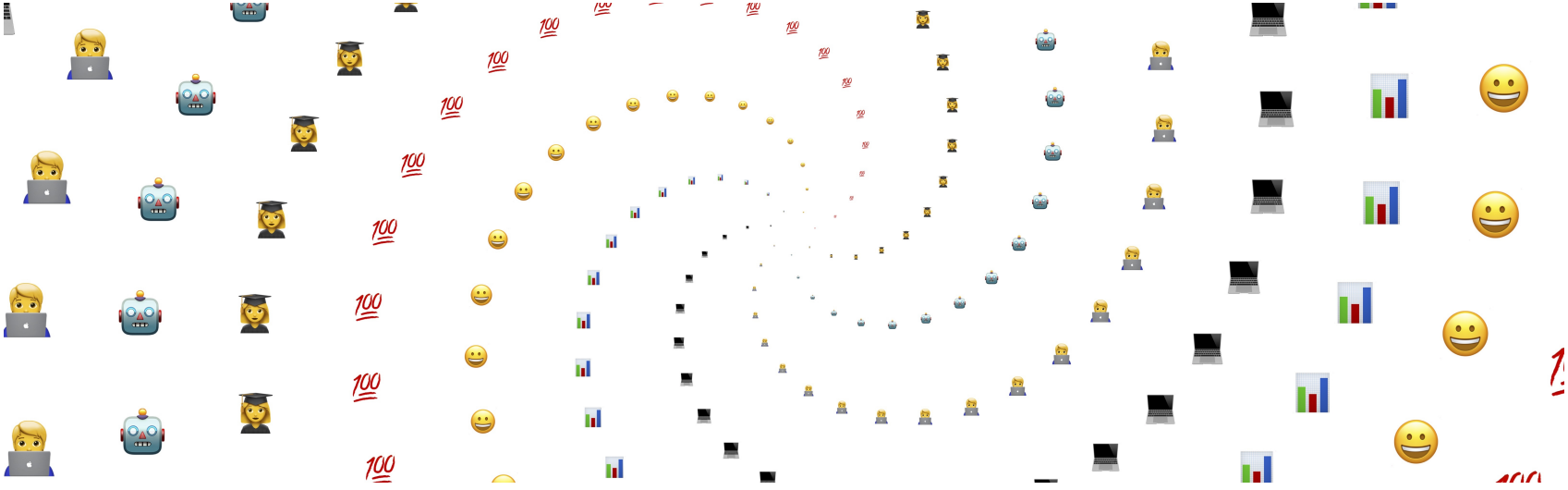
Schlüsselaustausch

Judith Beestermöller

Lehrdiplom Informatik
ETH Zürich



Kantonsschule Im Lee

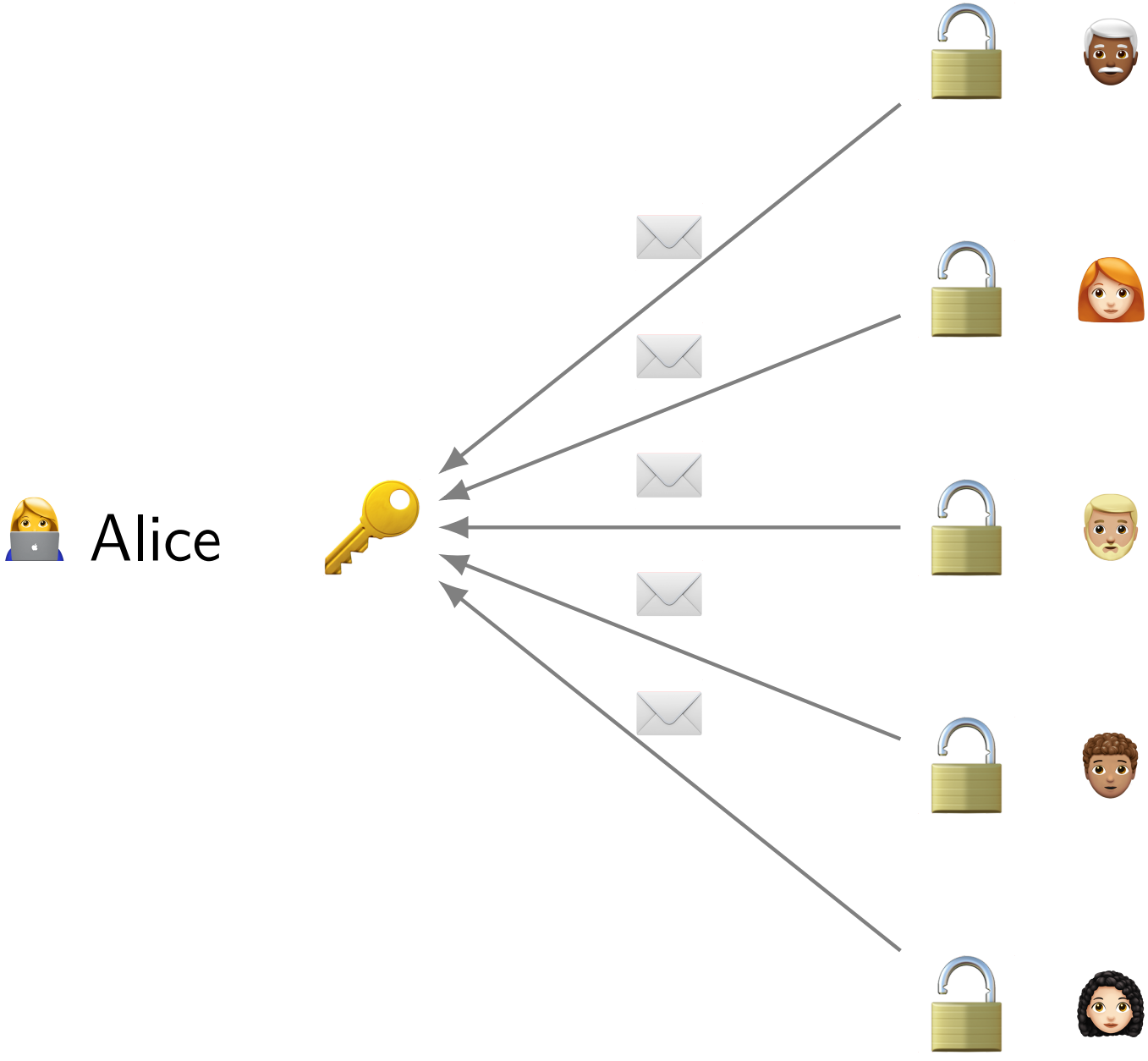
Asymmetrische Kryptographie

- Ein Kryptosystem, in dem man den selben Schlüssel zur Verschlüsselung wie zur Entschlüsselung verwendet, heisst symmetrisch.

Asymmetrische Kryptographie

- Ein Kryptosystem, in dem man den selben Schlüssel zur Verschlüsselung wie zur Entschlüsselung verwendet, heisst symmetrisch.
- Bei einem asymmetrischen Kryptosystem werden verschiedene Schlüssel zur Ver- und Entschlüsselung verwendet.

