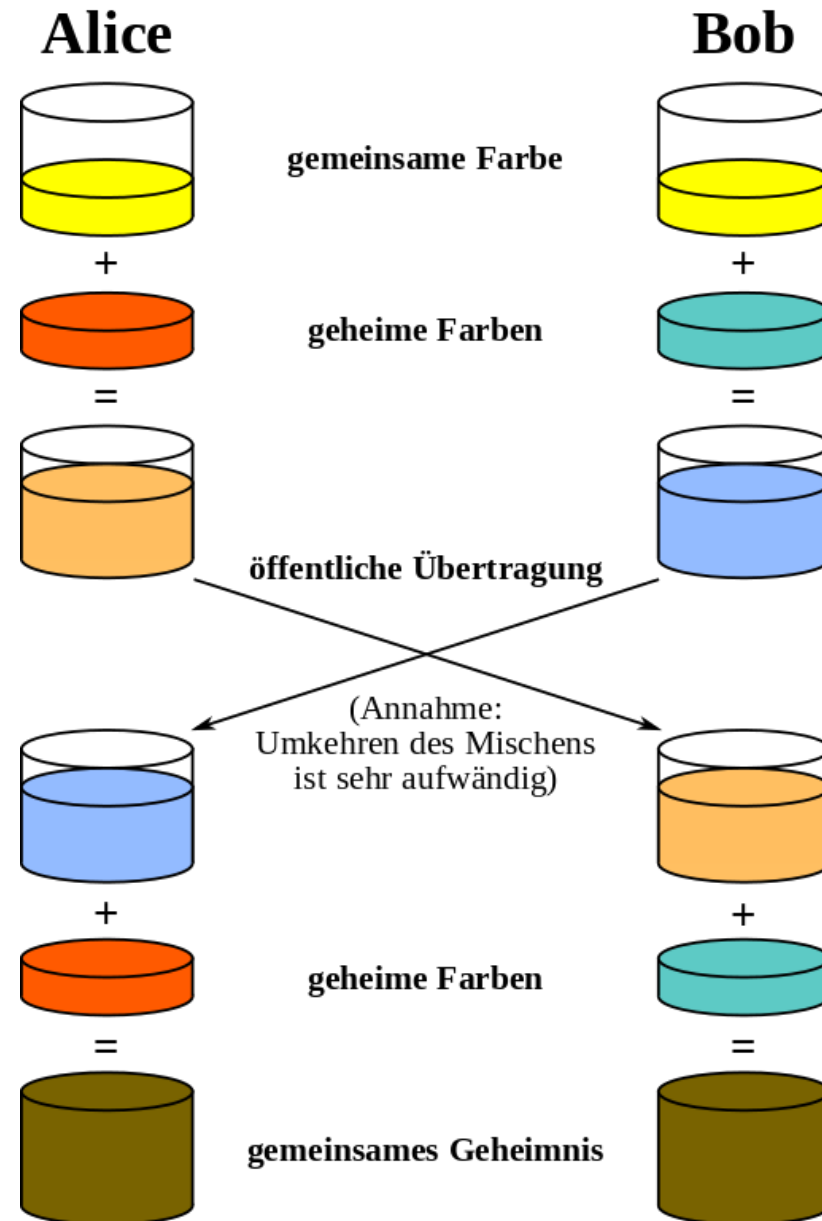
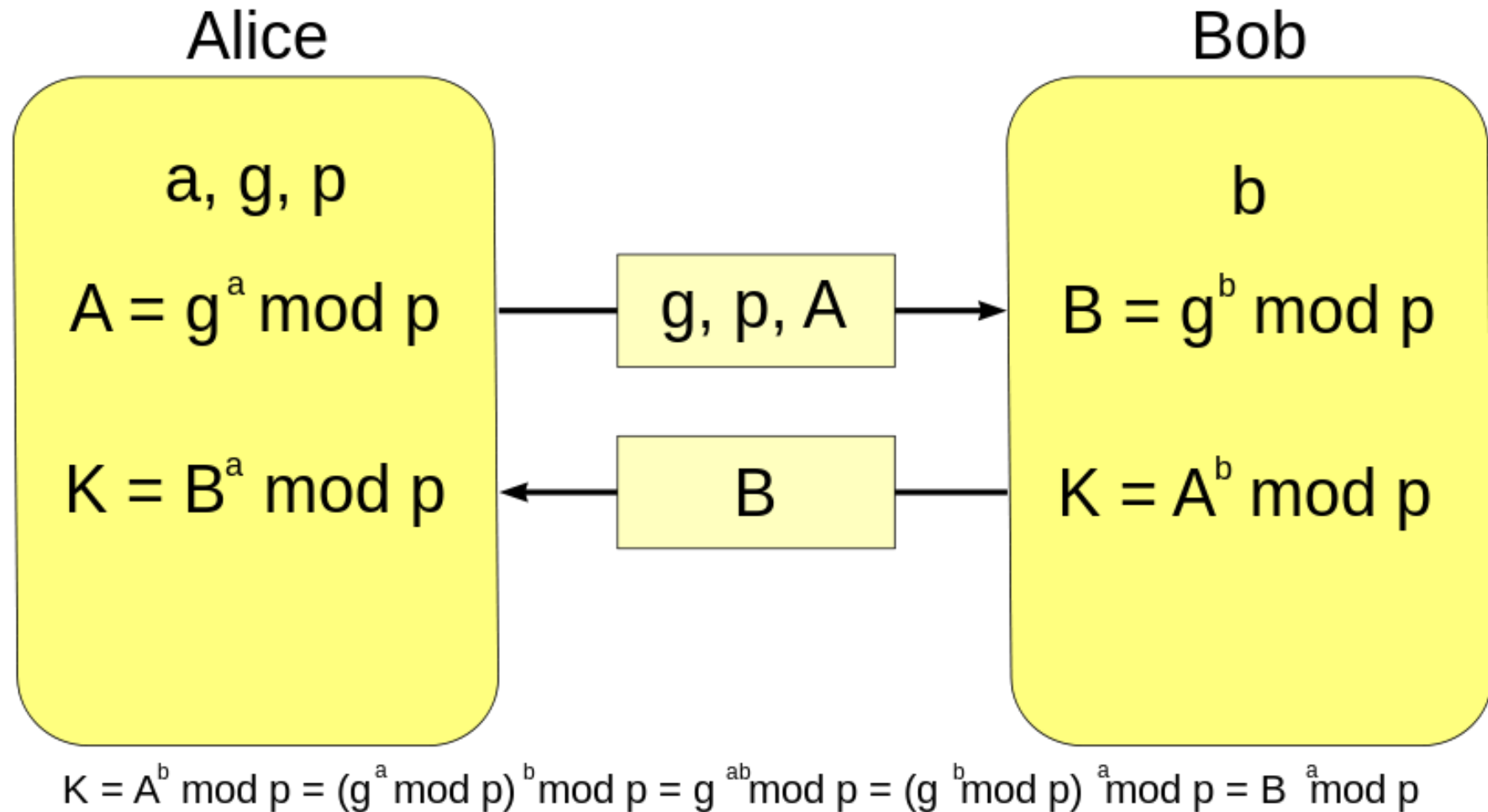


