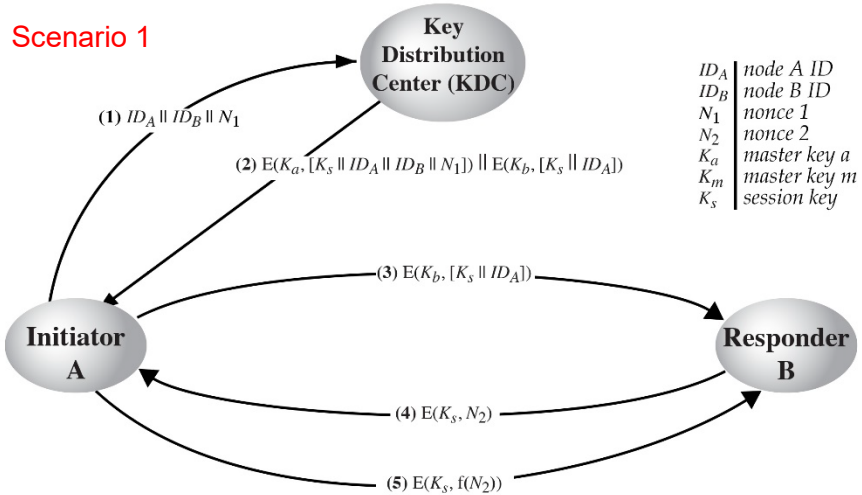
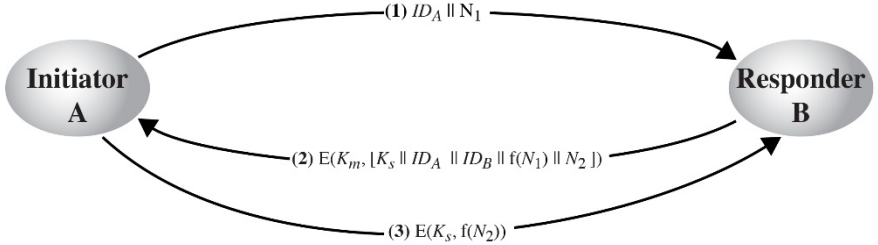
Question 2:

We have the following two Key Distribution scenarios:

Scenario 1



Scenario 2



Question 2:

- **A)** In scenario 1, should **nonce 1** always differ between different requests for a logical connection? Why?
- **B)** In scenario 1, is Responder B confident that the **session key** was produced by the KDC? Why?
- **C)** In scenario 1, assume that steps 4 and 5 are not performed. Is this dangerous? Why?
- **D)** Which scenario is the Decentralized one? What are the main advantages/disadvantages of each?
- **E)** What is the difference between **Session keys** and **Master keys**?
  What problem is being addressed in end-to-end key distribution with their use?