

# Assumptions and Goals

## Assumptions

- 4 principals : **A**lice, **B**ob, **M**allory and a Public-Key **S**erver
- Alice, Bob, Mallory and the Server have generated their own public/private key pair
- Alice, Bob and Mallory know the Server's public key **K<sub>ps</sub>**
- **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 make sure that they talk to the right person (authentication)

# The vulnerable version (1978)

