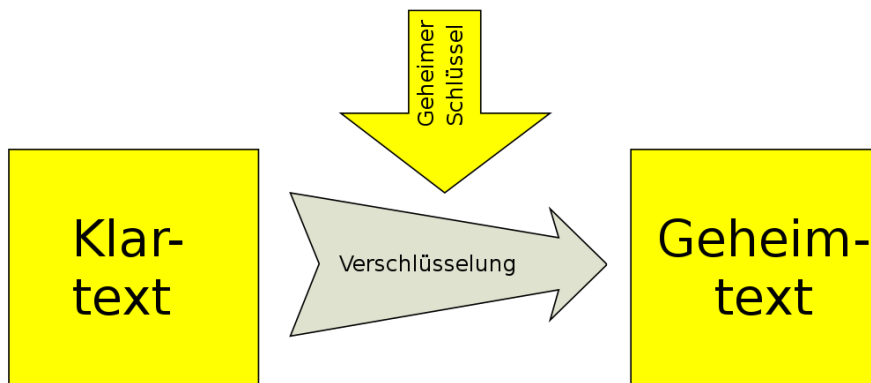


Verschlüsselung

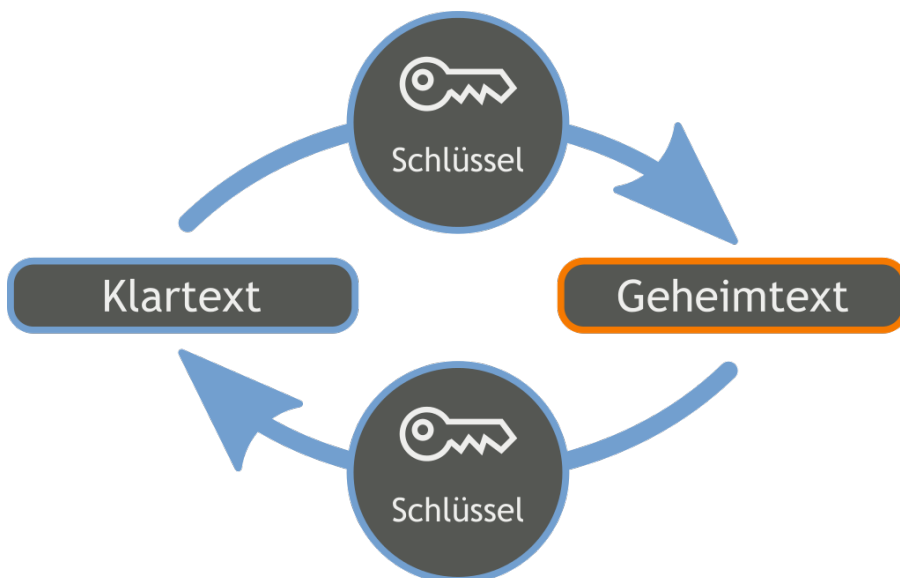
Grundsätzlich

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



symmetrische Verschlüsselung

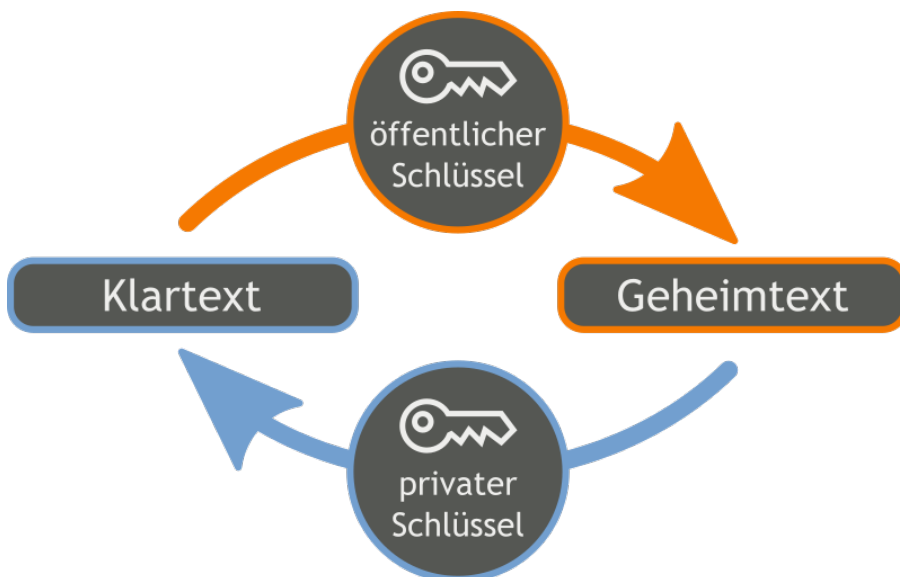
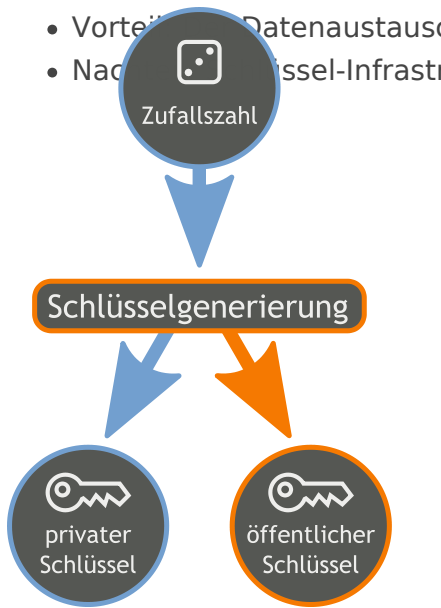
- beide Teilnehmer verwenden den gleichen Schlüssel
- Vorteil: Verschlüsselung und Entschlüsselung sehr schnell
- Nachteil: Der Schlüssel muss über einen gesicherten Kanal ausgetauscht werden



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 zugänglich gemacht werden

- Nachrichten werden mit Hilfe des öffentlichen Schlüssels des Gegenüber verschlüsselt und können nur mit Hilfe des privaten Schlüssels entschlüsselt werden
- Vorteil: Datenaustausch ist sehr sicher
