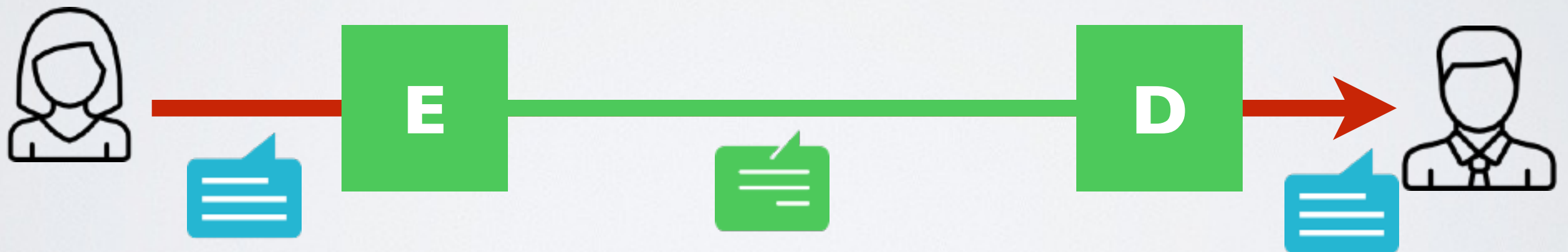
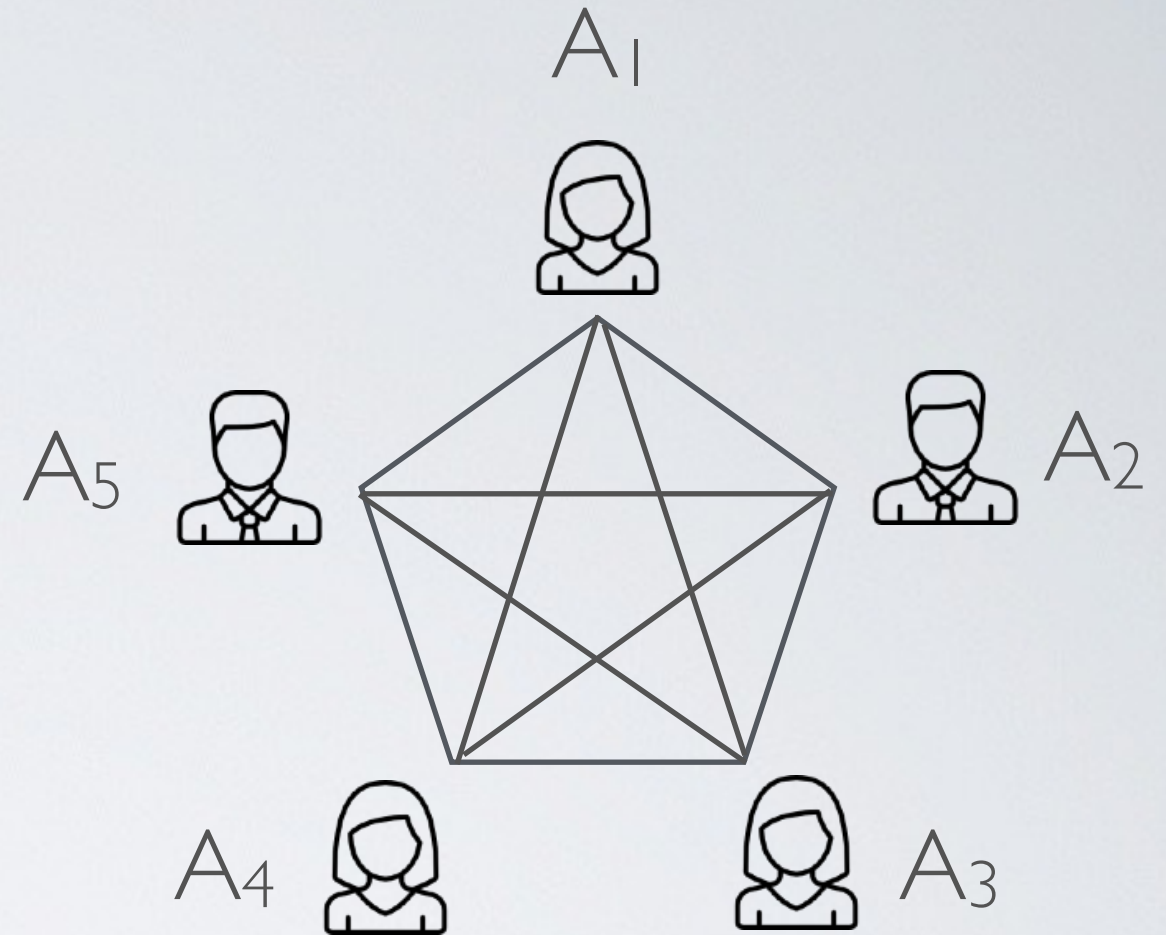


# The big challenge with symmetric cryptosystems?

How do we **agree**  
on the  ?



# Naive Key Management



$A_1, A_2 \dots A_5$  want to talk

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

⦿ Keys must be exchanged physically using a secure channel