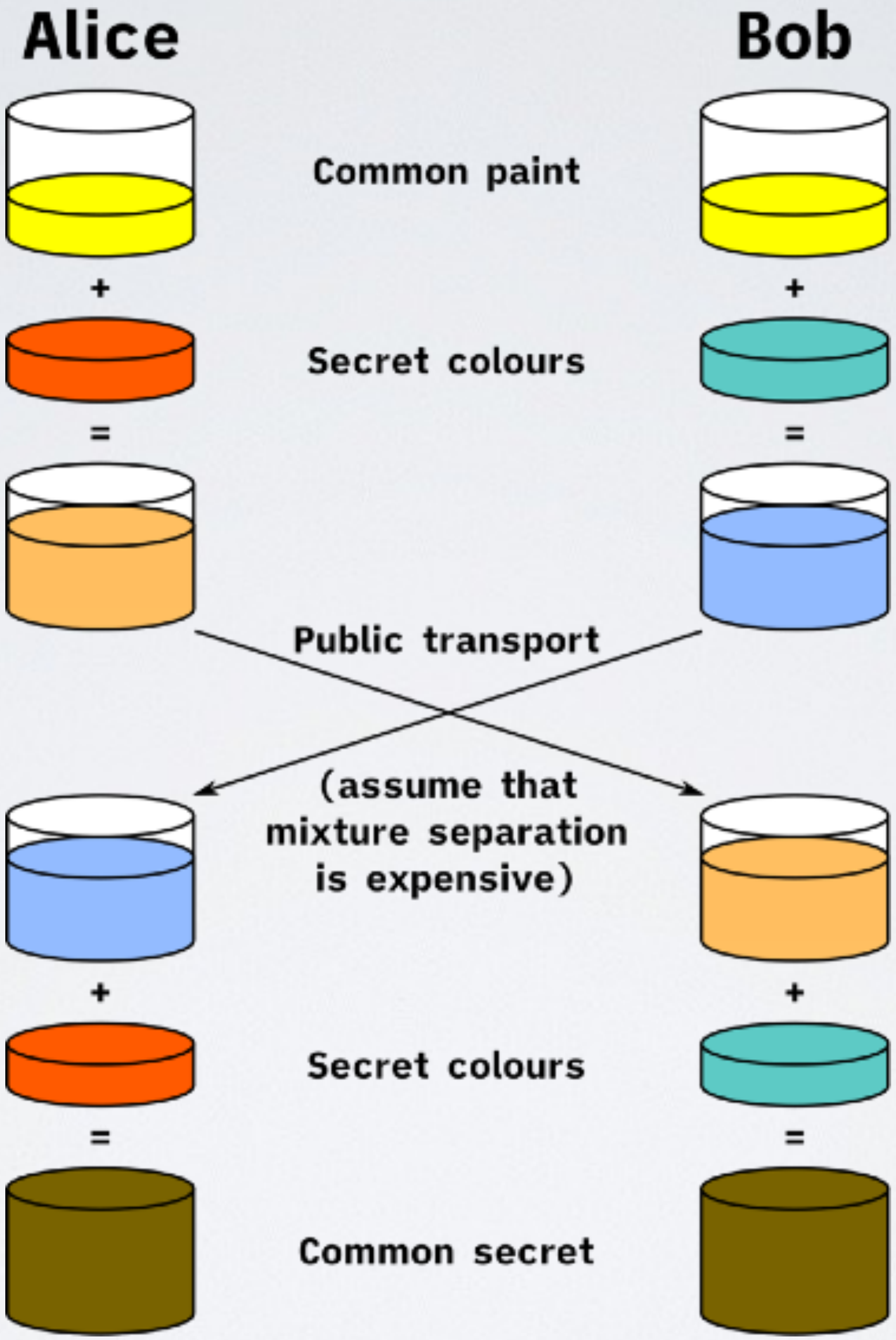
Can we avoid having a KDC ?

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**

The Diffie-Hellman-Merkel key exchange protocol


Alice
Bob
Common paint
+
+
Secret colours
=
=
Public transport
(assume that mixture separation is expensive)
+
+
Secret colours
=
=
Common secret