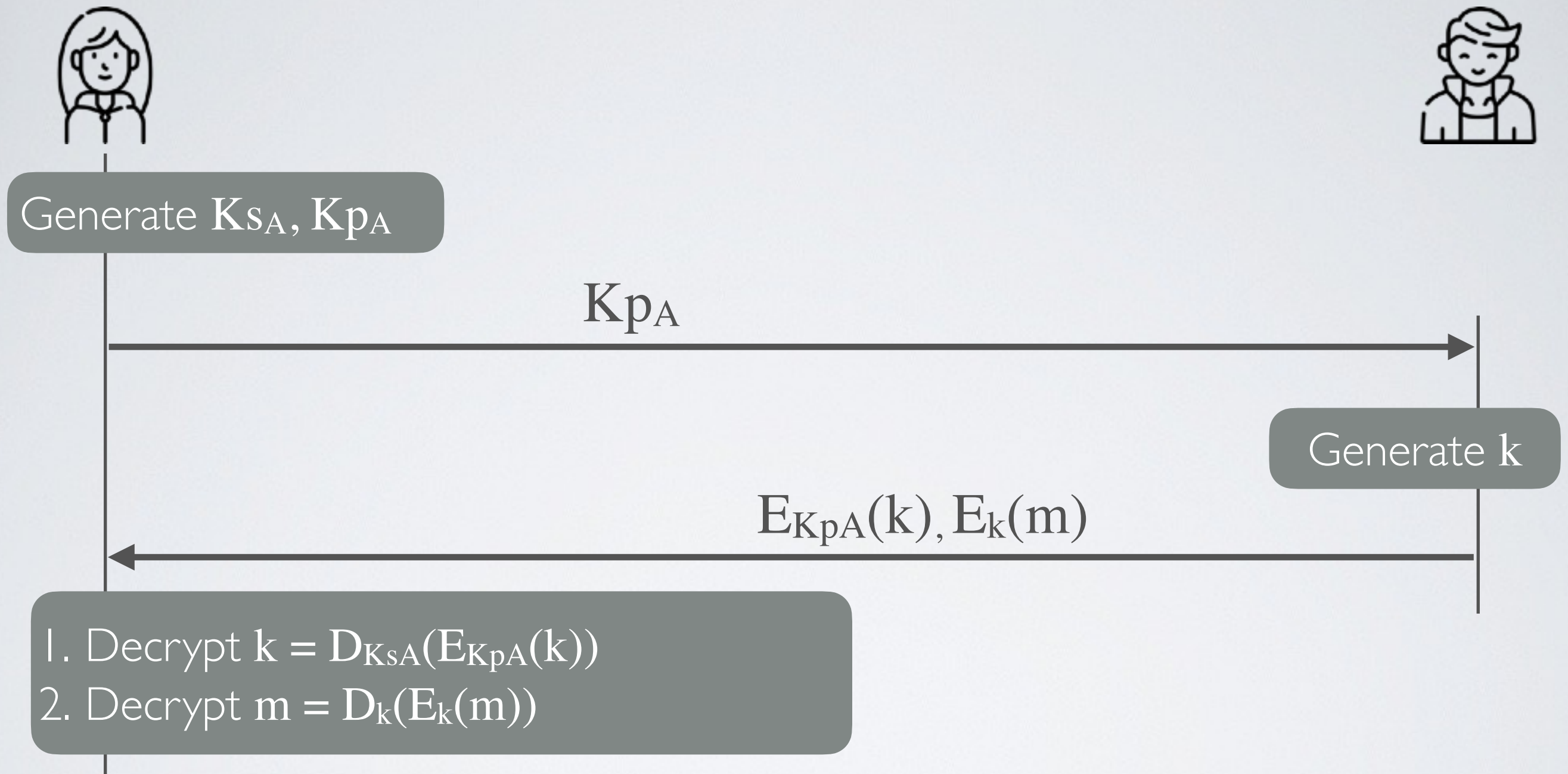


Naive key exchange using asymmetric encryption



- ◉ Protecting the shared key is the **responsibility of Alice only**
- ◉ Generating the shared key is the **responsibility of Bob only**

What is the solution?

Could Alice and Bob could magically come up with a key without exchanging it over the network?

➔ The magic is called **Diffie-Hellman-Merkle Protocol**