

A symmetric protocol
for key exchange

The big challenge with symmetric cryptosystems?

How do we **agree**
on the  ?

