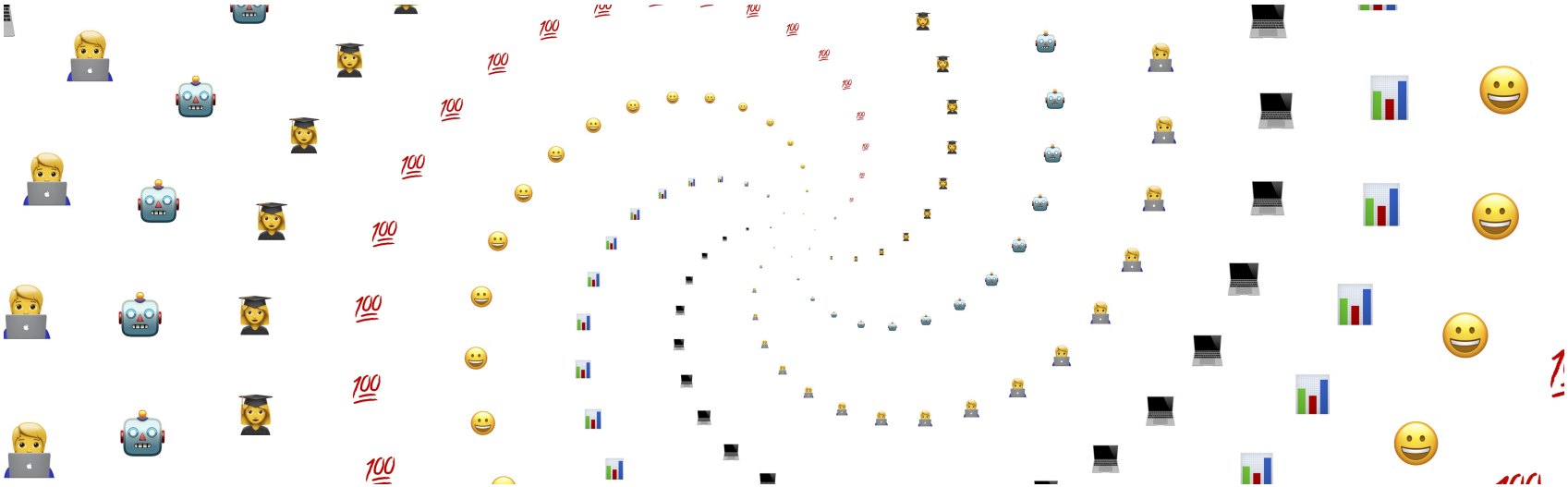
Schlüsselaustausch

Klassen

Judith Beestermöller

Lehrdiplom Informatik
ETH Zürich



Kantonsschule Im Lee

Schlüsselaustauschproblem

- Wenn der Schlüssel kürzer ist als der Klartext, kann man den Schlüssel mittels Häufigkeitsanalyse herausfinden.

Schlüsselaustauschproblem

- Wenn der Schlüssel kürzer ist als der Klartext, kann man den Schlüssel mittels Häufigkeitsanalyse herausfinden.
- Was ist, wenn der Schlüssel dieselbe Länge hat als der Klartext?

Schlüsselaustauschproblem

- Wenn der Schlüssel kürzer ist als der Klartext, kann man den Schlüssel mittels Häufigkeitsanalyse herausfinden.
- Was ist, wenn der Schlüssel dieselbe Länge hat als der Klartext?
- Wenn der Schlüssel nur ein einzigesmal verwendet wird, dann kann man den Klartext nicht herausfinden.

