Naive key exchange using asymmetric encryption

Generate K_{sA}, K_{pA}

K_{pA}

Generate k

$E_{KpA}(k), E_k(m)$

1. Decrypt $k = D_{KsA}(E_{KpA}(k))$
2. Decrypt $m = D_k(E_k(m))$

- 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**