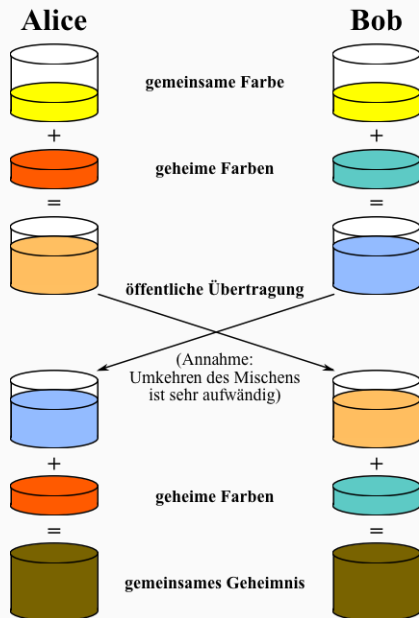


- Wir haben zahlreiche mehr oder minder gute Verschlüsselungsverfahren kennen gelernt
 - Einige sind auch heute nicht oder nur mit viel Aufwand zu “knacken”
- Welches Problem ist allen gemeinsam?
 - Beide Partner müssen sich auf eine Schlüssel einigen
 - Der Schlüssel kann nicht über den gleichen Kanal übertragen werden wie die späteren Nachrichten

Schlüsseltausch nach Diffie-Hellman



- Alice und Bob sind am Ende beide im Besitz der geheimen Farbe
- Ein Angreifer, der Orange oder Blau beim Transport abfängt, kann die geheime Farbe dennoch nicht erschließen
 - Es fehlt ihm das Wissen über die verwendeten geheimen Farben (diese wurden nie direkt ausgetauscht)
- Lässt sich ein Algorithmus finden, der ähnliches leistet?

Schlüsseltausch nach Diffie-Hellman

1. Alice und Bob einigen sich auf eine Primzahl p und eine Zahl g mit $2 \leq g \leq p - 2$
 - Diese Zahlen müssen nicht geheim gehalten werden
2. Alice und Bob erzeugen je eine geheime Zahl a bzw. b zwischen 1 und $p - 2$
3. Alice berechnet $A = g^a \bmod p$, Bob berechnet $B = g^b \bmod p$
4. A und B werden übertragen
5. Alice berechnet $K_1 = B^a \bmod p$, Bob berechnet $K_2 = A^b \bmod p$

Es gilt dann: $K_1 = K_2 = g^{ab} \bmod p$. Alice und Bob verfügen also über den gleichen Schlüssel.

Beispiel

- Alice und Bob einigen sich auf $p = 17$ und $g = 3$
- Alice wählt $a = 6$, Bob wählt $b = 12$
- Alice berechnet
$$A = g^a \bmod p = 3^6 \bmod 17 = 729 \bmod 17 = 15 \text{ (denn } 729 : 17 = 42 \text{ Rest } 15)$$
- Bob berechnet
$$B = g^b \bmod p = 3^{12} \bmod 17 = 531\,441 \bmod 17 = 4 \text{ (denn } 531441 : 17 = 31\,261 \text{ Rest } 4)$$
- Alice und Bob tauschen A und B aus
- Alice berechnet $B^a \bmod p = 4^6 \bmod 17 = 4\,096 \bmod 17 = 16$
- Bob berechnet $A^b \bmod p = 15^{12} \bmod 17 = 129\,746\,337\,890\,625 \bmod 17 = 16$

- Ein Angreifer kann zwar möglicherweise A , B , p und g “erbeuten”, aber damit **nicht** a , b oder g^{ab} berechnen
- Die Sicherheit des Verfahrens beruht darauf, dass das Potenzieren modulo p einfach zu berechnen ist, die Umkehrung (diskreter Logarithmus) jedoch nicht
 - Man spricht hier auch von einer Einwegfunktion
- In der Praxis werden deutlich größere Zahlen verwendet als im Beispiel

- Führt den Schlüsseltausch nach Diffie-Hellman in Partnerarbeit durch