An asymmetric protocol

for key exchange

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 ensure **Perfect Forward Secrecy**