Bild Private Key vs. Public Key



Asymmetrisches Kryptosystem Ablauf

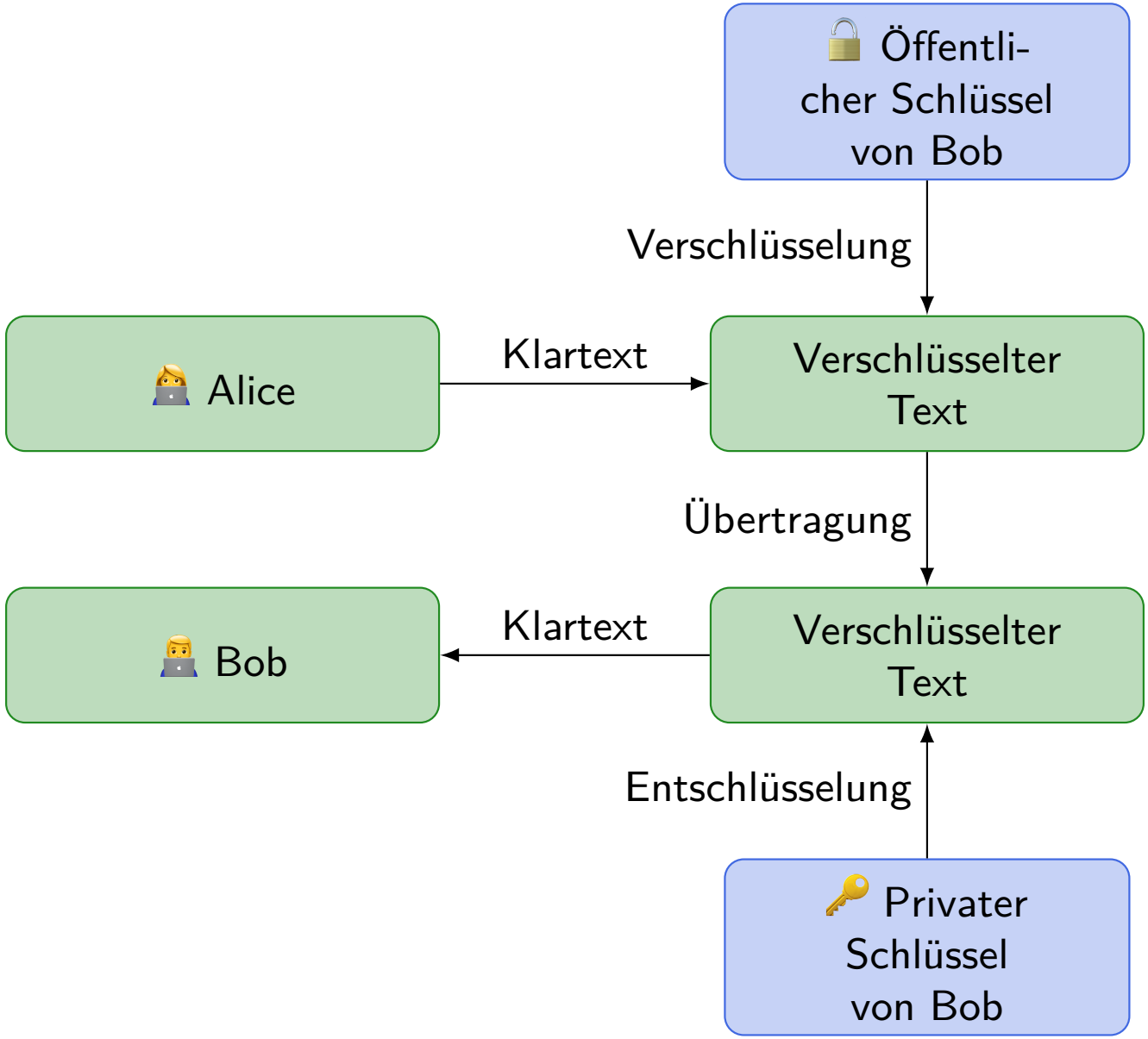


Abbildung: Prinzip der Public-Key-Verschlüsselung

DHM ein asymmetrisches Kryptosystem

- Auch wenn Diffie-Hellman-Merkle zur Schlüsselgenerierung und nicht zum ver-/entschlüsseln verwendet wird, gilt es als ein asymmetrisches Kryptosysytem.

DHM ein asymmetrisches Kryptosystem

- Auch wenn Diffie-Hellman-Merkle zur Schlüsselgenerierung und nicht zum ver-/entschlüsseln verwendet wird, gilt es als ein asymmetrisches Kryptosysytem.
- Frage: Was ist bei DHM der Public Key? Was ist der Private Key?

Definition Umkehrfunktion

Definition (Umkehrfunktion)

Sei $f : A \to B$ eine Funktion. Die Funktion $g : B \to A$ ist die Umkehrfuntkion auch Inverse von F wenn

$$g(f(a)) = a \quad \forall a \in A.$$

Häufig schreibt man die inverse Funktion einer Funktion f als f^{-1}.

Aufgabe

Aufgabe 0.1

1. Wählen Sie und Ihr/e Nachbar/in gemainsam eine beliebige invertierbare Funktion f aus (z. B. $f(x) = 3x - 4$), und bestimmen Sie f^{-1}.
2. Eine Person verschlüsselt nun eine Nachricht (Zahl) mit der Funktion f, die andere mit der Funktion f^{-1}.
3. Tauschen Sie die Ergebnisse aus und verwenden Sie dieselbe Funktion, die Sie zum Verschlüsseln Ihrer Nachricht verwendet haben, zum Entschlüsseln.
4. Erhalten Sie die Zahl, die Ihr/e Nachbar/in ursprünglich verschlüsselt hat?
5. Warum verwenden Sie zweimal dieselbe Funktion?

