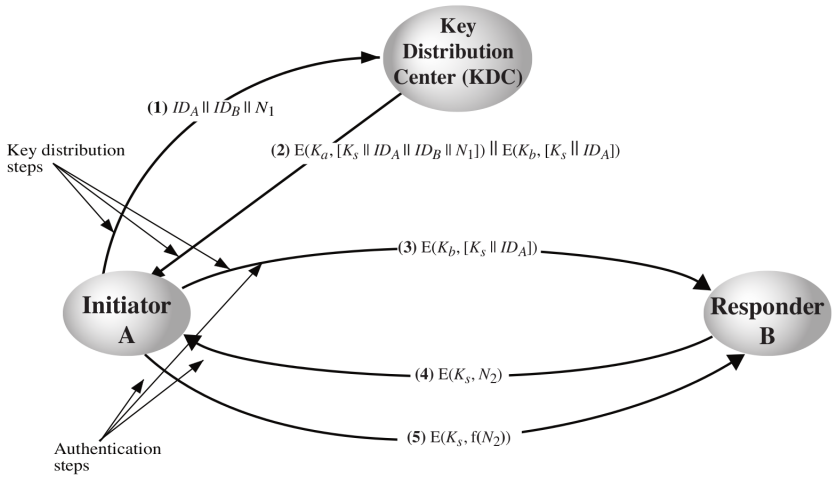
CSS322 – Quiz 6

Name: _____ ID: _____ Marks: ____ (4)

Question 1 [4 marks]

Consider the mechanism below. Assume the number of users in the network is the last two digits of your ID (A and B are two of the users).



(a) Excluding session keys, how many keys must the KDC know for this mechanism to work?

(b) If user A has applied this mechanism to communicate with all other users in the network, then how many keys does user A know?

(c) What is a disadvantage of this mechanism compared to the decentralised key distribution (in previous quiz)?

(d) If an attacker replayed message (3), then explain how this attack will be detected.