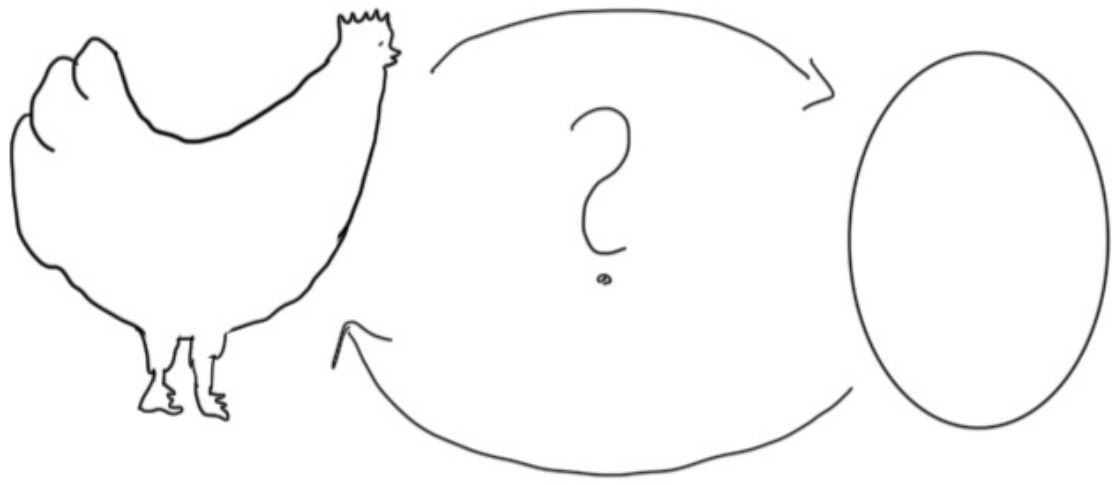
Schlüsselaustauschproblem

- Wenn der Schlüssel kürzer ist als der Klartext, kann man den Schlüssel mittels Häufigkeitsanalyse herausfinden.
- Was ist, wenn der Schlüssel dieselbe Länge hat als der Klartext?
- Wenn der Schlüssel nur ein einzigesmal verwendet wird, dann kann man den Klartext nicht herausfinden.
- Problem?

Schlüsselaustauschproblem

Definition (Schlüsselaustauschproblem)

Das Schlüsselaustauschproblem beschreibt die zentrale Herausforderung in der symmetrischen Kryptographie, einen gemeinsamen geheimen Schlüssel sicher zwischen zwei oder mehr Kommunikationspartnern auszutauschen, die über einen ansonsten unsicheren Kanal kommunizieren.



Schlüsselaustausch

- Ziel: Erstellung eines geheimen Schlüssels auf einem komplett öffentlichen Kanal

