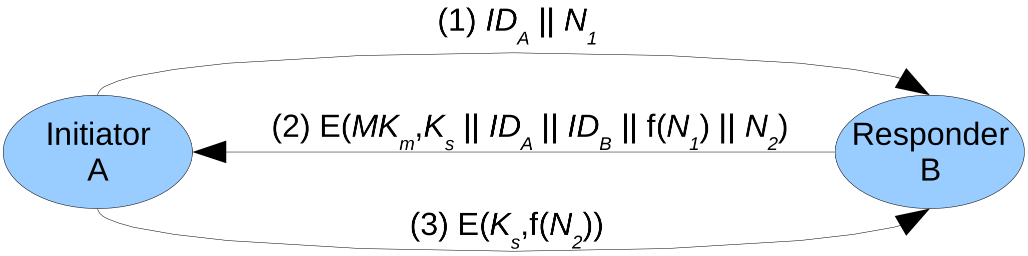
CSS322 – Quiz 3

Name: ____

ID: ______________________________ Mark: __________ (out of 10)

Question 1 [5 marks]

Below is an example de-centralised key distribution protocol that may be used. MK_m is the master key shared between two nodes A and B (this sharing must be done manually/physically), and K_s is the session key.



a) How many master keys are needed in a network using this key distribution protocol if there are 20 nodes in the network? [2 marks]

b) If a KDC (using the protocol covered in the lecture) was used instead of the above de-centralised protocol, how many master keys would be needed in the network? [1.5 marks]

c) What is the benefit of using the de-centralised protocol compared to simply using the physically exchanged master keys for encrypting the session data? [1.5 marks]

Question 2 [1.5 marks]

Consider the following algorithms/concepts: Linear Congruential Generator, DES, KDC. Which *cannot* be used to generate random numbers? If more than one cannot be used, you must write both; if all of them can be used, then write “all appropriate”.

Question 3 [3.5 marks]

Calculate the following (write answer in space provided, show any calculations below, you cannot use a calculator):

a) $\Phi(18)$ Answer: _________

b) $\Phi(37)$ Answer: _________

c) $3^{24} \bmod 25$ Answer: _________