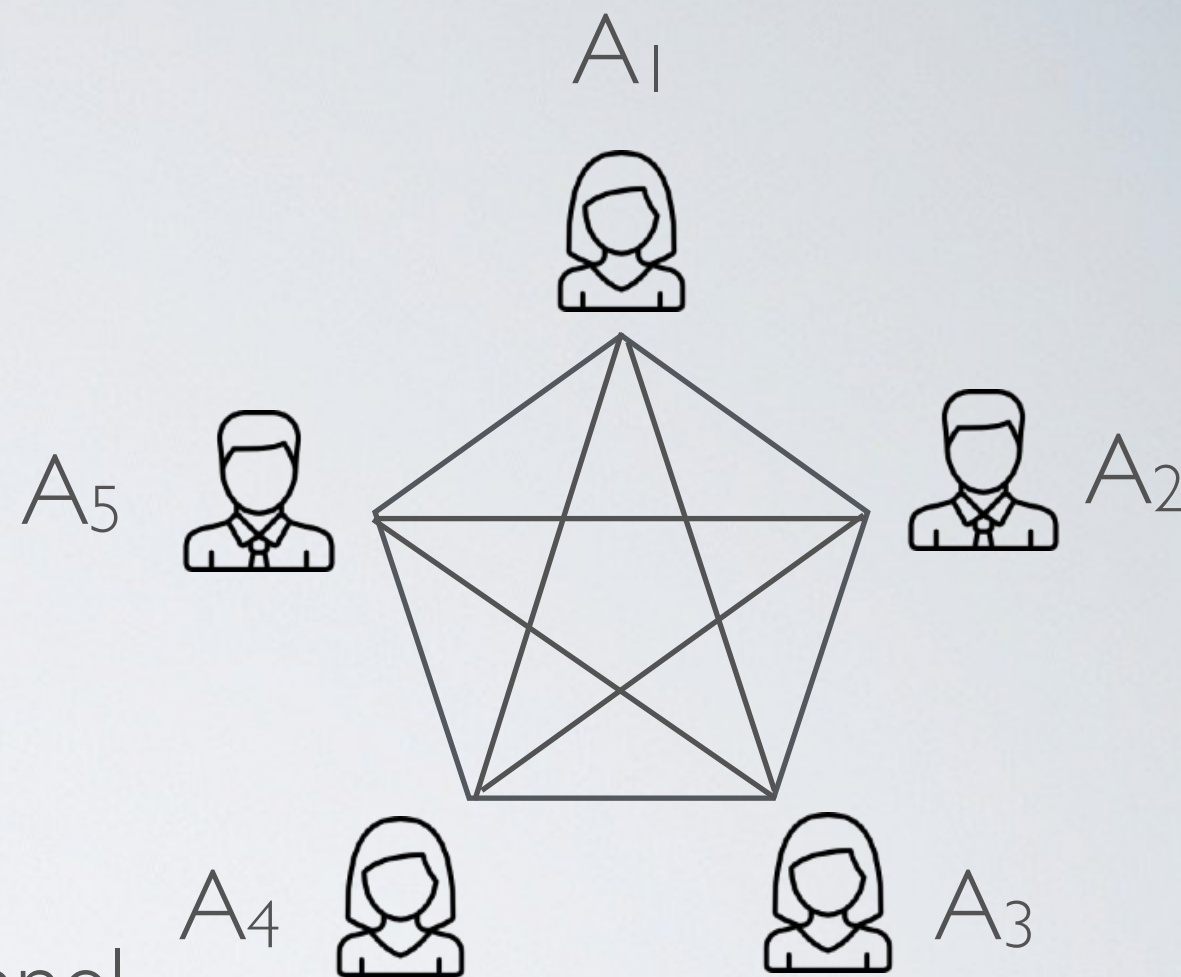**System Hypothesis**

- Synchronous communication channel

- Each participant share a unique symmetric key with each other

- Mallory can read, modify and forge message send over the network

Goals

- When two participant exchange a message, the system should protect the confidentiality and integrity of the message

Using Authenticated Encryption

$$A, E_k(m)$$

$$E_k(m')$$