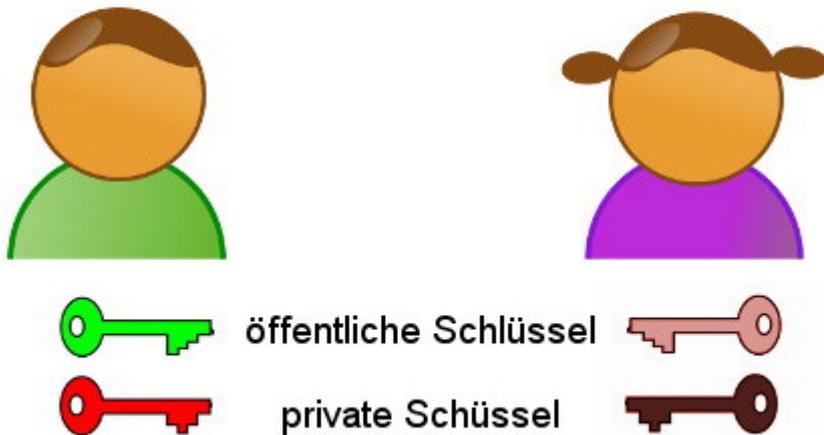
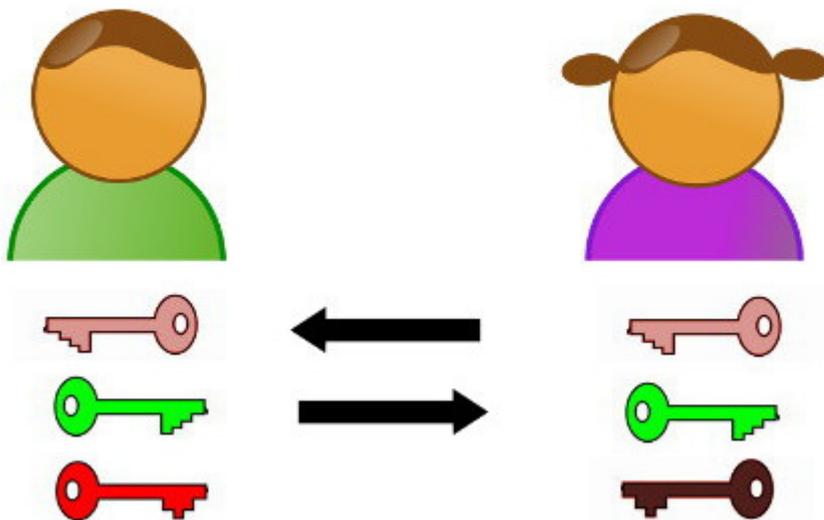


Alice und Bob

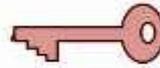
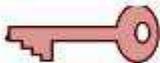
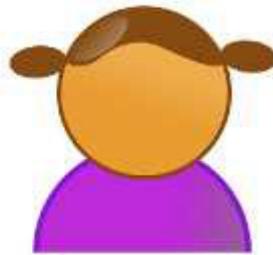
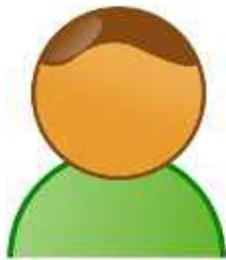
1. Schritt: Bob und Alice erzeugen jeweils ein Schlüsselpaar - einen "öffentlichen" ("public key") und einen "privaten" ("secret key") Schlüssel.



2. Schritt: Bob und Alice tauschen per E-Mail ihre öffentlichen Schlüssel aus.



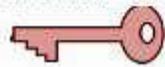
3. Schritt: Bob und Alice schreiben eine Nachricht und verschlüsseln die mit dem öffentlichen Schlüssel des Empfängers.



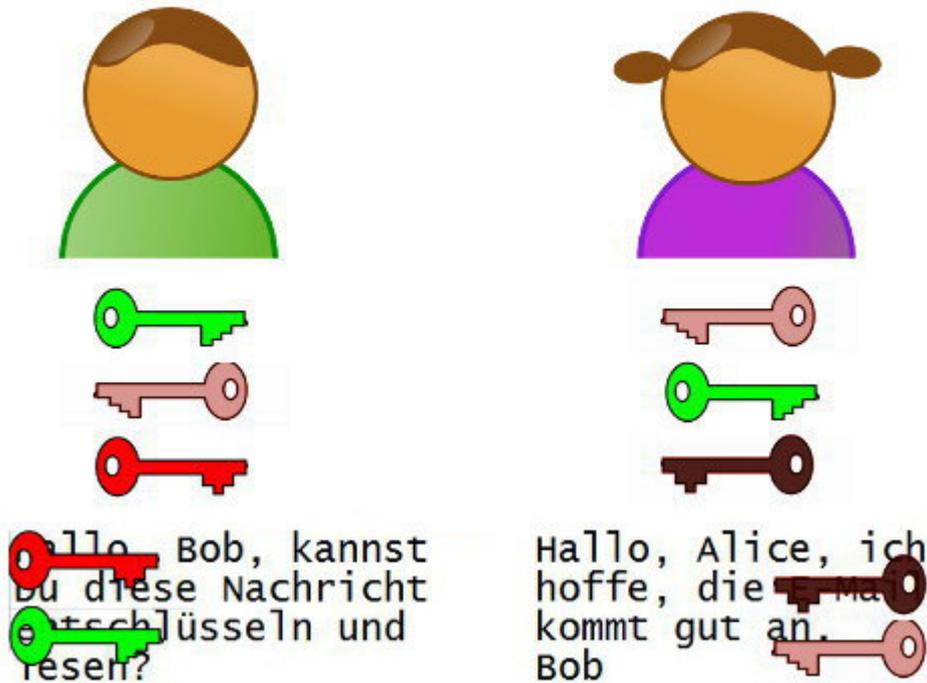
```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
  NACHRICHT AN ALICE
hQQ0A+KRd1qqJviNEA//bXtE6Qq
9sRxJOSS+Ys
rJDiqSTSK1L
6pmuWy0N0h2
ve/qMPkZ+FmPkFcktrQL4sY6Ta9
```



```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
  NACHRICHT AN BOB
f00Cw5bya1M1CGP/99WrVCx5M/
17uKiVKqJFTK
5Z/ucCT0DTc6
r1u0q0e000p+0T0v j38HPbFC6dpf
ih1V71deKaOdJgXRnyL4Unw+00
```



4. Schritt: Bob entschlüsselt Alices Nachricht mit seinem geheimen Schlüssel - nur der passt zu seinem öffentlichen Schlüssel, mit dem die Nachricht verschlüsselt war. Alice entschlüsselt Bobs Nachricht mit ihrem geheimen Schlüssel.



Ich habe vier kleine Grafiken gebaut, um das Prinzip der asymmetrischen Verschlüsselung einfach zu erklären. Die werde ich wohl in das Tutorial übertragen. Ich hatte keine vernünftigen Bilder in deutsche Sprache zum Thema gefunden. [Gimp](#) sei Dank kann man ja sehr schnell selbst etwas erstellen. Die Abbildungen stehen wie gewohnt unter der [Creative Commons Attribution-NonCommercial 3.0 Germany License](#).