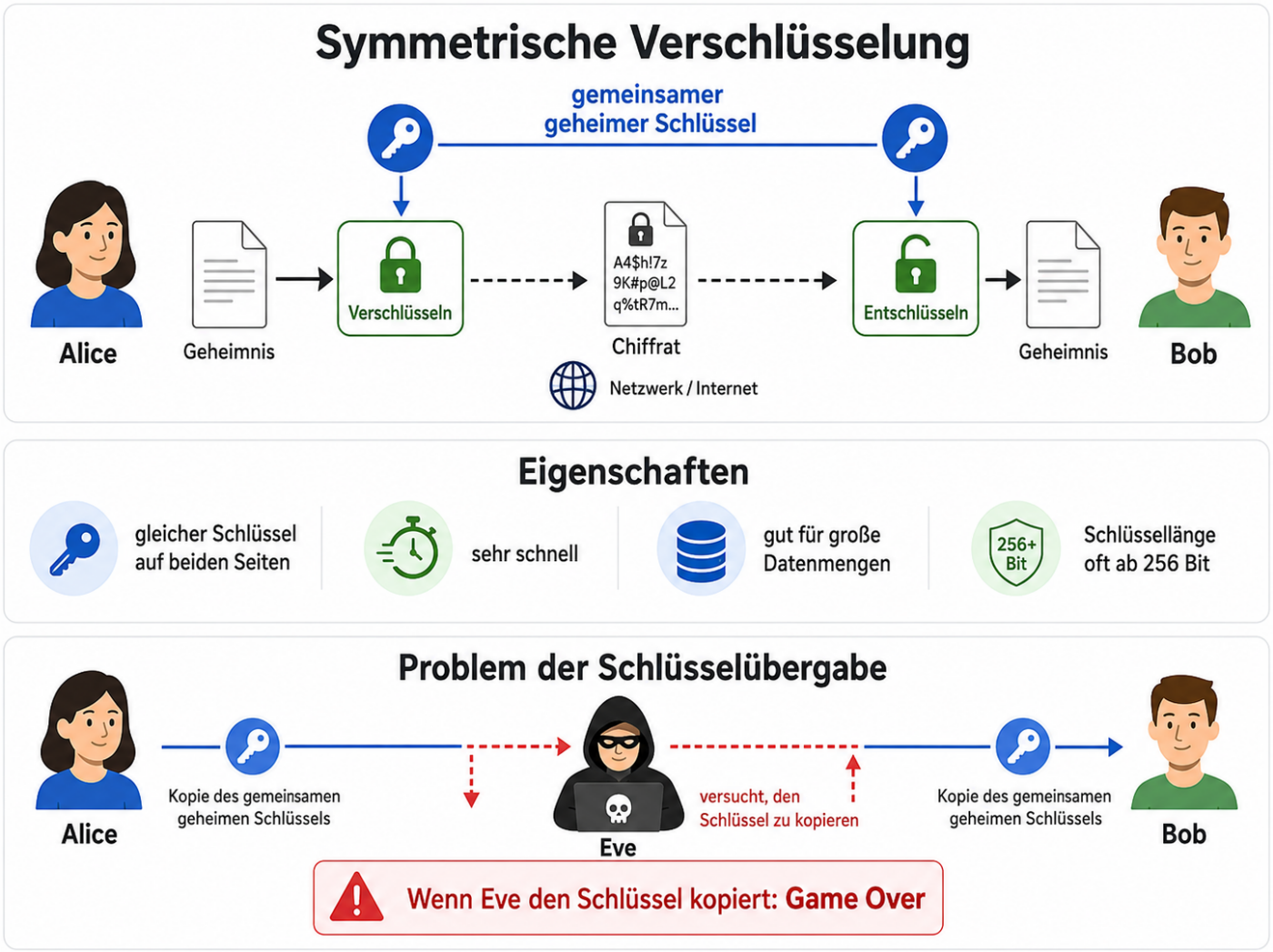
13.1 Symmetrische Verschlüsselung



Kurzüberblick

Bei der **symmetrischen Verschlüsselung** verwenden Sender und Empfänger **denselben geheimen Schlüssel**.

