Kryptographie & Privatsphäre

Bauhaus Digitalwerkstatt

News Alert

Restklassen

- Ergebnis ist der Rest von der ganzzahligen Division
- Die Menge der natürlichen Zahlen, die bei der ganzzahligen Division entstehen, nennt man Restklassen dieser Zahl
-
- Rechenoperation Modulo %
- Beispiel: 5 % 3 = 2 oder -2 % 3 = 1

Knobelei

"Ich bin eine Zahl zwischen 0 und 9. Wenn man mich durch 2 teilt, bleibt kein Rest übrig. Wenn man mich jedoch durch 3 teilt, bleibt ein Rest von 1 übrig. Welche Zahl bin ich?"

Restklassenringe

- wenn 2 Zahlen aus einer Restklasse addiert oder multipliziert werden, dann ist das Ergebnis von Modulo wieder eine Zahl dieser Restklasse
- Beispiel: Uhr mit Restklasse 12
- 9+5 = 14 = 2

Hausaufgabe

Aufgabe 1 & 2

Aufgabe 3

Asymmetrische Verschlüsselung

- öffentlichen Schlüssel (kennen alle Parteien)
- geheimen Schlüssel (jede Partei hat ihren eigene Schlüssel)
- Einwegfunktion

Einwegfunktion

- eine Funktion die einfach zu berechnen ist, ihre Umkehrung jedoch nicht möglich oder nicht effektiv möglich ist
- Beispiel: Falltür, Telefonbuch
- Beispiel: Multiplikation von Primzahlen <-> Zerlegung in Primzahlfaktoren

Knobelei

Alice und Bob sind beide Maler und möchten jetzt zum Spaß zwischen sich eine geheime Farbe ausmachen, die keiner sonst kennt. Um miteinander zu kommunizieren können sie ein Paket mit einer Farbtube schicken. Das Paket kann ja aber von jedem auf dem Weg geöffnet werden, wie machen sie jetzt eine geheime Farbe aus?

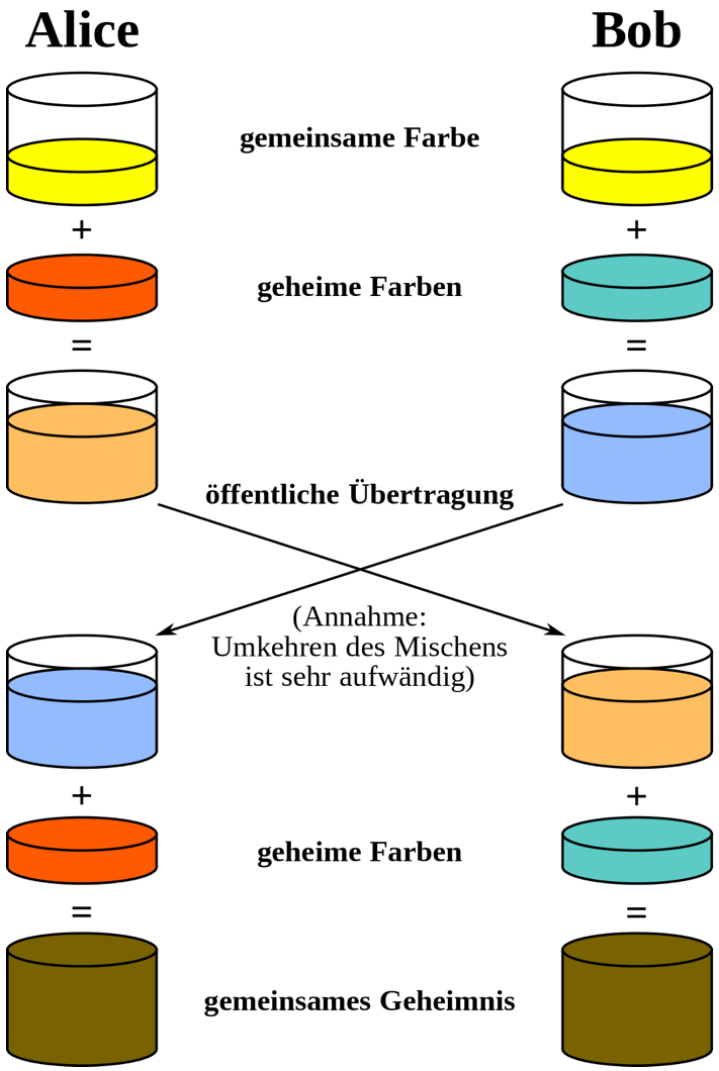
Tips:

- *was ist der geheime und öffentliche Schlüssel?*
- *was kann man als Einwegfunktion annehmen?*

Tips:

- *was ist der geheime und öffentliche Schlüssel?*
- *was kann man als Einwegfunktion annehmen?*
- *Einwegfunktion: das Mischen von Farben*

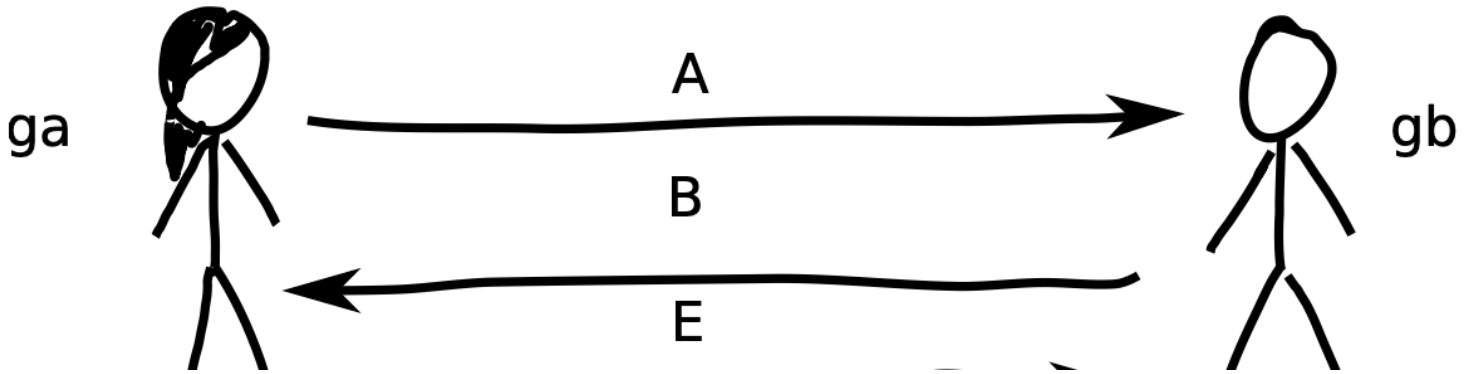
Lösung:


Alice
Bob
gemeinsame Farbe
+
+
geheime Farben
=
=
öffentliche Übertragung
(Annahme:
Umkehren des Mischens
ist sehr aufwändig)
+
+
geheime Farben
=
=
gemeinsames Geheimnis

Diffe-Hellman-Schlüsselaustausch

- öffentlichen Schlüssel: große Primzahl p und kleine natürliche Zahl g
- Einwegfunktion: diskrete Logarithmus: $b^x \mod p$

Alice:	secret $\mathbf{a}$; public $\mathbf{A} = g^{\mathbf{a}} \bmod p$
Bob:	secret $\mathbf{b}$; public $\mathbf{B} = g^{\mathbf{b}} \bmod p$
joint session key:	$\mathbf{K} = g^{\mathbf{ab}} = \mathbf{B}^{\mathbf{a}} = \mathbf{A}^{\mathbf{b}} \bmod p$



Ende