## Homework 10

- 1. What are the main disadvantages of the following protocol that establishes a mutual key between two parties *A* and *B* with the help of a mutually trusted third party *S*:
  - $A \rightarrow S: A, B$   $S \rightarrow A: \{K_{AB}\}_{K_{AS}} \text{ and } \{\{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$   $A \rightarrow B: \{K_{AB}\}_{K_{BS}}$  $A \rightarrow B: \{m\}_{K_{AB}}$
- 2. In the context of buffer-overflow attacks, explain briefly what is meant by a *NOP-sledge*.