

## **5.2 Question 2**

**5.2.A** In scenario 1, should nonce 1 always differ between different requests for a logical connection? Why?

**5.2.B** In scenario 1, is Responder B confident that the session key was produced by the KDC? Why?

**5.2.C** In scenario 1, assume that steps 4 and 5 are not performed. Is this dangerous? Why?

**5.2.D** Which scenario is the Decentralized one? What are the main advantages/disadvantages of each?

**5.2.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?