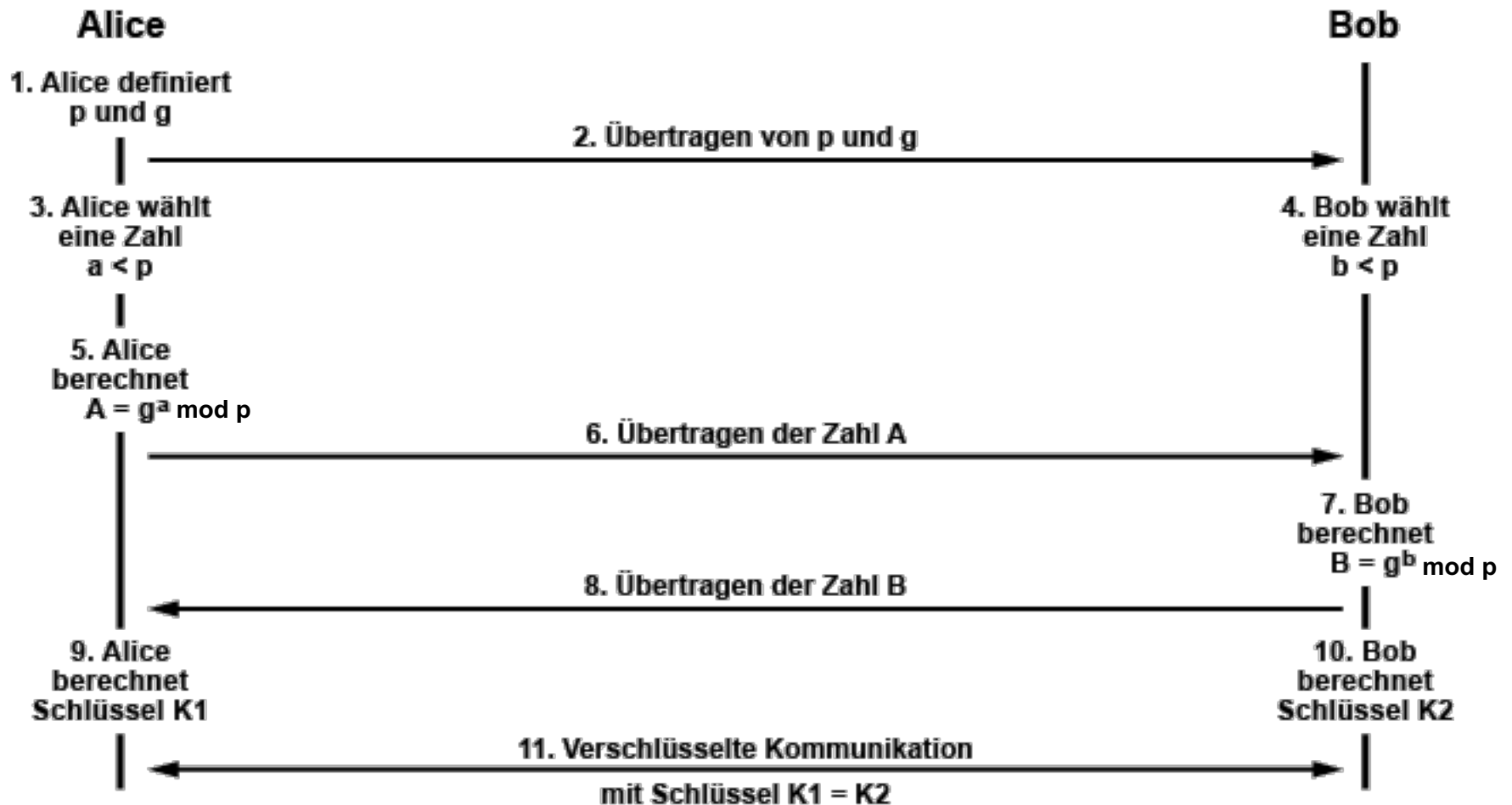
Diffie-Hellmann-Illustrationen (1)