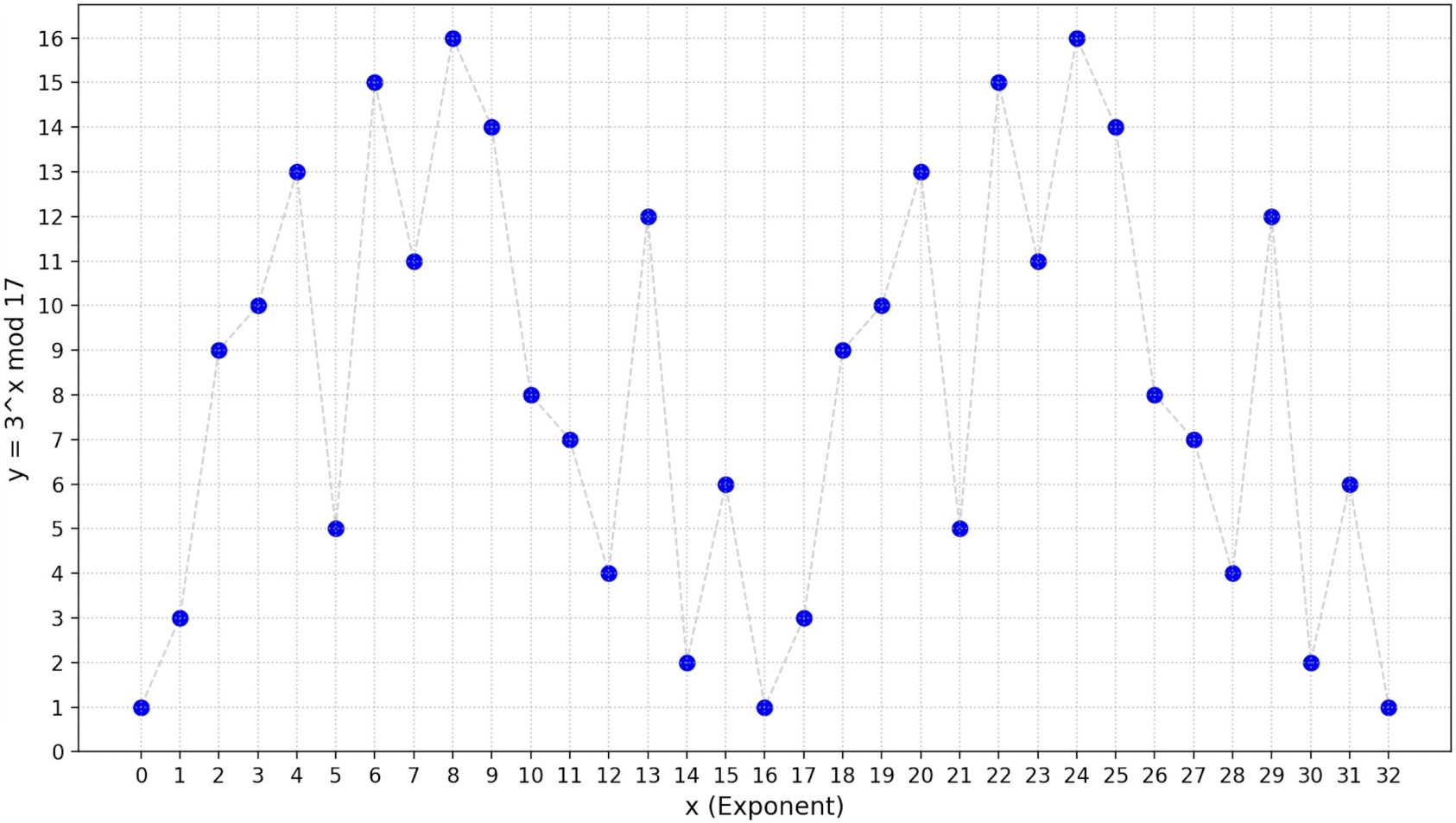
Definition Einwegfunktion

Definition (Einwegfunktion (informell))

Eine Einwegfunktion ist eine mathematische Funktion f, für die gilt:

- Man kann die Funktion $f(x) = y$ "einfach" berechnen; d.h. der Computer kann dies effizient.
- Die Umkehrfunktion $f^{-1}(y) = x$ ist "schwierig"zu berechnen und kann auch von einem Computer nicht effizient berechnet werden.

