2006 Paper 8 Question 7

Security

The Needham–Schroeder protocol is defined as

1. $A \longrightarrow S : A, B, N_A$
2. $S \longrightarrow A : \{N_A, B, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$
3. $A \longrightarrow B : \{K_{AB}, A\}_{K_{BS}}$
4. $B \longrightarrow A : \{N_B\}_{K_{AB}}$
5. $A \longrightarrow B : \{N_B - 1\}_{K_{AB}}$

(a) Explain the symbolism, and the purpose of the messages. [5 marks]

(b) Explain the "bug" in the protocol. [5 marks]

(c) Is the bug actually a vulnerability if one can assume (as the Needham–Schroeder paper does) that all principals execute the protocol faithfully? If not, why is it important? [5 marks]

(d) Describe how *one* modern protocol derived from Needham–Schroeder deals with the issue. [5 marks]