5 Software and Security Engineering (RJA)

The public-key Needham-Schroeder protocol is as follows:

$$\begin{array}{rcl} A & \longrightarrow & B : \{NA, A\}_{KB} \\ B & \longrightarrow & A : \{NA, NB\}_{KA} \\ A & \longrightarrow & B : \{NB\}_{KB} \end{array}$$

(*a*) Explain the notation used and the purpose of the protocol. [4 marks]

(*b*) What is wrong with this as a protocol design and how might this flaw be fixed? [10 marks]

(*c*) What would we still have to check about an implementation? [6 marks]