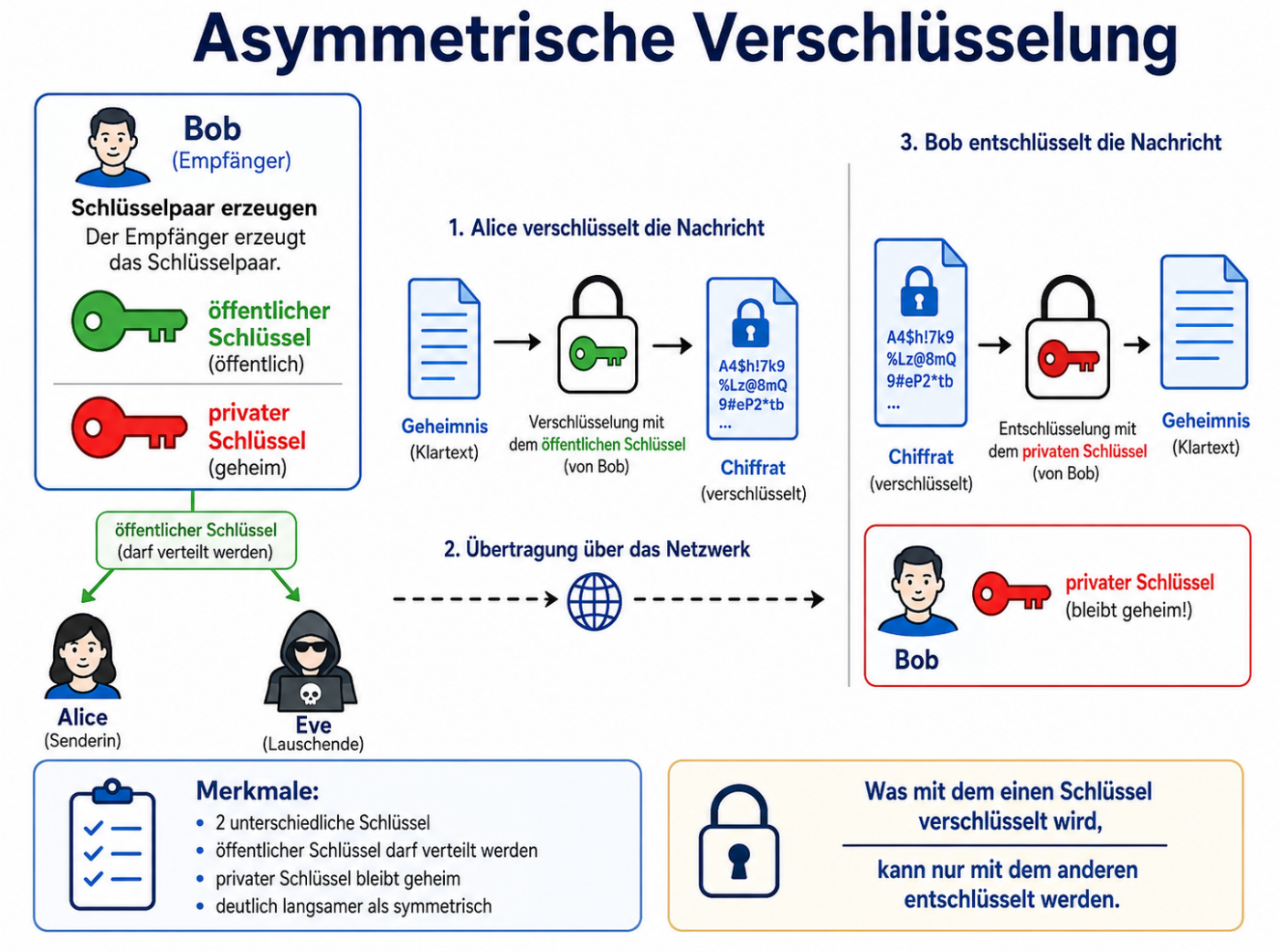
13.2 Asymmetrische Verschlüsselung



Kurzüberblick

Bei der **asymmetrischen Verschlüsselung** gibt es nicht nur einen gemeinsamen Schlüssel, sondern ein **Schlüsselpaar**.

