

Design of a cryptography protocol

The hypothesis on the system

- **What is the network model?**
bandwidth, latency, reliability, message ordering, synchronous vs asynchronous
- **What trusted setup is assumed?**
pre-shared keys, key generation
- **How powerful are the parties vs. attacker?**
computing power, source of randomness
- **Which adversary model is considered?**
outsider vs insider, passive vs active, man-in-the-middle, man-at-the-end, corruption
- **What kinds of failures are tolerated?**
crash faults, byzantine faults
- **What exact security properties are being claimed?**
confidentiality, integrity, authentication, non-repudiation, forward secrecy

Example 1 - **Interactive Protocol**

