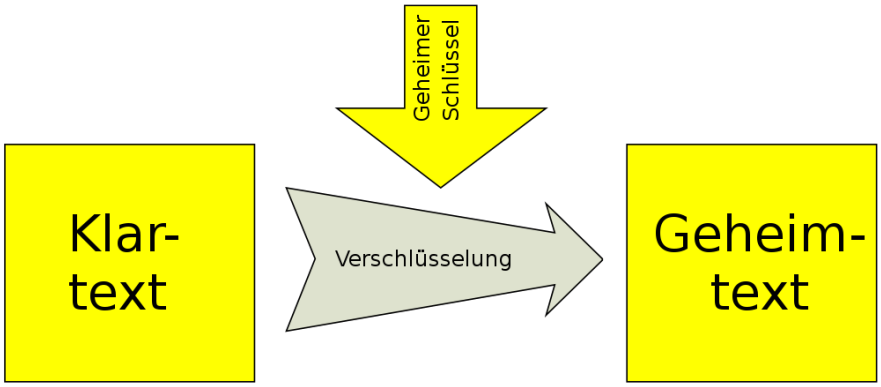
# Verschlüsselung

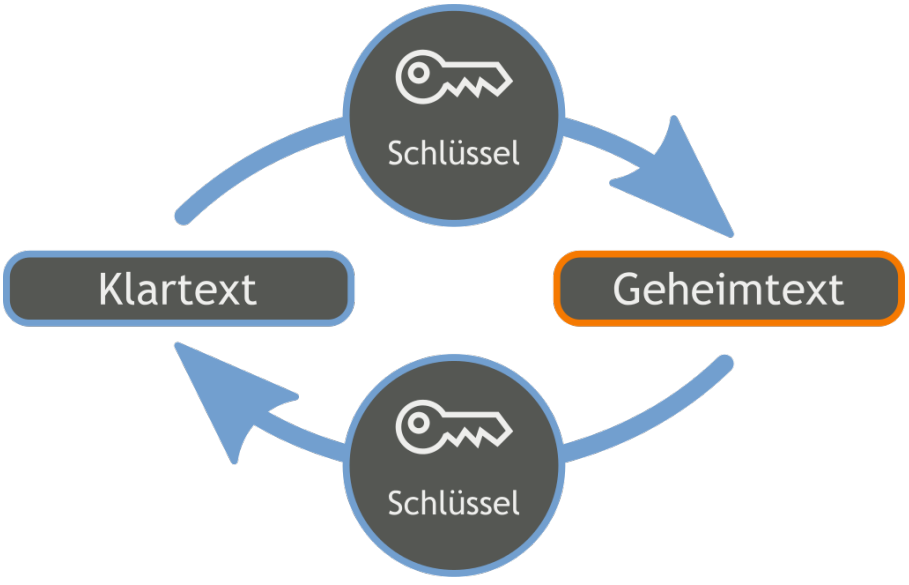
## Grundsätzlich

- Die von einem Schlüssel abhängige Umwandlung von Klartext in Geheimtext, so das der Klartext aus dem Geheimtext nur mit Hilfe des Schlüssels wieder gewonnen werden kann




## symmetrische Verschlüsselung

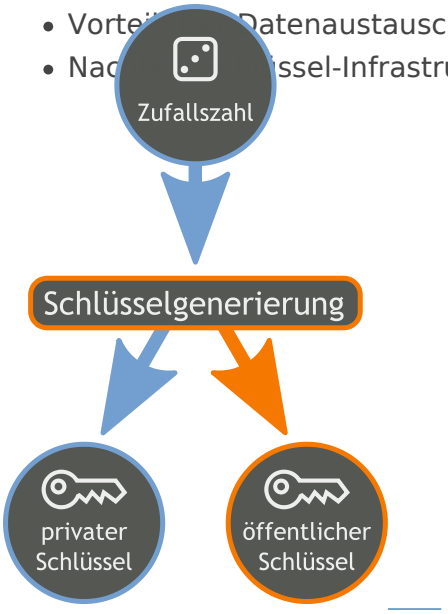
- beide Teilnehmer verwenden den gleichen Schlüssel
- Vorteil: Verschlüsselung und Entschlüsselung sehr schnell
- Nachteil: Der Schlüssel muss über einen gesicherten Kanal ausgetauscht werden

