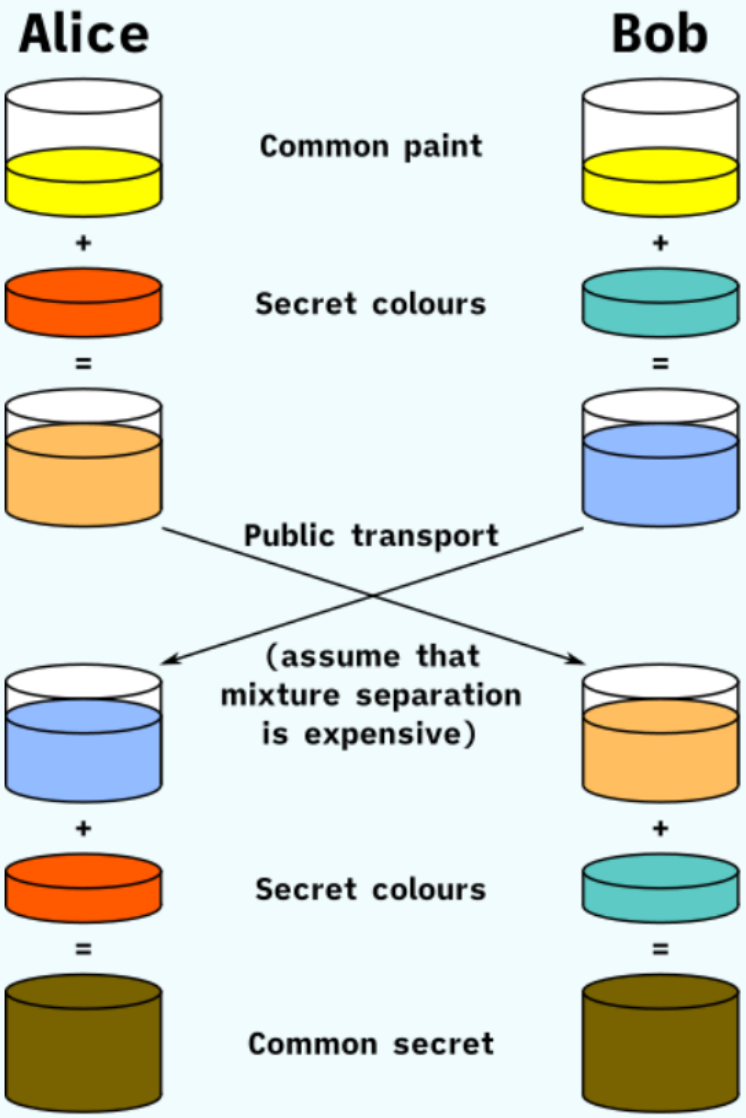
Key Exchange Algorithm

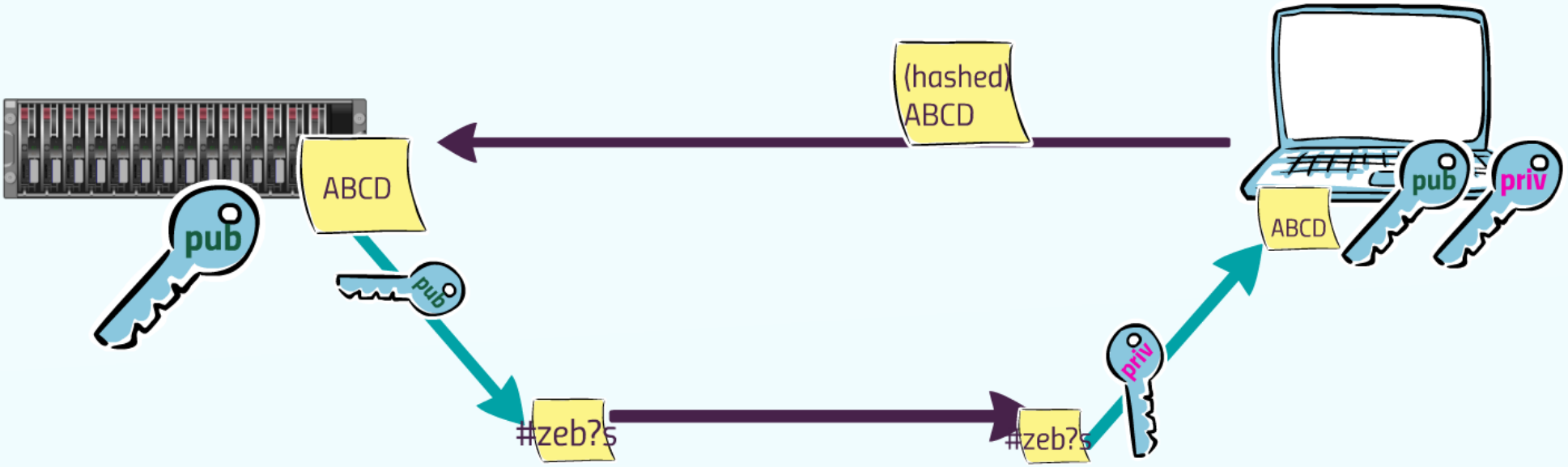


(Diffie-Hellman)

Source: wikipedia,
Original schema:
A.J. Han Vinck, University of Duisburg-Essen

Asymmetric cryptography public/private keys pair

User authentication



Server authentication: same principle, reverse sides