Umkehrfunktion Diffie-Hellman-Merkle



Hinweis Umkehrfunktionen

Bei allen Funktionen die für Asymetrische Kyptosysteme verwendet werden, kann man nicht beweisen, dass die Umkehrfunktion schwierig zu berechnen ist.

Hinweis Umkehrfunktionen

Bei allen Funktionen die für Asymetrische Kyptosysteme verwendet werden, kann man nicht beweisen, dass die Umkehrfunktion schwierig zu berechnen ist.
Wir haben nur **bisher** keinen schnellen Algorithmus gefunden.

RSA Schlüsselerzeugung

Das RSA-Verfahren besteht aus folgenden Schritten:

Vorgehen

1. **Schlüsselerzeugung:**
   - Wählen Sie zwei Primzahlen p und q.
   - Berechnen Sie das **RSA-Modul** $n = p \cdot q$.
   - Berechnen Sie die **Eulersche Funktion** $\varphi(n) = (p-1)(q-1)$.
   - Wählen Sie den **Verschlüsselungsexponenten** e, so dass e teilerfremd zu $\varphi(n)$ und $e < \varphi(n)$ ist.
   - Berechnen Sie den **Entschlüsselungsexponenten** d, so dass $(e \cdot d) \mod \varphi(n) = 1$.
   - Die Zahlen p, q und $\varphi(n)$ werden nun nicht mehr benötigt und können gelöscht werden.

RSA Verschlüsselung

Vorgehen

1. **Verschlüsselung:**
   - Der Absender verschlüsselt eine **Klartext-Nachricht m** (als Zahl) mit dem **öffentlichen Schlüssel** $(\mathbf{e}, \mathbf{n})$:

$$c = \mathbf{m}^e \mod n.$$

   - Das Ergebnis c ist der Kryptotext.
2. **Entschlüsselung:**
   - Der Empfänger entschlüsselt die **verschlüsselte Nachricht c** mit dem **privaten Schlüssel** $(\mathbf{d}, \mathbf{n})$:

$$\mathbf{m} = c^d \mod n.$$

   - Das Ergebnis **m** ist die ursprüngliche Nachricht.

RSA Beispiel Schlüsselerzeugung

1. Wir wählen zwei (für diese Übung kleine) Primzahlen aus, $p = 3$ und $q = 11$. Daraus folgt:

$$n = p \cdot q = 3 \cdot 11 = 33$$
$$\varphi(n) = (p-1)(q-1) = 2 \cdot 10 = 20$$

RSA Beispiel Schlüsselerzeugung

1. Wir wählen zwei (für diese Übung kleine) Primzahlen aus, $p = 3$ und $q = 11$. Daraus folgt:

$$n = p \cdot q = 3 \cdot 11 = 33$$
$$\varphi(n) = (p-1)(q-1) = 2 \cdot 10 = 20$$

2. Wir wählen $e = 3$, da $\text{ggT}(3, 20) = 1$ und $e < \varphi(n)$.

RSA Beispiel Schlüsselerzeugung

1. Wir wählen zwei (für diese Übung kleine) Primzahlen aus, $p = 3$ und $q = 11$. Daraus folgt:

$$n = p \cdot q = 3 \cdot 11 = 33$$
$$\varphi(n) = (p-1)(q-1) = 2 \cdot 10 = 20$$

2. Wir wählen $e = 3$, da $\text{ggT}(3, 20) = 1$ und $e < \varphi(n)$.
3. Wir berechnen d, so dass $(e \cdot d) \mod \varphi(n) = 1$ ergibt:

$$(d \cdot 3) \mod 20 = 1 \quad \rightarrow \quad d = 7.$$

RSA Beispiel Schlüsselerzeugung

1. Wir wählen zwei (für diese Übung kleine) Primzahlen aus, $p = 3$ und $q = 11$. Daraus folgt:

$$n = p \cdot q = 3 \cdot 11 = 33$$
$$\varphi(n) = (p-1)(q-1) = 2 \cdot 10 = 20$$

