

One major issue

Key distribution

If $A_1, A_2 \dots A_5$ want to talk, then n public keys must be distributed physically to each user using a secure channel

Why not?



K_{SB}, K_{pB}

$\text{Sign}_{skB}(\text{"I'm Bob"}, K_{pB})$



K_{SM}, K_{pM}

$\text{Sign}_{skM}(\text{"I'm Bob"}, K_{pM})$