Das bedeutet:

- Alice hat den geheimen Schlüssel.
- Bob hat denselben geheimen Schlüssel.
- Eve darf diesen Schlüssel nicht besitzen.
- Mit demselben Schlüssel wird verschlüsselt und entschlüsselt.

> **IHK-Merksatz:**
> Symmetrisch bedeutet: **ein gemeinsamer geheimer Schlüssel auf beiden Seiten**.

Grundidee

Alice möchte Bob eine geheime Nachricht schicken.

Dafür passiert Folgendes:

Schritt	Erklärung
1	Alice schreibt eine Nachricht im Klartext.
2	Alice verschlüsselt die Nachricht mit dem gemeinsamen geheimen Schlüssel.
3	Über das Netzwerk wird nur der Geheimtext übertragen.
4	Bob entschlüsselt den Geheimtext mit demselben geheimen Schlüssel.
5	Bob erhält wieder den ursprünglichen Klartext.

Einfaches Beispiel

Zustand	Beispiel
Klartext	Passwort: geheim123
gemeinsamer Schlüssel	blauer geheimer Schlüssel
Geheimtext / Chiffrat	A4$h!7k9%Lz@8mQ
entschlüsselter Klartext	Passwort: geheim123

Wichtig ist nicht der Beispieltext selbst, sondern das Prinzip:

> **Nur wer den gemeinsamen geheimen Schlüssel besitzt, kann die Nachricht wieder lesen.**

Eigenschaften der symmetrischen Verschlüsselung

Punkt	Erklärung
Schlüsselanzahl	ein gemeinsamer geheimer Schlüssel
Schlüsselart	beide Seiten nutzen denselben Schlüssel
Geschwindigkeit	sehr schnell
Eignung	gut für große Datenmengen
Hauptproblem	sichere Übergabe des Schlüssels

Punkt	Erklärung
Gefahr	Wenn Eve den Schlüssel bekommt, kann sie entschlüsseln
typische Beispiele	AES, ChaCha20
Sonderfall	One-Time-Pad

Warum ist symmetrische Verschlüsselung schnell?

Symmetrische Verfahren sind für große Datenmengen gut geeignet, weil sie rechnerisch deutlich effizienter sind als asymmetrische Verfahren.

Darum wird symmetrische Verschlüsselung in der Praxis häufig genutzt für:

- große Dateien
- Datenströme
- VPN-Datenverkehr
- HTTPS-Nutzdaten
- WLAN-Verschlüsselung
- verschlüsselte Backups
- Festplattenverschlüsselung

> **Kurz gesagt:**
> Symmetrische Verschlüsselung ist die schnelle Methode für die eigentlichen Nutzdaten.

Das Hauptproblem: Schlüsselübergabe

Der größte Nachteil ist nicht die eigentliche Verschlüsselung, sondern die Frage:

> **Wie bekommt Bob den geheimen Schlüssel, ohne dass Eve ihn kopieren kann?**

Alice und Bob brauchen denselben Schlüssel.
Dieser Schlüssel muss also irgendwie zu Bob gelangen.

Wenn Alice den Schlüssel einfach ungeschützt über das Netzwerk sendet, kann Eve ihn abfangen.

Ablauf des Schlüsselübergabe-Problems

Schritt	Was passiert?	Risiko
1	Alice erzeugt einen geheimen Schlüssel.	noch sicher
2	Bob braucht eine Kopie dieses Schlüssels.	Übergabe nötig
3	Alice sendet den Schlüssel an Bob.	Eve könnte mithören
4	Eve kopiert den Schlüssel.	Sicherheit verloren
5	Eve kann spätere Nachrichten entschlüsseln.	Game Over

> **Achtung Prüfungsfalle:**
> Die Verschlüsselung kann mathematisch stark sein.
> Wenn der Schlüssel aber in falsche Hände kommt, ist die Kommunikation trotzdem unsicher.

Was passiert, wenn Eve den Schlüssel bekommt?

