1a)-b) see problem sheet on Time Service

1c)

2) a)

I) This protocol allows A to initiate a symmetric key K\_AB, pass it to a server S (so S has a copy of this key) and then S forwards this key to B so that A and B can now send encrypted messages to each other. This assumes A and B already has key K\_AS and K\_BS respectively.

Ii)

msg3: B --> A: {N\_B}\_K\_AB;

Msg4: A --> B: {N\_B – 1}\_K\_AB

B) google it 😊 don’t tell me what to do 😡

C)