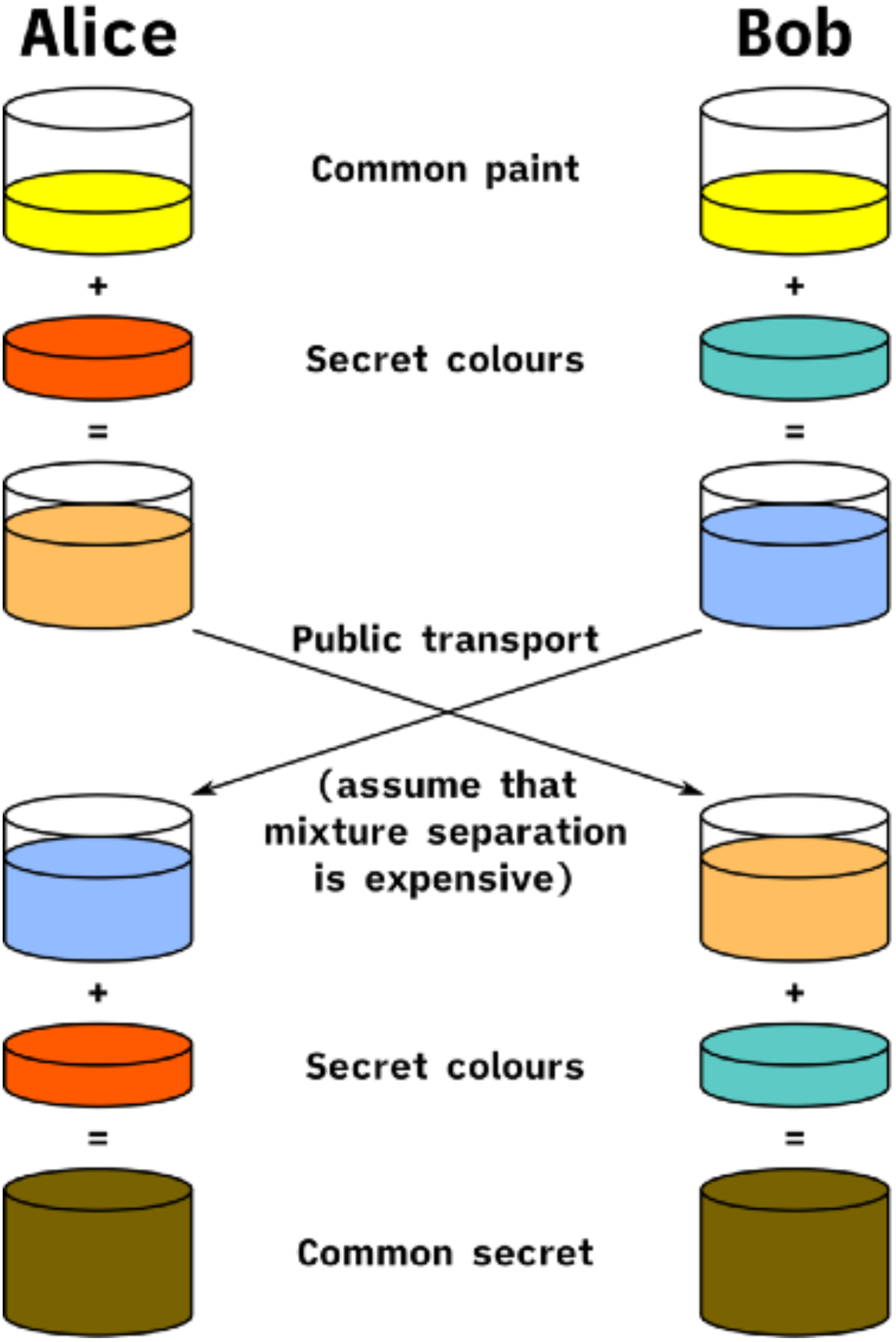
$$K = g^{ab} \bmod p = (g^{a} \bmod p)^{b} \bmod p = (g^{b} \bmod p)^{a} \bmod p$$