Wenn Eve den gemeinsamen geheimen Schlüssel besitzt, kann sie:

- verschlüsselte Nachrichten entschlüsseln
- mitlesen
- eigene Nachrichten verschlüsseln
- sich eventuell als Teilnehmer ausgeben
- die Sicherheit der Verbindung zerstören

Deshalb gilt:

> **Der Schlüssel ist das eigentliche Geheimnis.**

Vorteil und Nachteil auf einen Blick

Vorteil	Nachteil
sehr schnell	sichere Schlüsselübergabe ist schwierig
gut für große Datenmengen	beide Seiten brauchen denselben geheimen Schlüssel
technisch effizient	Schlüsselverlust macht alles unsicher
in der Praxis sehr wichtig	skaliert schlecht bei vielen Kommunikationspartnern

---

Warum skaliert das schlecht?

Wenn nur Alice und Bob miteinander kommunizieren, reicht ein gemeinsamer Schlüssel.

Bei vielen Personen wird es schwieriger.

Situation	Problem
Alice und Bob	ein gemeinsamer Schlüssel reicht
Alice, Bob und Carla	mehrere Schlüssel nötig
viele Benutzer	sehr viele Schlüssel zwischen den Beteiligten nötig
Unternehmen oder Internet	reine symmetrische Schlüsselverteilung wird unpraktisch

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

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

Das wird später bei **13.6 Hybride Verschlüsselung** wichtig.

Typische Praxisbeispiele

Bereich	Rolle der symmetrischen Verschlüsselung
WLAN	Nutzdaten werden verschlüsselt übertragen
VPN	Daten im Tunnel werden verschlüsselt
HTTPS / TLS	Nutzdaten werden nach dem Schlüsselaustausch symmetrisch verschlüsselt
Festplattenverschlüsselung	Daten auf dem Datenträger werden symmetrisch geschützt
Backups	Sicherungskopien können symmetrisch verschlüsselt werden

---

Typische IHK-Fragen zu symmetrischer Verschlüsselung

Was ist symmetrische Verschlüsselung?

Bei der symmetrischen Verschlüsselung verwenden Sender und Empfänger **denselben geheimen Schlüssel** zum Ver- und Entschlüsseln.

Was ist der wichtigste Vorteil?

Sie ist **schnell** und eignet sich gut für **große Datenmengen**.

Was ist der wichtigste Nachteil?

Der gemeinsame geheime Schlüssel muss **sicher an beide Kommunikationspartner verteilt** werden.

Was passiert, wenn ein Angreifer den Schlüssel bekommt?

Dann kann der Angreifer die verschlüsselten Daten entschlüsseln. Die Sicherheit ist dann verloren.

Warum verwendet man trotzdem symmetrische Verschlüsselung?

Weil sie sehr effizient ist und deshalb in der Praxis für die eigentlichen Nutzdaten verwendet wird.

Prüfungsfalle: symmetrisch vs. asymmetrisch

Merkmal	Symmetrisch	Asymmetrisch
Schlüsselanzahl	ein gemeinsamer Schlüssel	zwei Schlüssel
Schlüsselarten	geheimer Schlüssel	öffentlicher und privater Schlüssel
Geschwindigkeit	schnell	langsamer
Problem	sichere Schlüsselübergabe	mehr Rechenaufwand
typischer Einsatz	große Datenmengen	Schlüsselaustausch, Signatur, Zertifikate

> **Merksatz:**
> Symmetrisch ist schnell, aber die Schlüsselübergabe ist das Problem.
> Asymmetrisch hilft bei der Schlüsselübergabe, ist aber langsamer.

Zusammenfassung

Die symmetrische Verschlüsselung nutzt **einen gemeinsamen geheimen Schlüssel**.

Dieser Schlüssel wird für beide Richtungen verwendet:

- Alice verschlüsselt mit dem Schlüssel.
- Bob entschlüsselt mit demselben Schlüssel.
- Bob kann auch mit demselben Schlüssel verschlüsseln.
- Alice kann mit demselben Schlüssel entschlüsseln.

Der große Vorteil ist die hohe Geschwindigkeit.

Der große Nachteil ist die sichere Übergabe des Schlüssels.

> **IHK-Spickzettel:**
> Symmetrisch = gleicher geheimer Schlüssel
> Vorteil = schnell
> Nachteil = Schlüsselübergabe
> Gefahr = Schlüsselverlust
> Praxis = Nutzdatenverschlüsselung bei WLAN, VPN, HTTPS/TLS, Backups und Festplatten

---

Revision #4
Created 2 June 2026 23:25:00 by Admin
Updated 3 June 2026 06:18:12 by Admin