2. Wir wählen $e = 3$, da $\text{ggT}(3, 20) = 1$ und $e < \varphi(n)$.
3. Wir berechnen d, so dass $(e \cdot d) \mod \varphi(n) = 1$ ergibt:

$$(d \cdot 3) \mod 20 = 1 \quad \rightarrow \quad d = 7.$$

4. Der öffentliche Schlüssel ist $(e, n) = (3, 33)$. Der private ist $(d, n) = (7, 33)$.

RSA Beispiel Schlüsselerzeugung

1. Wir wählen zwei (für diese Übung kleine) Primzahlen aus, $p = 3$ und $q = 11$. Daraus folgt:

$$n = p \cdot q = 3 \cdot 11 = 33$$
$$\varphi(n) = (p-1)(q-1) = 2 \cdot 10 = 20$$

2. Wir wählen $e = 3$, da $\text{ggT}(3, 20) = 1$ und $e < \varphi(n)$.
3. Wir berechnen d, so dass $(e \cdot d) \mod \varphi(n) = 1$ ergibt:

$$(d \cdot 3) \mod 20 = 1 \quad \rightarrow \quad d = 7.$$

4. Der öffentliche Schlüssel ist $(e, n) = (3, 33)$. Der private ist $(d, n) = (7, 33)$.
5. Sei $m = 5$, dann ist

$$c = m^e \mod n = 5^3 \mod 33 = 26 \quad \text{und}$$
$$c^d \mod n = 26^7 \mod 33 = 5$$

Aufgabe

Was macht RSA schwierig zu brechen?

Aufgabe 0.2

Versuchen Sie herauszufinden was die Umkehrfunktion ist, auf die RSA basiert.

1. Welche Gleichung muss Eve lösen, damit sie die verschlüsselte Nachricht entschlüsseln kann?
2. Was wissen wir über die Unbekannten in der Gleichung?/ Welche andere Gleichung müsste Eve lösen, um die Unbekannte zu finden?

Eulersche Phi Funktion

- Die Eulersche Phi Funktion $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ ist definiert als $\varphi(x) := \mid \{a \in \mathbb{N} \mid 1 \leq a \leq x \wedge ggt(a, x) = 1\} \mid$.

Eulersche Phi Funktion

- Die Eulersche Phi Funktion $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ ist definiert als $\varphi(x) := \mid \{a \in \mathbb{N} \mid 1 \leq a \leq x \wedge ggt(a, x) = 1\} \mid$.
  $\to$ Zählt wie viele natürliche Zahlen zwischen 1 und n teilerfremd zu n sind.

Eulersche Phi Funktion

- Die Eulersche Phi Funktion $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ ist definiert als $\varphi(x) := \mid \{a \in \mathbb{N} \mid 1 \leq a \leq x \wedge ggt(a, x) = 1\} \mid$.
  $\to$ Zählt wie viele natürliche Zahlen zwischen 1 und n teilerfremd zu n sind.
- $\varphi(p) = p - 1$ wenn p eine Primzahl.

Eulersche Phi Funktion

- Die Eulersche Phi Funktion $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ ist definiert als $\varphi(x) := \mid \{a \in \mathbb{N} \mid 1 \leq a \leq x \wedge ggt(a, x) = 1\} \mid$.
  $\to$ Zählt wie viele natürliche Zahlen zwischen 1 und n teilerfremd zu n sind.
- $\varphi(p) = p - 1$ wenn p eine Primzahl.
- $\varphi(p^k) = p^k \cdot p^{k-1}$, da die einzigen Teiler von p^k die Zahlen $1 \cdot p, 2 \cdot p, \ldots, p^{k-1}p$ sind.

