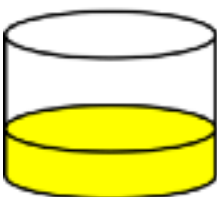


$$K = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$$

Alice



+



=

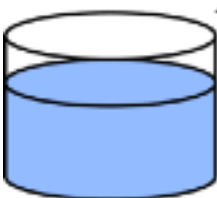


Common paint

Secret colours

Public transport

(assume that
mixture separation
is expensive)



+

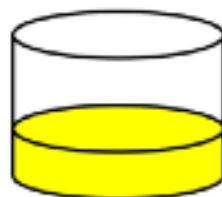


=



Common secret

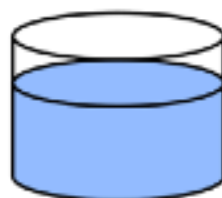
Bob



+



=



+



=



p, g

p, g

a

a

a

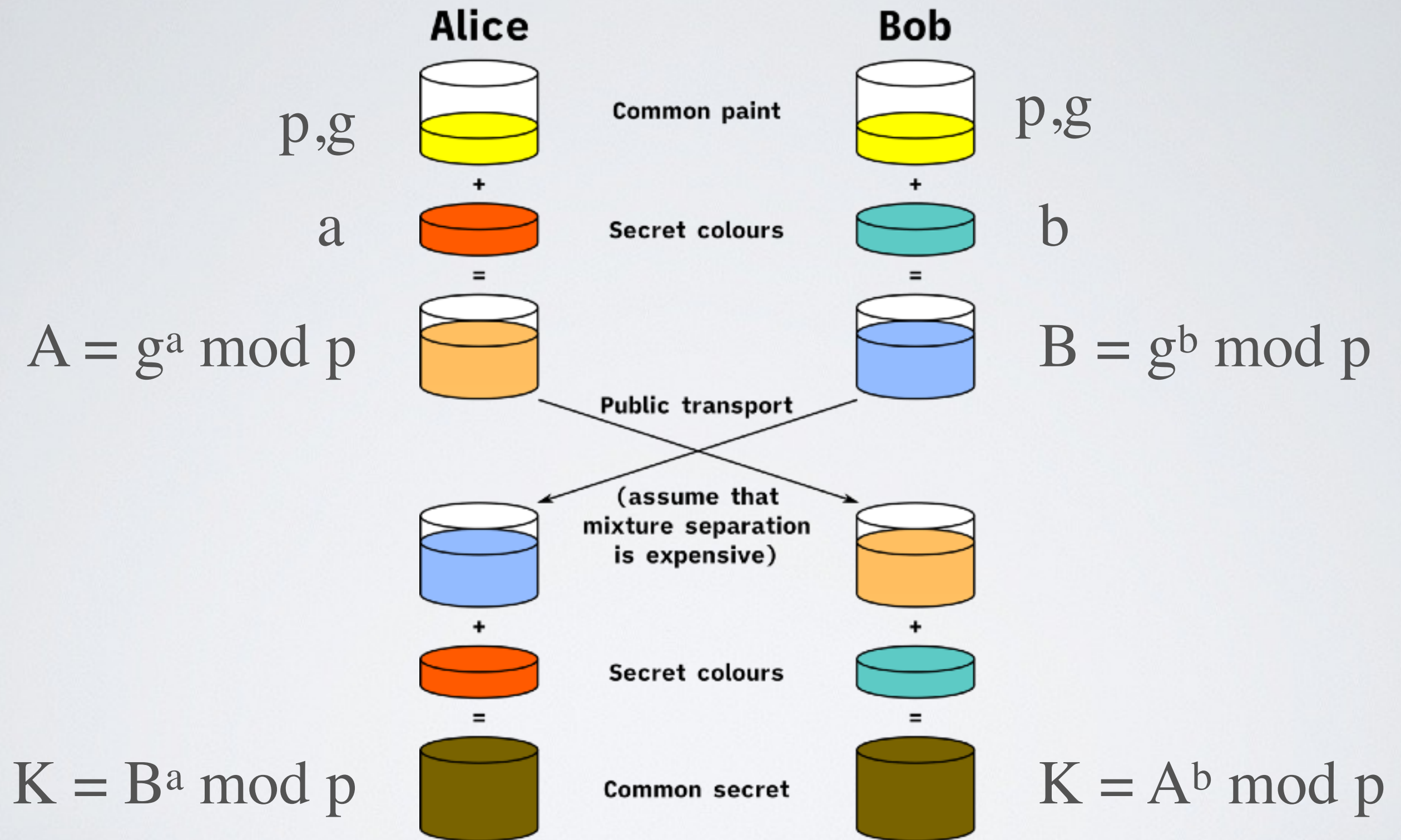
b

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

$$K = B^a \bmod p \qquad K = A^b \bmod p$$

The Diffie-Hellman-Merkle key exchange protocol

The Diffie-Hellman-Merkel key exchange protocol



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

The Diffie-Hellman-Merkel key exchange protocol

