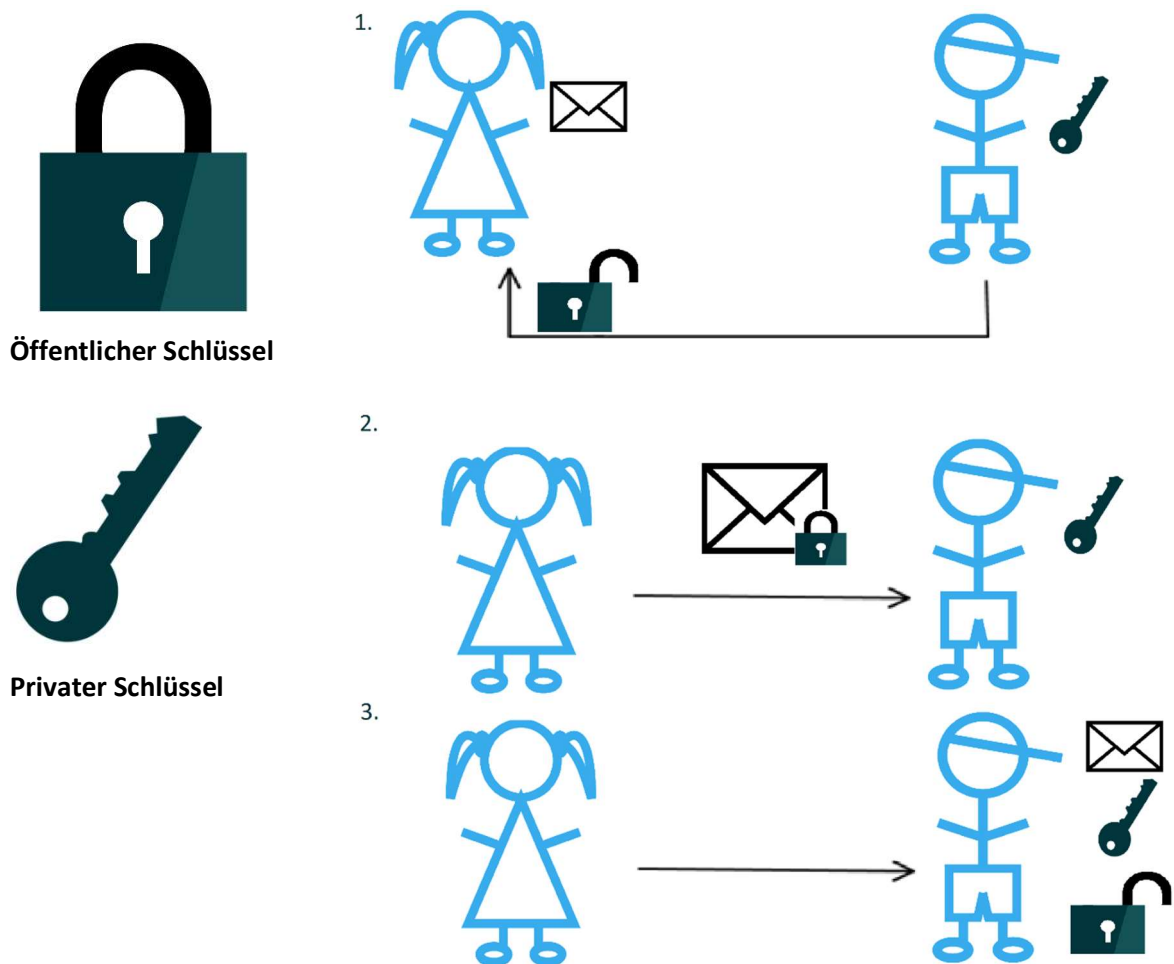
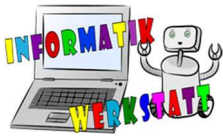


Public-Key Verschlüsselung - RSA

1. Bob (Empfänger) gibt Alice (Sender) einen öffentlichen Schlüssel (*public key*)
2. Alice kann mit diesem öffentlichen Schlüssel den Brief verschlüsseln. Das ist so, als ob er an der Nachricht ein Schloss anbringt, das nur mit dem passenden Schlüssel geöffnet werden kann. Der passende Schlüssel ist der private Schlüssel, den Bob hat.
3. Bob erhält den Brief und kann das Schloss mit seinem privaten Schlüssel öffnen.

Hier im Beispiel will Lena Max einen Liebesbrief schicken. Sie will, dass nur Max den Brief lesen kann. Deswegen verschlüsselt sie ihn mit einem Schloss, das sie vorher von ihm bekommen hat. Da nur Max den Schlüssel für dieses Schloss hat, kann nur er den Brief lesen.





Beispiel

Wenn du nun ein Wort verschlüsseln möchtest, brauchst du als erstes den öffentlichen Schlüssel, also Max's Schloss. Dann gehst du so vor:

- 1) Zuerst musst du die Buchstaben der zu verschlüsselnden Nachricht in Zahlen mithilfe des ASCII-Codes umwandeln:
HALLO: 72, 65, 76, 76, 79
- 2) Danach verschlüsselst du die Zahlen, indem du sie in Formel einsetzt. Dazu musst du für die Buchstaben „e“ und „N“ die angegebenen Werte des **öffentlichen Schlüssels** einsetzen. Das „M“ ersetzt du einfach mit dem Buchstaben im ASCII-Code.

öffentlicher Schlüssel: Modul $N = 187$, Exponent $e = 7$

$$C = M^e \bmod N$$

$$H: 72^7 \bmod 187 = 30$$

$$A: 65^7 \bmod 187 = 142$$

$$L: 76^7 \bmod 187 = 32$$

$$O: 79^7 \bmod 187 = 139$$

→ HALLO = 30, 142, 32, 32, 139

- 3) Willst du nun diese Zahlen wieder entschlüsseln, musst du einfach für „d“ und „N“ die angegebenen Zahlen des **privaten Schlüssels** einsetzen. Danach musst du noch das „C“ durch die verschlüsselte Zahl ersetzen.

privaten Schlüssel: Modul $N = 187$, Exponent $d = 23$

$$M = C^d \bmod N$$

$$H: 30^{23} \bmod 187 = 72$$

$$A: 142^{23} \bmod 187 = 65$$

- 4) Danach vergleichst du die Ergebnisse wieder mit ASCII Tabelle, um die einzelnen Zahlenwerte in Zeichen/Buchstaben umwandeln:
72 → H
65 → A, ...