Dieses Schlüsselpaar besteht aus:

- einem **öffentlichen Schlüssel**
- einem **privaten Schlüssel**

Der öffentliche Schlüssel darf verteilt werden.
Der private Schlüssel bleibt geheim.

> **IHK-Merksatz:**
> Asymmetrisch bedeutet: **zwei unterschiedliche Schlüssel**.
> Einer ist öffentlich, einer bleibt privat.

Grundidee

Wenn Alice eine geheime Nachricht an Bob senden möchte, muss Bob zuerst ein Schlüsselpaar erzeugen.

Das ist wichtig:

> **Der Empfänger des Geheimnisses erzeugt das Schlüsselpaar.**

In unserem Beispiel ist Bob der Empfänger.

Bob erzeugt also:

Schlüssel	Bedeutung
öffentlicher Schlüssel	darf an Alice und andere Personen weitergegeben werden
privater Schlüssel	bleibt geheim bei Bob

Alice nutzt dann **Bobs öffentlichen Schlüssel**, um die Nachricht zu verschlüsseln.

Bob nutzt seinen **privaten Schlüssel**, um die Nachricht zu entschlüsseln.

Warum braucht man zwei Schlüssel?

Bei der symmetrischen Verschlüsselung gibt es ein Problem:

Alice und Bob brauchen denselben geheimen Schlüssel.
Dieser Schlüssel muss sicher übertragen werden.

Bei der asymmetrischen Verschlüsselung ist das anders:

Der öffentliche Schlüssel darf offen verteilt werden.
Dadurch muss kein geheimer Schlüssel ungeschützt verschickt werden.

> **Kurz gesagt:**
> Asymmetrische Verschlüsselung hilft beim Problem der sicheren

> Schlüsselübergabe.

Ablauf: Alice sendet ein Geheimnis an Bob

Schritt	Erklärung
1	Bob erzeugt ein Schlüsselpaar.
2	Bob behält den privaten Schlüssel geheim.
3	Bob veröffentlicht seinen öffentlichen Schlüssel.
4	Alice nimmt Bobs öffentlichen Schlüssel.
5	Alice verschlüsselt damit ihre Nachricht.
6	Die verschlüsselte Nachricht wird über das Netzwerk übertragen.
7	Bob entschlüsselt mit seinem privaten Schlüssel.
8	Bob kann den Klartext lesen.

Einfaches Beispiel

Rolle	Was passiert?
Bob	erzeugt öffentlichen und privaten Schlüssel
Bob	gibt den öffentlichen Schlüssel frei
Alice	verschlüsselt mit Bobs öffentlichem Schlüssel
Eve	kann den öffentlichen Schlüssel ebenfalls sehen
Bob	entschlüsselt mit seinem privaten Schlüssel
Eve	kann nicht entschlüsseln, weil ihr der private Schlüssel fehlt

---

Wichtiger Grundsatz

Was mit dem einen Schlüssel verschlüsselt wird, kann nur mit dem anderen passenden Schlüssel entschlüsselt werden.

Das bedeutet hier:

Aktion	Schlüssel
Verschlüsseln für Bob	Bobs öffentlicher Schlüssel
Entschlüsseln durch Bob	Bobs privater Schlüssel

> **Merksatz:**
> Zum geheimen Senden an Bob nutzt Alice **Bobs öffentlichen Schlüssel**.
> Zum Lesen nutzt Bob **seinen privaten Schlüssel**.

Öffentlicher Schlüssel

Der öffentliche Schlüssel darf verteilt werden.

Er kann zum Beispiel:

- auf einer Webseite stehen
- in einem Zertifikat enthalten sein
- an Kommunikationspartner gesendet werden
- von Alice verwendet werden
- auch von Eve gesehen werden

Das ist nicht schlimm, weil der öffentliche Schlüssel allein nicht zum Entschlüsseln reicht.