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

p,g

p,g

a

b

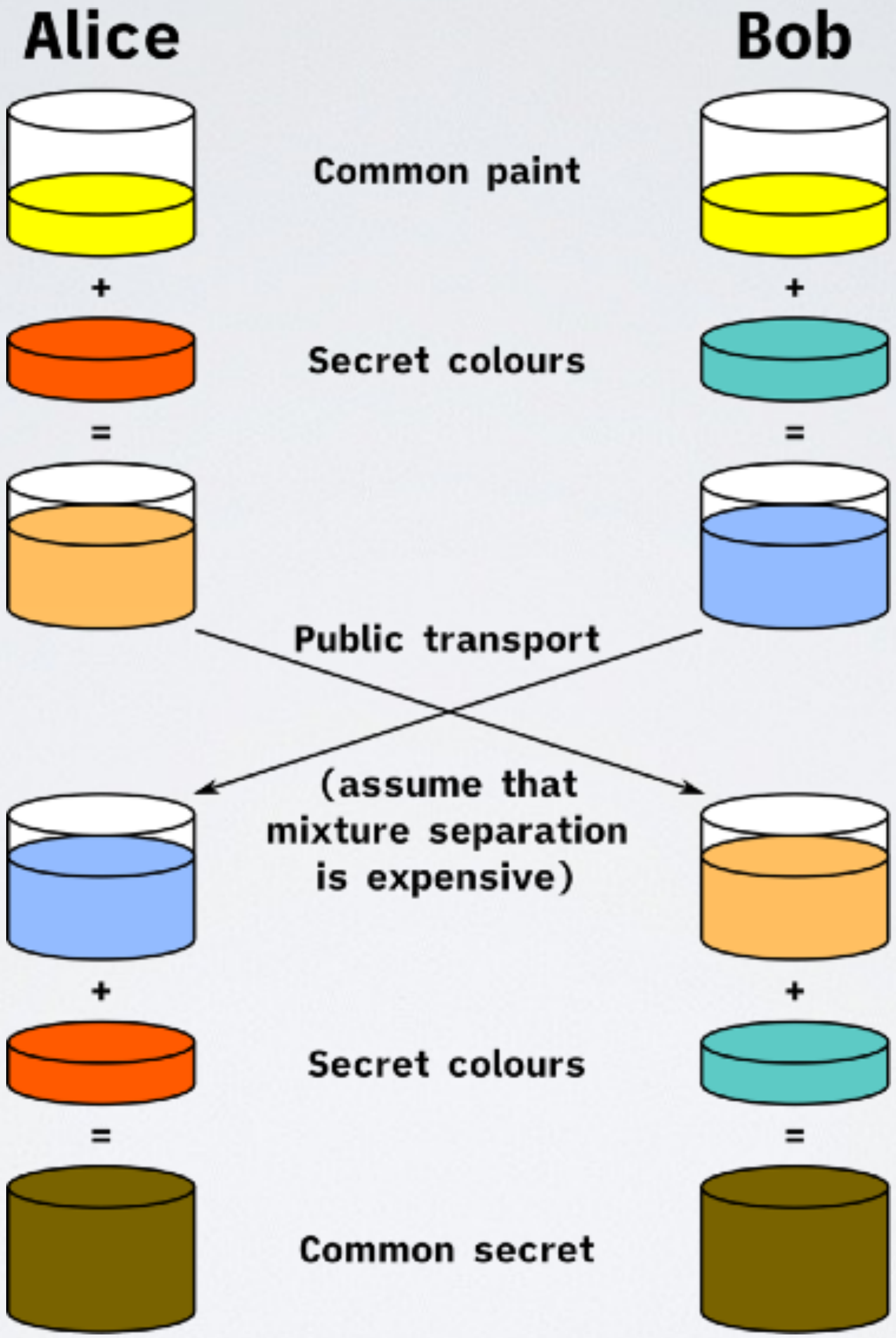
$A = g^a \bmod p$ $B = g^b \bmod p$

$K = B^a \bmod p$

$K = A^b \bmod p$

The Diffie-Hellman-Merkel key exchange protocol

The Diffie-Hellman-Merkel key exchange protocol



p,g

a

$A = g^a \bmod p$

$K = B^a \bmod p$

p,g

b

$B = g^b \bmod p$

$K = A^b \bmod p$

$$\boxed{K = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p}$$

The Diffie-Hellman-Merkel key exchange protocol