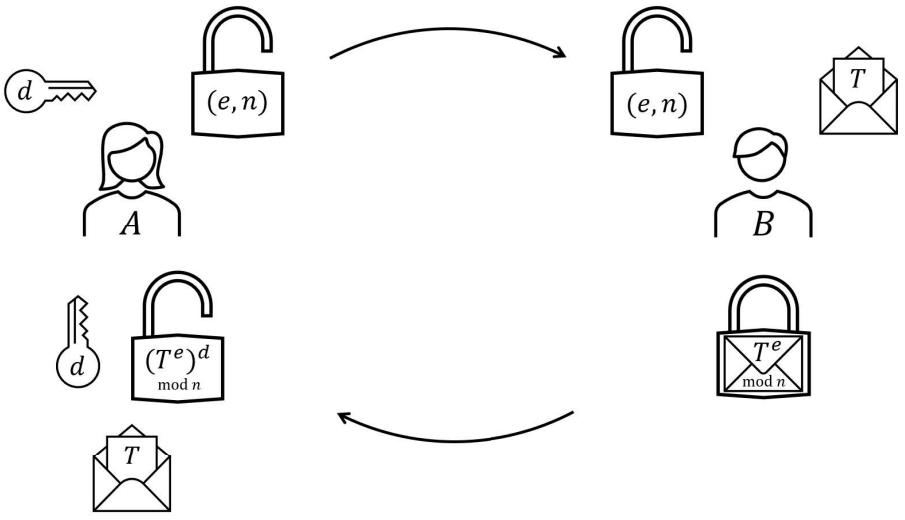
MSG-Zirkel 9b

RSA III: Die Ver- und Entschlüsselung

1. Wie funktioniert das RSA-Verfahren?

1. **Erzeugung des öffentlichen Schlüssels:** Alice wählt zwei Primzahlen p und q und bildet deren Produkt $n = pq$. Dann berechnet sie $\varphi(n) := (p-1)(q-1)$ und wählt ein dazu teilerfremdes $e \in \mathbb{N}$. Das Zahlenpaar (e, n) ist Alice' öffentlicher Schlüssel.
2. **Erzeugung des privaten Schlüssels:** Alice ermittelt ein Inverses von e modulo $\varphi(n)$, d. h. ein $d \in \mathbb{N}$ mit $ed \equiv 1 \mod \varphi(n)$. Die Zahl d ist ihr privater Schlüssel.
3. **Verschlüsselung der Nachricht:** Bob überführt seine Nachricht in eine natürliche Zahl $T < n$. Dann nutzt er Alice' öffentlichen Schlüssel, um $T^e \mod n$ zu berechnen. Das ist die verschlüsselte Nachricht, die er an Alice sendet.
4. **Entschlüsselung der Nachricht:** Alice nutzt ihren privaten Schlüssel d, um $(T^e)^d \mod n$ zu berechnen. Weil
$$(T^e)^d \equiv T \mod n \tag{RSA}$$
gilt, erhält sie so Bobs unverschlüsselte Nachricht T.



(a) Alice wählt die Primzahlen $p = 5$ und $q = 11$ und erhält $N = pq = 55$. Sie berechnet $\varphi(n) := (p-1)(q-1) = 40$ und wählt die dazu teilerfremde Zahl $e = 7$.

Ermittle mithilfe des erweiterten euklidischen Algorithmus Alice' privaten Schlüssel, also eine Zahl $d \in \mathbb{N}$ mit $ed \equiv 1 \mod \varphi(n)$. *(Kontrolle: $d = 23$)*

(b) Bob möchte die Nachricht $T = 8$ verschlüsselt an Alice senden.

Bestimme die verschlüsselte Nachricht $T^e \mod n$. *(Kontrolle: $T^e \mod n = 2$)*

(c) Alice erhält von Bob die verschlüsselte Nachricht $T^e \mod n = 2$.

Entschlüssle diese Nachricht, indem du $(T^e)^d \mod n$ berechnest.

2. Warum funktioniert das RSA-Verfahren?

Die mathematische Grundlage des RSA-Kryptosystems ist die „RSA-Gleichung“

$$(T^e)^d \equiv T \mod n.$$

Beweise die Gültigkeit dieser Gleichung mithilfe der folgenden Anleitung:

(a) Es seien $a, b \in \mathbb{Z}$ und p, q zwei verschiedene Primzahlen. Zeige, dass gilt:

$$a \equiv b \mod p \quad \wedge \quad a \equiv b \mod q \quad \Rightarrow \quad a \equiv b \mod pq$$

(b) Mit den Bezeichnungen aus der Beschreibung des RSA-Verfahrens gilt $ed \equiv 1 \mod \varphi(n)$ mit $\varphi(n) = (p-1)(q-1)$.

Begründe, dass es ganze Zahlen k bzw. l gibt mit

$$ed = k \cdot (p-1) + 1 \quad \text{bzw.} \quad ed = l \cdot (q-1) + 1.$$

(c) Beweise nun mithilfe von (b) und dem kleinen Satz von Fermat, dass

$$(T^e)^d \equiv T \mod p \quad \text{und} \quad (T^e)^d \equiv T \mod q$$

gilt.

Wegen (a) und (c) folgt direkt die Gültigkeit der RSA-Gleichung.

Christoph Lieben c.lieben@hu-berlin.de