Limitations of using a key distribution centre

The key distribution server is a bootleneck and **weak link**

- The attacker could record the key exchange and the encrypted session, if one day either **Kas** or **Kbs** is broken, the attacker can decrypt the session

➡ Having a KDC does not offer "Perfect Forward Secrecy"

Can we avoid having a KDC ?

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**