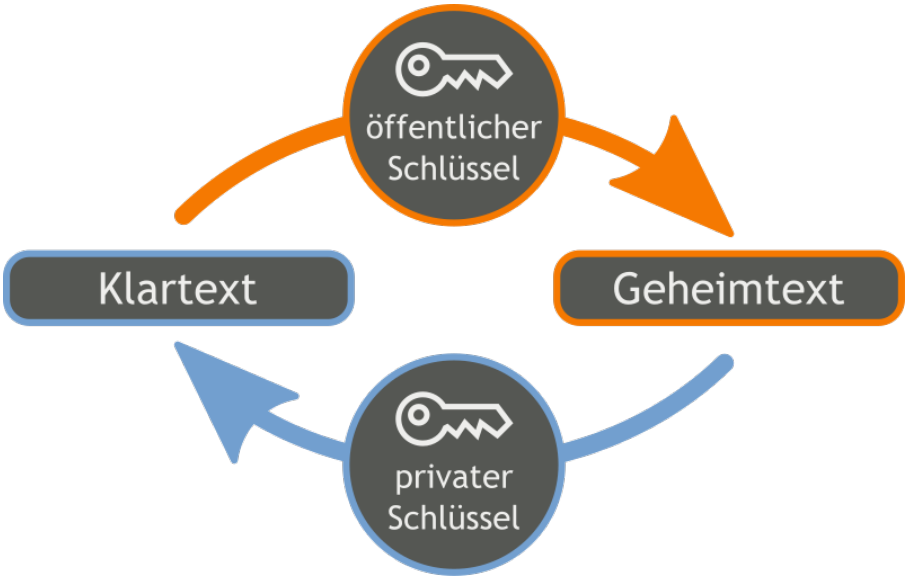



## asymmetrische Verschlüsselung

- Aufteilung in einen privaten und einen öffentlichen Schlüssel
- Der private Schlüssel wird mit niemanden geteilt und von niemandem eingesehen
- Der öffentliche Schlüssel kann frei zugängig gemacht werden

- Nachrichten werden mit Hilfe des öffentlichen Schlüssels des Gegenüber verschlüsselt und können nur mit Hilfe des privaten Schlüssels entschlüsselt werden
- Vorte[illegible]Datenaustausch ist sehr sicher
- Nac[illegible]ssel-Infrastruktur notwendig und Kommunikations nicht mehr so schnell



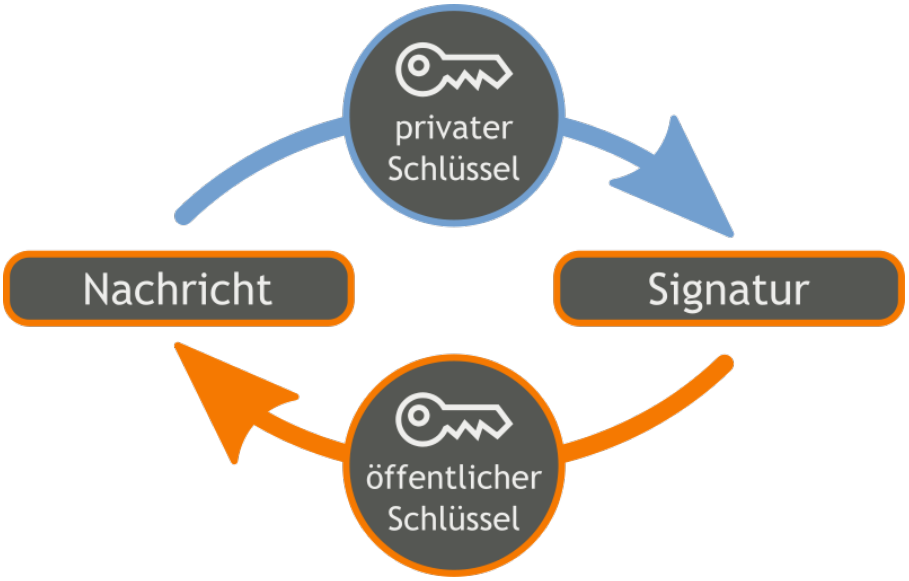




- Lösung: Kombination beider Verfahren
  - Nach dem Verbindungsaufbau wird mit Hilfe von privaten und öffentlichen Schlüsseln ein gemeinsamer Schlüssel ausgehandelt. Damit ist die Kommunikation zu Beginn kurz langsamer, man kann sich aber sicher sein, dass der gemeinsame Schlüssel geheim ist.
  - Aufbau: handelt mit Hilfe des asymmetrischen Schlüssels einen symmetrischen Schlüssel aus
  - Austausch: Daten werden mit Hilfe des symmetrischen Schlüssels ausgetauscht
  - Abbau: Verbindung wird beendetk

## Signatur

- Authentizität: Stammen die Informationen wirklich vom Absender

- Integrität: Sind die Informationen nicht verändert worden
- Lösung:
  - erstellen einer Prüfsumme
  - Signieren der Prüfsumme mit Hilfe des privaten Schlüssels
  - Kontrolle der Authentizität durch Entschlüsseln der Signatur mit Hilfe des öffentlichen Schlüssels
  - Kontrolle der Integriät durch eigene Berechnung der Prüfsumme und Vergleich mit gesendeter, signierter Prüfsumme




---

Created 2022-08-02 14:47:01 UTC by Joshua Lieder
Updated 2022-11-04 10:58:55 UTC