2010 Paper 7 Question 13

Security

Woo & Lam proposed a protocol that would enable a client A to log on to a server B using an authentication service S.

$$\begin{aligned}
&\text{A} \rightarrow \text{B}: \ A \\
&\text{B} \rightarrow \text{A}: \ N_B \\
&\text{A} \rightarrow \text{B}: \ \{N_B\}_{KAS} \\
&\text{B} \rightarrow \text{S}: \ \{A, \{N_B\}_{KAS}\}_{KBS} \\
&\text{S} \rightarrow \text{B}: \ \{N_B\}_{KBS}
\end{aligned}$$

(*a*) Explain the protocol notation. [4 marks]

(*b*) Explain why the protocol is insecure. [12 marks]

(*c*) How should it be fixed? [4 marks]