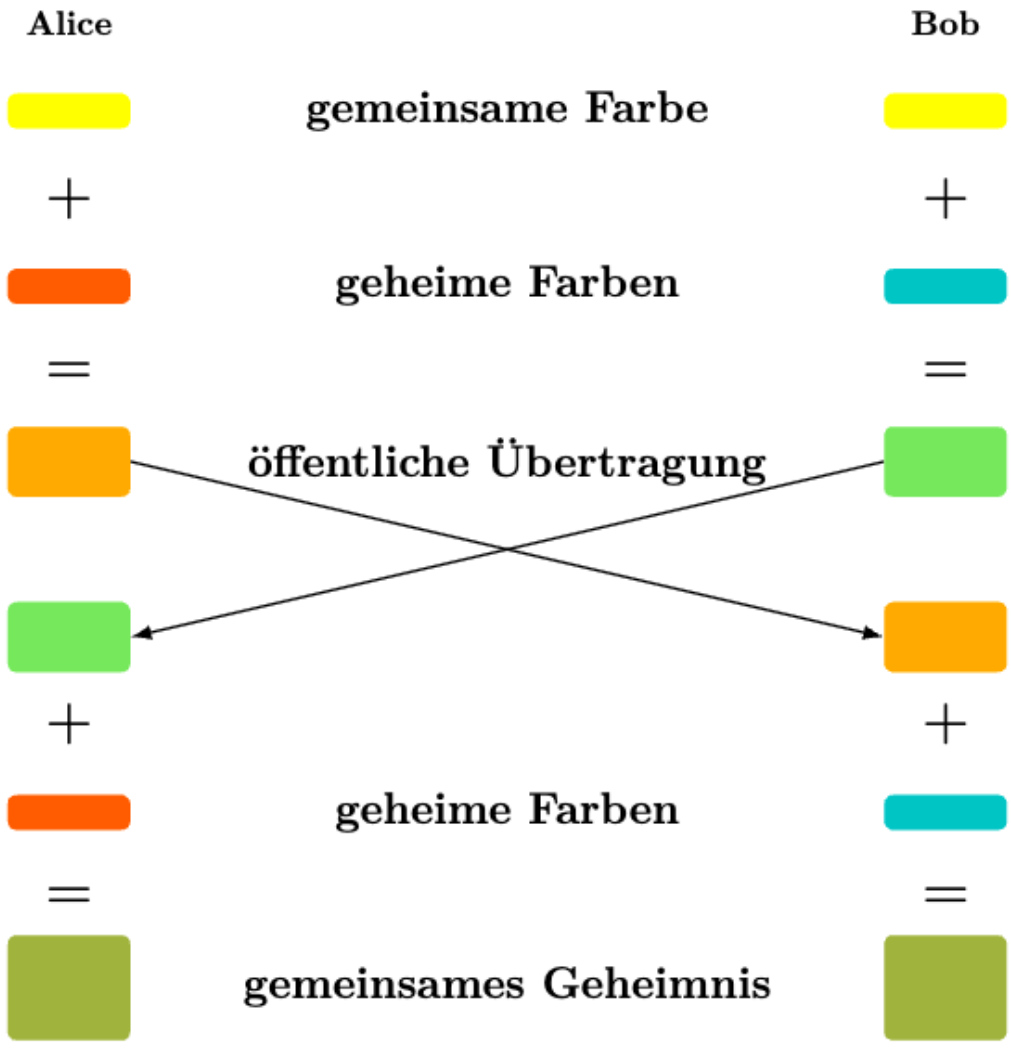
Schlüsselaustausch

- Ziel: Erstellung eines geheimen Schlüssels auf einem komplett öffentlichen Kanal
- Beim Bin-One-Time-Pad haben Sie bereits einen Naiven Schlüsselaustausch gesehen

Schlüsselaustausch

- Ziel: Erstellung eines geheimen Schlüssels auf einem komplett öffentlichen Kanal
- Beim Bin-One-Time-Pad haben Sie bereits einen Naiven Schlüsselaustausch gesehen
- Problem: Eve konnte anhand der übersendeten Nachrichten ebenfalls den Schlüssel einfach herausfinden

Schlüsselaustausch



Schlüsselaustausch

Aufgabe 0.1

Mischen Sie zwei Farben und versuchen Sie die Ursprungsfarben wiederherzustellen. Schaffen Sie es, wenn Sie die Farben am Computer mischen und Sie die RGB-Werte der Farben kennen?

Schlüsselaustausch

Aufgabe 0.2

- Welche Eigenschaft der Farbmischung nutzen Alice und Bob, damit beide am Ende die gleiche geheime Farbe erhalten?
- Wie würden wir diese Eigenschaft in der Mathematik nennen?
- Welche mathematischen Operationen kennen Sie, die diese Eigenschaften haben?

Diffie-Hellman-Merkel

Vorgehen (DIFFIE-HELLMAN-MERKLE (DHM))

Ausgangssituation: Alice und Bob haben sich zuvor öffentlich auf eine grosse Primzahl p und eine positive natürliche Zahl g geeinigt. Dabei ist g kleiner als p.

1. Alice wählt zufällig eine positive ganze Zahl a mit $a < p$ und hält diese geheim. Dann berechnet sie mit dieser geheimen Zahl: $x := g^a \mod p$ und sendet x an Bob.
2. Bob wählt zufällig eine positive ganze Zahl b mit $b < p$ und hält diese geheim. Dann berechnet er die Zahl $y := g^b \mod p$ und sendet y an Alice.
3. Alice erhält y von Bob und berechnet mit ihrer geheimen Zahl a die Zahl $s_{AB} := y^a \mod p$.
4. Bob berechnet mit dem erhaltenen x und seiner geheimen Zahl b die Zahl $s_{BA} := x^b \mod p$.

Diffie-Hellman-Merkel

Aufgabe 0.3

Führen Sie das DHM Verfahren selber mit Ihrer/Ihrem Sitznachbarn/in aus. Verwenden Sie

$$p := 19 \quad \text{und} \quad g := 8$$

(Sie können auch eigene Werte wählen) als öffentlich bekannte Schlüssel.

Diffie-Hellman-Merkel

Aufgabe 0.4

Versuchen Sie das Kommunikationsprotokoll DHM zu knacken, indem Sie für die gegebenen Werte p, g, x und y jeweils die geheimen Zahlen a und b berechnen und daraus dann den vereinbarten Schlüssel s_{AB}.

- $g = 4, p = 13, x = 12, y = 3$
- $g = 5, p = 7, x = 6, y = 2$