> **Wichtig:**
> Öffentlich bedeutet nicht unsicher.
> Der öffentliche Schlüssel ist dafür gedacht, verteilt zu werden.

Privater Schlüssel

Der private Schlüssel ist das eigentliche Geheimnis.

Er darf nicht weitergegeben werden.

Wenn der private Schlüssel gestohlen wird, ist die Sicherheit gefährdet.

Der private Schlüssel wird genutzt zum Beispiel für:

- Entschlüsseln
- digitale Signatur
- Identitätsnachweis
- Zugriff auf geschützte Kommunikation

> **Achtung Prüfungsfalle:**
> Der private Schlüssel wird niemals veröffentlicht.
> Er bleibt beim Besitzer.

Vorteile der asymmetrischen Verschlüsselung

Vorteil	Erklärung
kein geheimer Schlüssel muss vorher gemeinsam übertragen werden	Der öffentliche Schlüssel darf verteilt werden
geeignet für Schlüsselaustausch	Ein Sitzungsschlüssel kann sicher übertragen werden
ermöglicht digitale Signaturen	Absender und Integrität können geprüft werden
Grundlage für Zertifikate	Identitäten können mit öffentlichen Schlüsseln verbunden werden

Nachteile der asymmetrischen Verschlüsselung

Nachteil	Erklärung
langsamer als symmetrische Verschlüsselung	Rechenaufwand ist höher
nicht ideal für große Datenmengen	Für große Daten nutzt man besser symmetrische Verschlüsselung
private Schlüssel müssen gut geschützt werden	Verlust oder Diebstahl ist kritisch
Zertifikatsprüfung kann nötig sein	Man muss wissen, ob der öffentliche Schlüssel wirklich zur richtigen Person gehört

Warum verschlüsselt man nicht einfach alles asymmetrisch?

Asymmetrische Verschlüsselung ist praktisch, aber langsam.

Für große Datenmengen wäre das ineffizient.

Darum nutzt man in der Praxis meistens ein **hybrides Verfahren**:

- asymmetrisch für den sicheren Schlüsselaustausch
- symmetrisch für die schnelle Datenverschlüsselung

Das ist wichtig für:

- HTTPS
- TLS
- VPN
- sichere Kommunikation im Internet

> **Kurz gesagt:**
> Asymmetrisch löst das Schlüsselübergabe-Problem.
> Symmetrisch verschlüsselt danach schnell die eigentlichen Daten.

Vergleich: symmetrisch und asymmetrisch

Merkmal	Symmetrisch	Asymmetrisch
Anzahl der Schlüssel	ein gemeinsamer Schlüssel	zwei Schlüssel
Schlüsselarten	geheimer Schlüssel	öffentlicher und privater Schlüssel
Geschwindigkeit	schnell	langsamer
Hauptproblem	Schlüsselübergabe	höherer Rechenaufwand
typischer Einsatz	große Datenmengen	Schlüsselaustausch, Zertifikate, Signatur
Beispielprinzip	Alice und Bob haben denselben Schlüssel	Alice nutzt Bobs öffentlichen Schlüssel

---

Bezug zur digitalen Signatur

Asymmetrische Verfahren können nicht nur für Verschlüsselung genutzt werden.

Sie können auch für digitale Signaturen genutzt werden.

Dabei ist die Richtung anders:

Zweck	Verwendeter Schlüssel
Nachricht an Bob verschlüsseln	Bobs öffentlicher Schlüssel
Nachricht von Bob entschlüsseln	Bobs privater Schlüssel
Signatur von Bob erstellen	Bobs privater Schlüssel
Signatur von Bob prüfen	Bobs öffentlicher Schlüssel

> **Wichtig:**
> Verschlüsselung schützt die Vertraulichkeit.
> Signatur prüft Authentizität und Integrität.

