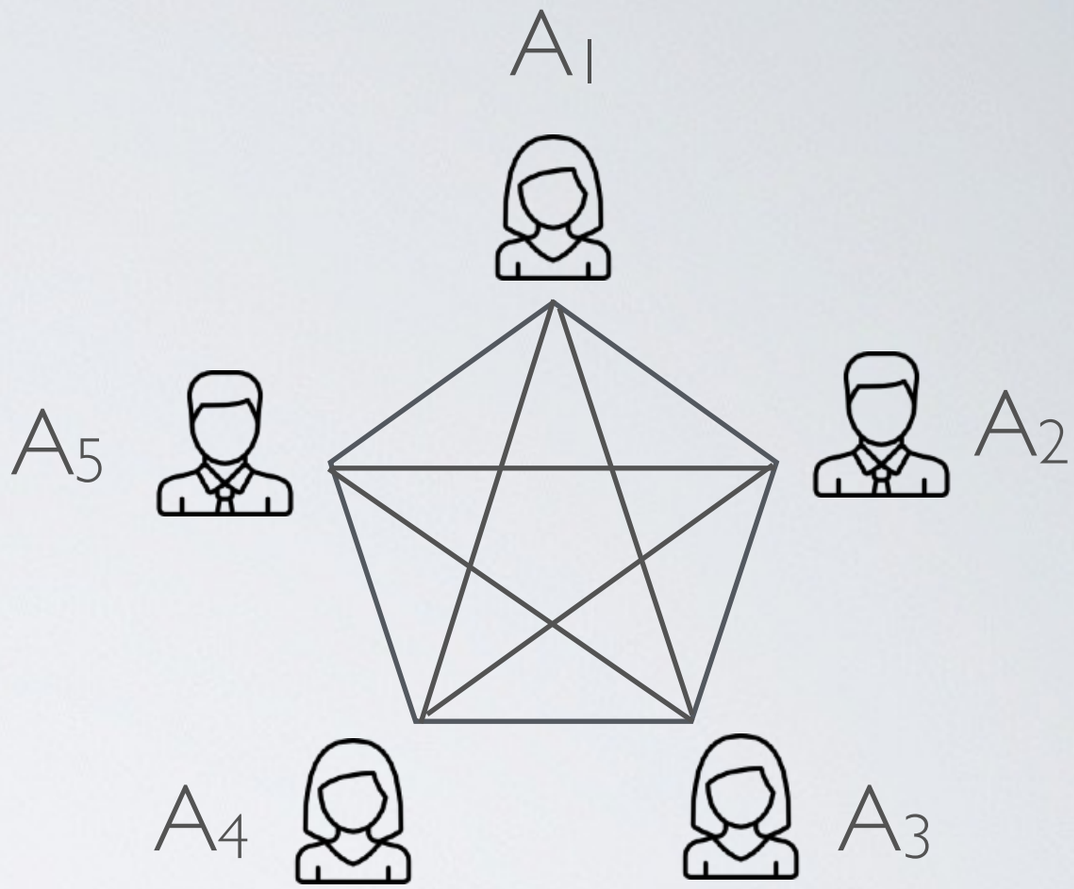
Naive Key Management

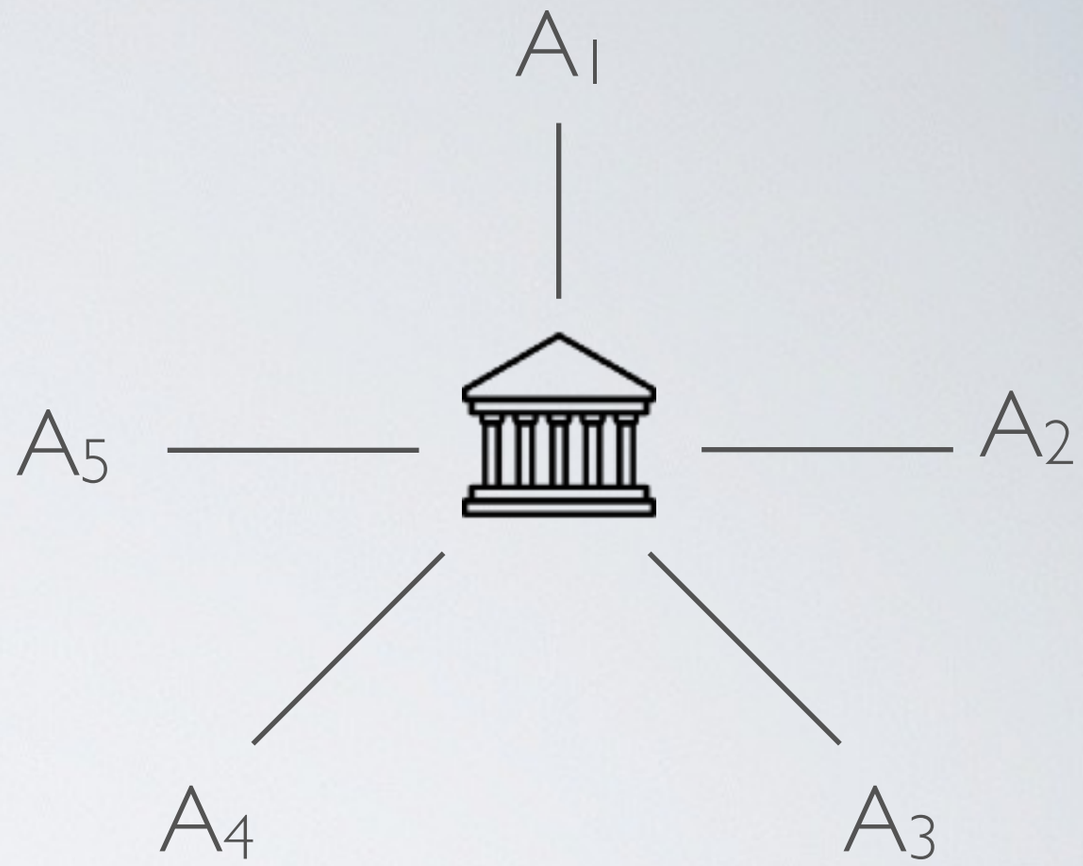


$A_1, A_2 \ldots A_5$ want to talk

➡ Each pair needs a key : **n (n-1) / 2** keys

◉ Keys must be exchanged physically using a secure channel

(Better) centralized solution



$A_1, A_2 \ldots A_5$ 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