The Needham-Schroeder symmetric protocol for key exchange

Assumptions

- 4 principals : **A**lice, **B**ob, **M**allory, Key Distribution **S**erver
- **S** shares a key with **A**, **B** and M respectively $\mathbf{K_{as}}$, $\mathbf{K_{bs}}$, $\mathbf{K_{ms}}$
- **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)