5 Software and Security Engineering (RJA)

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

\[
\begin{align*}
A & \rightarrow B : \{NA, A\}_{KB} \\
B & \rightarrow A : \{NA, NB\}_{KA} \\
A & \rightarrow B : \{NB\}_{KB}
\end{align*}
\]

(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]