Eulersche Phi Funktion

- Die Eulersche Phi Funktion $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ ist definiert als $\varphi(x) := \mid \{a \in \mathbb{N} \mid 1 \leq a \leq x \wedge ggt(a, x) = 1\} \mid$.
  $\to$ Zählt wie viele natürliche Zahlen zwischen 1 und n teilerfremd zu n sind.
- $\varphi(p) = p - 1$ wenn p eine Primzahl.
- $\varphi(p^k) = p^k \cdot p^{k-1}$, da die einzigen Teiler von p^k die Zahlen $1 \cdot p, 2 \cdot p, \ldots, p^{k-1}p$ sind.
- Für a, b teilerfremd gilt $\varphi(a \cdot b) = \varphi(a)\varphi(b)$.

Eulersche Phi Funktion

- Die Eulersche Phi Funktion $\varphi : \mathbb{N}_+ \to \mathbb{N}_+$ ist definiert als $\varphi(x) := \mid \{a \in \mathbb{N} \mid 1 \leq a \leq x \wedge ggt(a, x) = 1\} \mid$.
  $\to$ Zählt wie viele natürliche Zahlen zwischen 1 und n teilerfremd zu n sind.
- $\varphi(p) = p - 1$ wenn p eine Primzahl.
- $\varphi(p^k) = p^k \cdot p^{k-1}$, da die einzigen Teiler von p^k die Zahlen $1 \cdot p, 2 \cdot p, \ldots, p^{k-1}p$ sind.
- Für a, b teilerfremd gilt $\varphi(a \cdot b) = \varphi(a)\varphi(b)$.
- Sei $n = p_1^{k_1} \cdot p_2^{k_2} \ldots p_j^{k_j}$ die Primfactorzerlegung von $n \in \mathbb{N}$,
  $\to \varphi(n) = \prod_{i=1}^{j} p_i^{k_i - 1}(p_i - 1)$

Umkehrfunktion RSA

Aufgabe 0.3

Lösungsvorschlag zu Aufgabe 0.3

Um eine Verschlüsselte Nachricht zu entschlüsseln, muss Eve d herausfinden. Sie weiss, dass $e \cdot d \mod \varphi(n) = 1$, wobei $n = p \cdot q$. Da p und q Primzahlen sind, sind sie teilerfremd und es muss $\varphi(n) = (p-1)(q-1)$. Dies bedeutet, dass wenn Eve n in seine Primfaktoren zerlegen kann, dann kann sie RSA knacken. Das Problme ist, dass wir keinen effizienten Algorithmus kennen, der die Primfaktorzerlegung berechnet.

Aufgabe RSA

Aufgabe 0.4

Suchen Sie sich eine/n Partner/in und spielen Sie das RSA Protokoll gemeinsam durch.

1. Wählen Sie $p = 7$ und $q = 13$ (Sie können auch andere Primzahlen verwenden). Berechnen Sie n und $\varphi(n)$ gemeinsam.
2. Danach sollte jeder alleine einen öffentlichen und einen privaten Schlüssel berechnen.
3. Teilen Sie ihrer/m Partner/in den öffentlichen Schlüssel mit und verslüsseln Sie eine Nachricht an Ihre/n Partner/in, mit dem Schlüssel, den Sie erhalten haben.
4. Entschlüssel Sie die Nachricht, die Sie von Ihrer/m Partner/in bekommen, mit Ihrem privaten Schlüssel.

Zusammenfassung

- **Asymmetrische Kryptosystem** Verwenden einen öffentlichen Schlüssel zum verschlüsseln und einen privaten Schlüssel zum entschlüsseln.

Zusammenfassung

- **Asymmetrische Kryptosystem** Verwenden einen öffentlichen Schlüssel zum verschlüsseln und einen privaten Schlüssel zum entschlüsseln.
- Die Schwierigkeit, asymmetrische Kryptosysteme zu knacken, liegt dadrin, dass es schwieig ist, die **Inverse** der Verschlüsselungsfunktion zu bestimmen.

Zusammenfassung

- **Asymmetrische Kryptosystem** Verwenden einen öffentlichen Schlüssel zum verschlüsseln und einen privaten Schlüssel zum entschlüsseln.
- Die Schwierigkeit, asymmetrische Kryptosysteme zu knacken, liegt dadrin, dass es schwieig ist, die **Inverse** der Verschlüsselungsfunktion zu bestimmen.
- **RSA** Beispiel für ein asymmetrisches Kryptosystem