Typische Praxisbeispiele

Bereich	Rolle der asymmetrischen Verschlüsselung
HTTPS / TLS	sicherer Schlüsselaustausch und Zertifikate
VPN	Aufbau sicherer Verbindungen
digitale Signatur	Echtheit und Unverändertheit prüfen
Zertifikate	öffentlicher Schlüssel wird einer Identität zugeordnet
E-Mail-Verschlüsselung	öffentliche Schlüssel können zum Verschlüsseln genutzt werden
SSH	Schlüsselpaare können zur Anmeldung genutzt werden

Typische IHK-Fragen zur asymmetrischen Verschlüsselung

Was ist asymmetrische Verschlüsselung?

Bei der asymmetrischen Verschlüsselung gibt es zwei unterschiedliche Schlüssel: einen öffentlichen und einen privaten Schlüssel.

Wer erzeugt das Schlüsselpaar?

Der Empfänger erzeugt das Schlüsselpaar, wenn er verschlüsselte Nachrichten empfangen möchte.

Was passiert mit dem öffentlichen Schlüssel?

Der öffentliche Schlüssel darf verteilt werden.

Was passiert mit dem privaten Schlüssel?

Der private Schlüssel bleibt geheim beim Besitzer.

Welchen Schlüssel nutzt Alice, wenn sie Bob eine geheime Nachricht senden möchte?

Alice nutzt **Bobs öffentlichen Schlüssel**.

Welchen Schlüssel nutzt Bob zum Entschlüsseln?

Bob nutzt **seinen privaten Schlüssel**.

Warum ist asymmetrische Verschlüsselung wichtig?

Sie löst das Problem, wie man sicher einen Schlüssel austauschen kann.

Warum nutzt man asymmetrische Verschlüsselung nicht für alle Daten?

Weil sie langsamer ist als symmetrische Verschlüsselung.

Prüfungsfalle: öffentlicher Schlüssel ist nicht geheim

Der öffentliche Schlüssel darf von allen gesehen werden.

Auch Eve darf ihn kennen.

Das ist nicht das Problem.

Das Problem wäre nur, wenn Eve den **privaten Schlüssel** bekommt.

Schlüssel	Darf Eve ihn sehen?	Sicherheitsproblem?
öffentlicher Schlüssel	ja	nein
privater Schlüssel	nein	ja, sehr kritisch

> **Achtung:**
> Öffentlich heißt hier wirklich öffentlich.
> Geheim bleiben muss nur der private Schlüssel.

Prüfungsfalle: Wer verschlüsselt mit welchem Schlüssel?

Wenn Alice eine Nachricht geheim an Bob senden möchte:

Person	Aktion
Bob	erzeugt Schlüsselpaar
Bob	veröffentlicht öffentlichen Schlüssel
Alice	verschlüsselt mit Bobs öffentlichem Schlüssel
Bob	entschlüsselt mit Bobs privatem Schlüssel

> **Merksatz:**
> Immer an den Empfänger denken:
> Wer lesen soll, dessen öffentlicher Schlüssel wird zum Verschlüsseln genutzt.

Zusammenfassung

Die asymmetrische Verschlüsselung nutzt ein Schlüsselpaar:

- öffentlicher Schlüssel
- privater Schlüssel

Der öffentliche Schlüssel darf verteilt werden.

Der private Schlüssel bleibt geheim.

Alice verschlüsselt eine Nachricht für Bob mit **Bobs öffentlichem Schlüssel**.

Bob entschlüsselt die Nachricht mit **Bobs privatem Schlüssel**.

Der große Vorteil ist:

- Die Schlüsselübergabe wird einfacher.

Der große Nachteil ist:

- Das Verfahren ist langsamer als symmetrische Verschlüsselung.

> **IHK-Spickzettel:**
> Asymmetrisch = öffentlicher + privater Schlüssel
> Öffentlich = darf verteilt werden
> Privat = bleibt geheim
> Verschlüsseln für Bob = Bobs öffentlicher Schlüssel
> Entschlüsseln durch Bob = Bobs privater Schlüssel
> Vorteil = löst Schlüsselübergabe
> Nachteil = langsamer als symmetrisch

Revision #2
Created 2 June 2026 23:27:33 by Admin
Updated 3 June 2026 06:18:12 by Admin