

# The Needham-Shroeder symmetric protocol for key exchange

## Assumptions

- 4 principals : Alice, Bob, Mallory, Key Distribution Server
- S shares a key with A, B and M respectively  $K_{as}$ ,  $K_{bs}$ ,  $K_{ms}$
- A, B, M and S talk to each other using the same protocol

## Goals

When two parties want to engage in the communication, they want to

1. make sure that they talk to the right person (authentication)
2. establish a session key

# The vulnerable version of the protocol (1978)