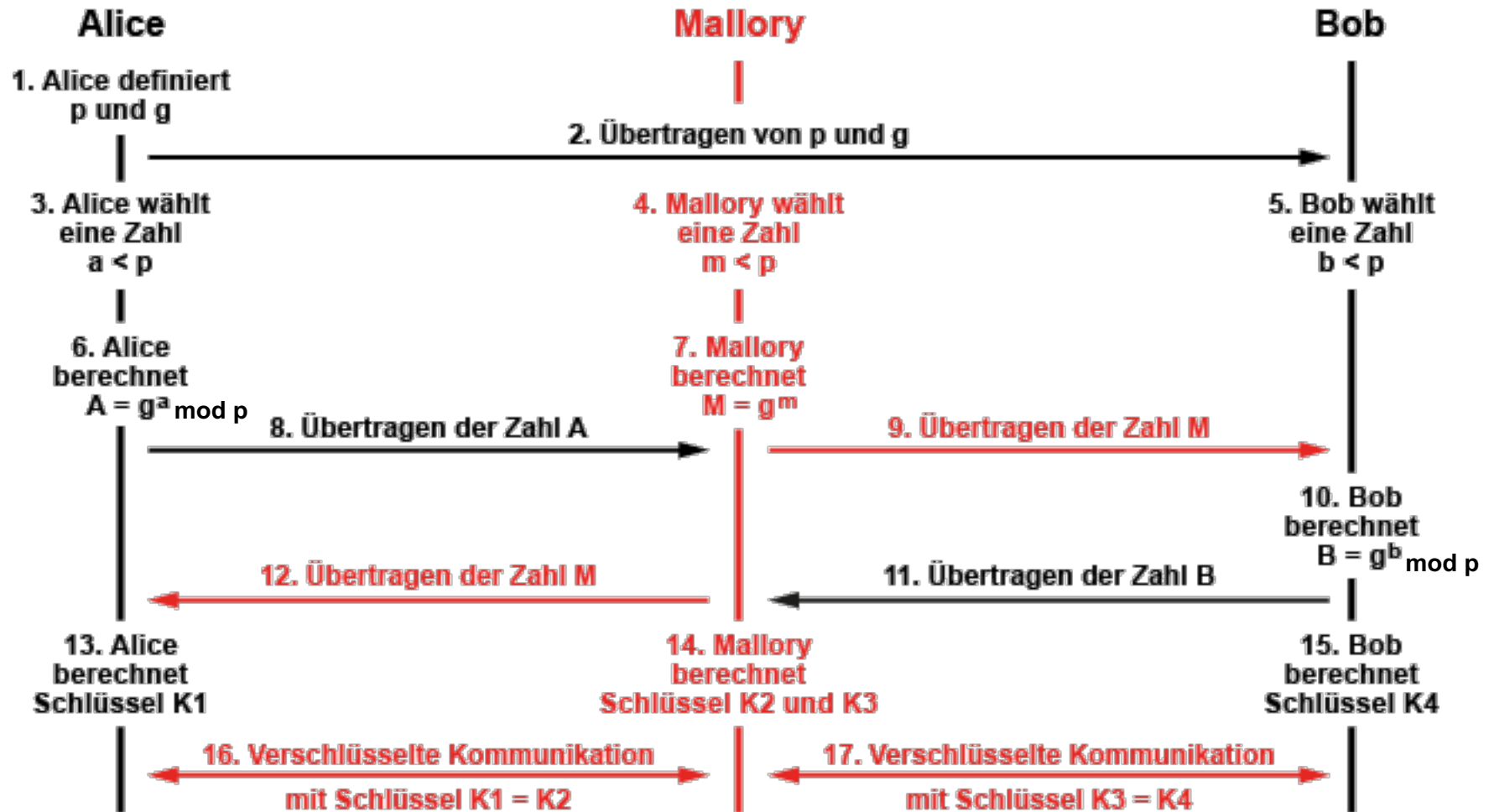
Diffie-Hellmann-Illustrationen (2)



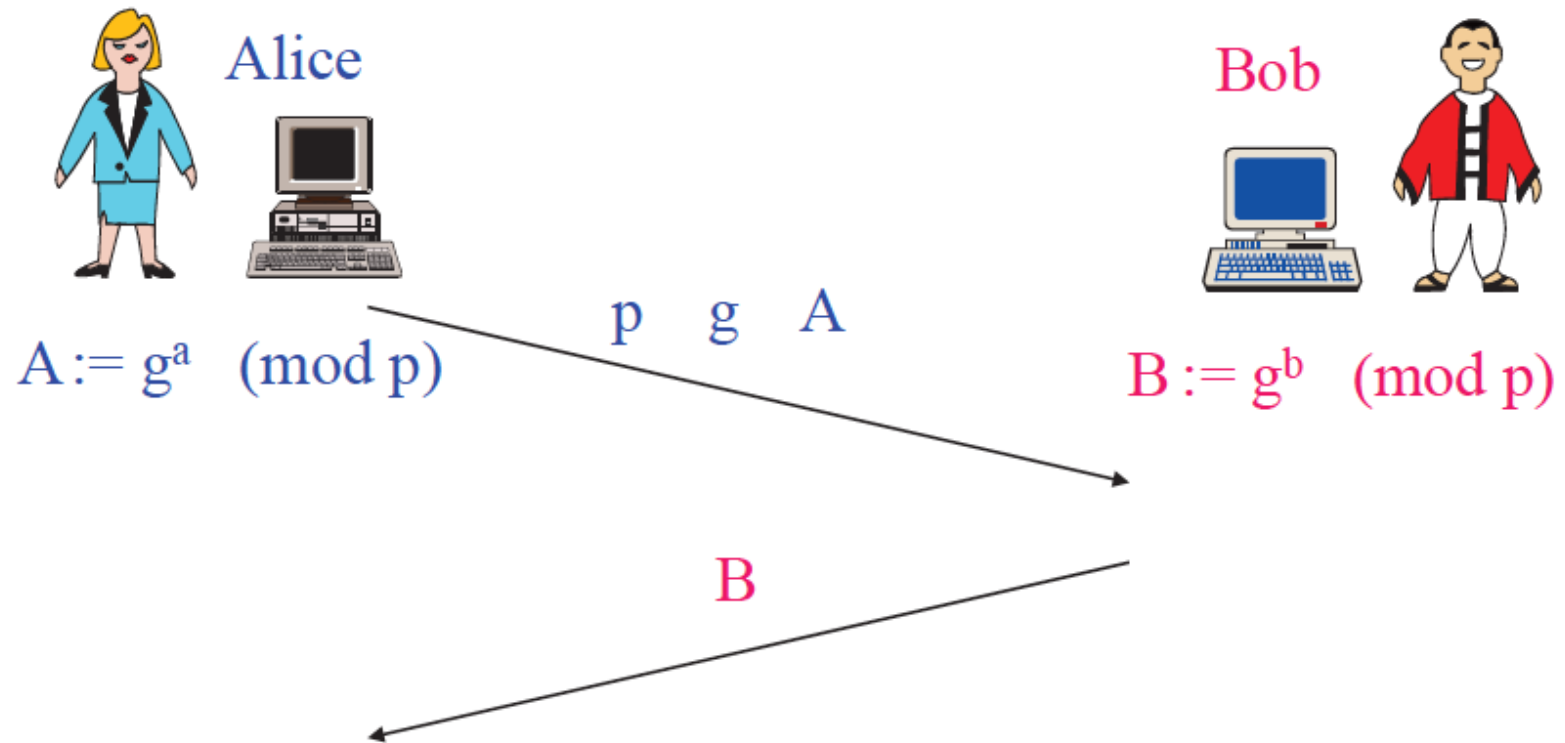
Diffie-Hellmann-Illustrationen (3a)



Diffie-Hellmann-Illustrationen (3b)



Diffie-Hellman Protokoll



$$\Rightarrow k_{AB} \equiv B^a \equiv A^b \equiv k_{BA} \pmod{p}$$