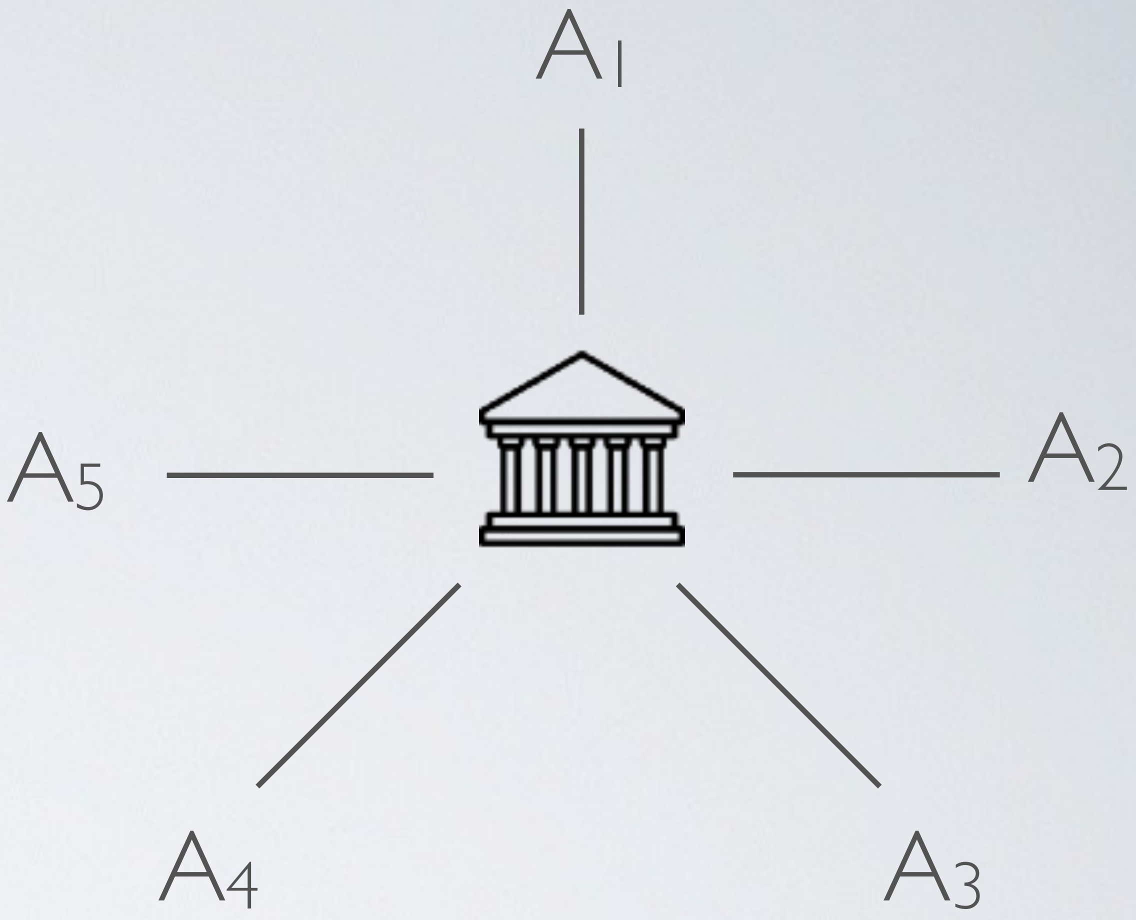
(Better) centralized solution



A_1, A_2 … A_5 can talk to the KDC (Key Distribution Center)

- ➡ When A_i and A_j want to talk, the KDC can generate a new key and distribute it to them
- ◉ We still have n keys to distribute somehow using a secure channel
- ◉ The KDC must be trusted
- ◉ The KDC is a single point of failure
- ➡ The is how *Kerberos* works

The Needham-Shroeder 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 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