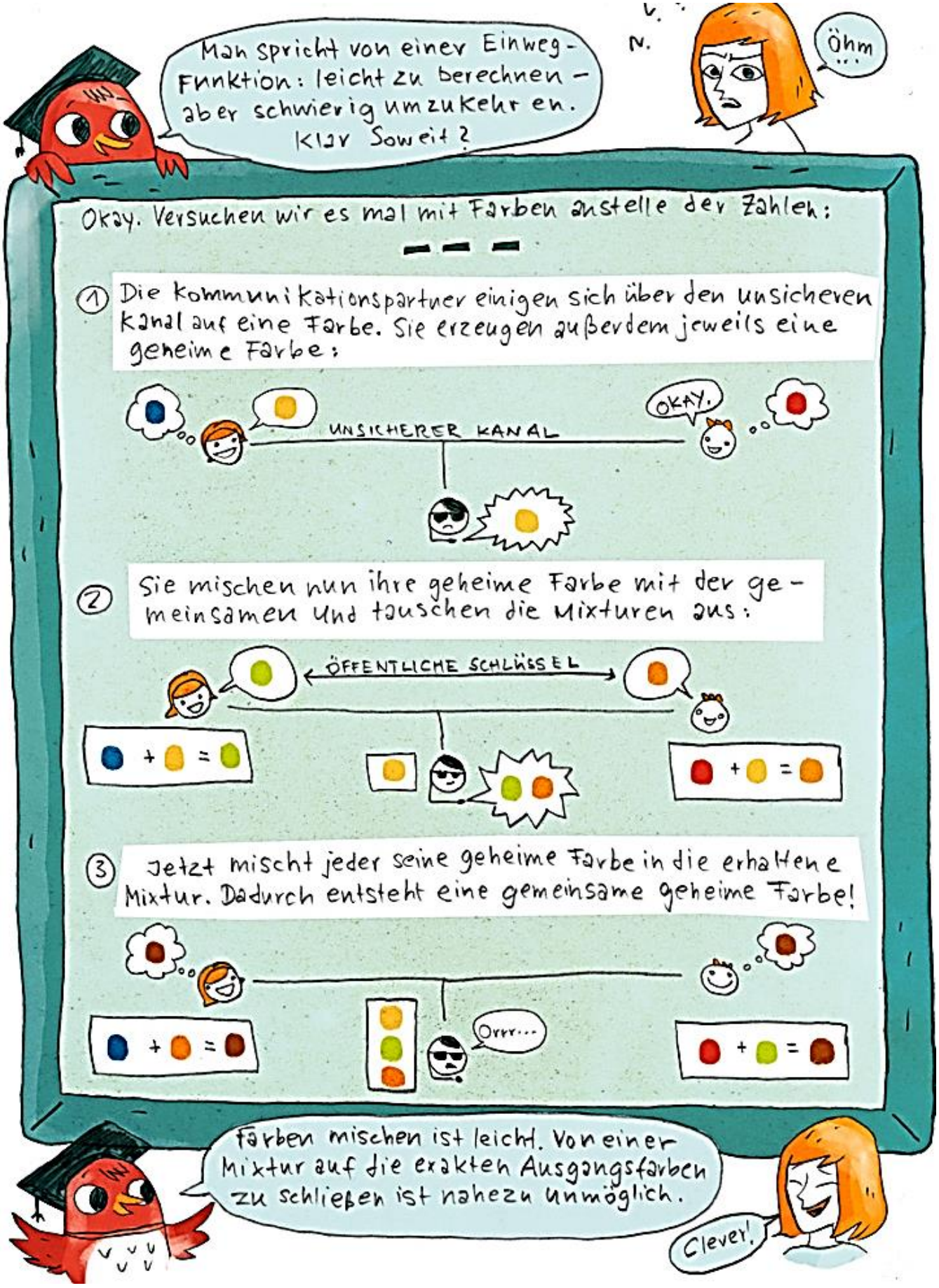
# Einwegfunktion




Quelle: Klar soweit? Helmholtz-Wissenschaftscomics

# Diffie -Hellmann Verfahren zum Schlüsseltausch

Lange galt es als unmöglich, im »öffentlichen Raum einen geheimen Schlüssel auszutauschen. Aber 1976 wurde von Martin Hellman, Whitfield Diffie und Ralph Merkle der **Diffie-Hellman-Algorithmus** entwickelt. Er ermöglicht die Vereinbarung eines gemeinsamen geheimen Schlüssels über eine unsichere Verbindung.

Alice und Bob vereinbaren zu Beginn öffentlich eine Primzahl **p** und eine natürliche Zahl **g** mit **g < p**. Alice wählt noch eine Zahl **a < p**, die nur sie kennt und berechnet **$A = g^a \bmod p$**.
Bob wählt die Zahl **b < p**, die nur er kennt und berechnet **$B = g^b \bmod p$.**
**A** und **B** werden öffentlich ausgetauscht.
Ein Angreifer kennt also **p**, **g**, **A** und **B**, aber nicht **a** und **b.**
Den geheimen Schlüssel **$K=A^b \bmod p=B^a$ mode p** können nur Alice und Bob berechnen.


Quelle: Klar soweit? Helmholtz-Wissenschaftscomics

Alice und Bob vereinbaren öffentlich: $p = 13$ und $g = 4$:

| privater Raum: | öffentlicher Raum: | privater Raum: |
|---|---|---|
|  Alice |  Eve | Bob  |
| | $p = 13,\ g = 4$ | |
| Wähle a, mit a < p | | Wähle b, mit b < p |
| $a = 3$ | | $b = 5$ |
| Berechne $A = g^a \mod p$ | | Berechne $B = g^b \mod p$ |
| $A = g^a \mod p$<br>$A = 4^3 \mod 13$<br>$= 64 \mod 13$<br>$= 12$ | | $B = g^b \mod p$<br>$B = 4^5 \mod 13$<br>$= 1024 \mod 13$<br>$= 10$ |
| | $A = 12 \rightarrow$ | |
| | $\leftarrow B = 10$ | |
| Berechne $K = B^a \mod p$ | | Berechne $K = A^b \mod p$ |
| $K = 10^3 \mod 13$<br>$= 1000 \mod 13$<br>$= 12$ | | $K = 12^5 \mod 13$<br>$= 248832 \mod 13$<br>$= 12$ |

Quelle: Klar soweit? Helmholtz-Wissenschaftscomics