- Nachteil: Schlüssel-Infrastruktur notwendig und Kommunikation nicht mehr so schnell

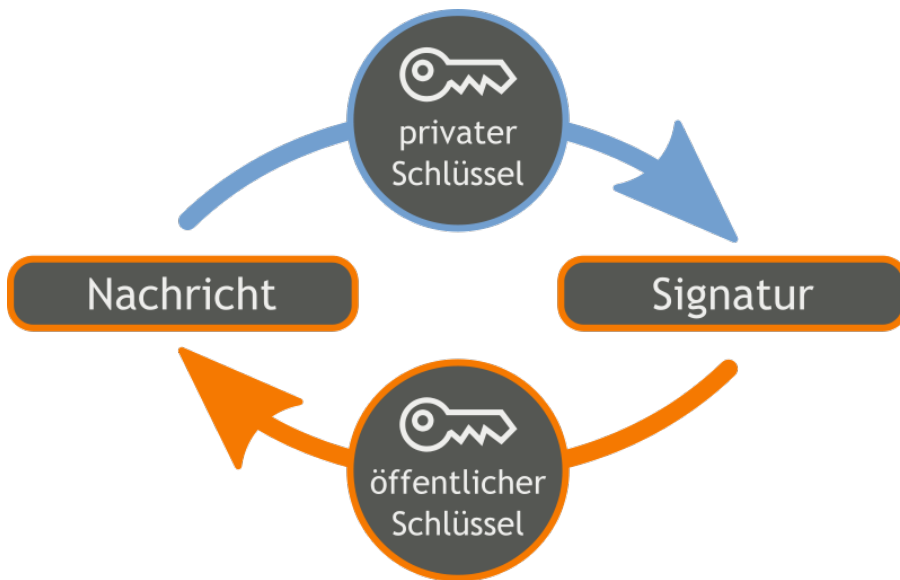


- Lösung: Kombination beider Verfahren
 - Nach dem Verbindungsaufbau wird mit Hilfe von privaten und öffentlichen Schlüsseln ein gemeinsamer Schlüssel ausgehandelt. Damit ist die Kommunikation zu Beginn kurz langsamer, man kann sich aber sicher sein, dass der gemeinsame Schlüssel geheim ist.
 - Aufbau: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

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 Integrität durch eigene Berechnung der Prüfsumme und Vergleich mit gesendeter, signierter Prüfsumme



Revision #6

Created 2 August 2022 14:47:01 by Joshua Lieder

Updated 4 November 2022 10:58:55 by Christoph Wirth