13.0 Grundlagen der Verschlüsselung

Kurzüberblick

Verschlüsselung bedeutet, dass lesbare Daten so umgewandelt werden, dass sie ohne passenden Schlüssel nicht mehr verständlich sind.

Aus einer lesbaren Nachricht wird ein unlesbarer Geheimtext.

Beispiel:

```
Klartext: Hallo Bob
Geheimtext: A4$h!7k9%Lz@8mQ
```

Erst mit dem passenden Schlüssel kann daraus wieder der ursprüngliche Inhalt entstehen.

> **IHK-Merksatz:**
> Verschlüsselung schützt Inhalte vor unbefugtem Mitlesen.

Quelle und Einordnung

Diese Seite gehört zu:

13. Verschlüsselung und Sicherheitsgrundlagen

In unserer BookStack-Struktur steht dieses Kapitel nach:

11. Firewalls, NAT und DMZ
12. Sniffing, Analyse und Fehlersuche

und vor:

14. VPN, Intranet und Extranet

Warum?

Firewalls regeln, wer wohin kommunizieren darf.
Sniffing zeigt, dass Datenverkehr mitgelesen werden kann.
Verschlüsselung schützt den Inhalt der übertragenen oder gespeicherten Daten.
VPN nutzt Verschlüsselung, um sichere Verbindungen über unsichere Netze aufzubauen.

Warum braucht man Verschlüsselung?

Daten werden in Netzwerken oft über Wege übertragen, die man nicht vollständig kontrolliert.

Beispiele:

- Internet
- WLAN
- öffentliche Netze
- Cloud-Dienste
- VPN-Verbindungen
- E-Mail-Kommunikation
- Webzugriffe über HTTPS

Ohne Verschlüsselung könnten Daten leichter mitgelesen oder missbraucht werden.

Typische schützenswerte Daten sind:

- Passwörter
- Zugangsdaten
- persönliche Daten
- Bankdaten
- Kundendaten
- Firmendaten
- Backups
- private Nachrichten

> **Kurz gesagt:**
> Verschlüsselung sorgt dafür, dass abgefangene Daten ohne Schlüssel nicht sinnvoll gelesen werden können.

Grundbegriffe

Begriff	Bedeutung
Klartext	ursprüngliche lesbare Nachricht
Geheimtext / Chiffrat	verschlüsselte Nachricht
Schlüssel	Wert zum Ver- oder Entschlüsseln
Verschlüsseln	Klartext wird in Geheimtext umgewandelt
Entschlüsseln	Geheimtext wird wieder in Klartext umgewandelt
Algorithmus	mathematisches Verfahren der Verschlüsselung

Begriff	Bedeutung
Alice	typische Senderin in Kryptografie-Beispielen
Bob	typischer Empfänger in Kryptografie-Beispielen
Eve	Angreiferin, Lauscherin oder Manipulatorin

Einfaches Ablaufmodell

Schritt	Erklärung
1	Alice hat eine lesbare Nachricht.
2	Alice verschlüsselt die Nachricht mit einem Schlüssel.
3	Über das Netzwerk wird nur der Geheimtext übertragen.
4	Bob entschlüsselt den Geheimtext mit dem passenden Schlüssel.
5	Bob kann die ursprüngliche Nachricht lesen.

Vereinfacht:

```
Klartext + Schlüssel -> Verschlüsselung -> Geheimtext
Geheimtext + passender Schlüssel -> Entschlüsselung -> Klartext
```

Die drei wichtigsten Sicherheitsziele

Bei Verschlüsselung und IT-Sicherheit tauchen immer wieder drei Begriffe auf:

Sicherheitsziel	Leitfrage	Beispiel
Vertraulichkeit	Können Unbefugte die Daten lesen?	Verschlüsselung, VPN, HTTPS
Integrität	Wurden die Daten verändert?	Hash, digitale Signatur
Authentizität	Ist der Absender oder die Identität echt?	Zertifikat, digitale Signatur, Login

> **IHK-Merksatz:**
> Vertraulichkeit = nur Berechtigte können lesen
> Integrität = Daten wurden nicht verändert
> Authentizität = Identität oder Absender ist echt

Vertraulichkeit

Vertraulichkeit bedeutet:

Nur berechtigte Personen oder Systeme können den Inhalt lesen.

Beispiele:

- HTTPS schützt Webdaten.
- VPN schützt Daten über unsichere Netze.
- WPA2 / WPA3 schützt WLAN-Datenverkehr.
- Festplattenverschlüsselung schützt gespeicherte Daten.

> **Merksatz:**
> Vertraulichkeit schützt vor Mitlesen.

Integrität

Integrität bedeutet:

Daten wurden nicht verändert.

Man möchte erkennen können, ob eine Nachricht, Datei oder Übertragung manipuliert wurde.

Beispiele:

- Hashwert einer Datei prüfen
- digitale Signatur prüfen
- Prüfsumme vergleichen

> **Merksatz:**
> Integrität schützt nicht unbedingt vor Mitlesen, sondern erkennt Veränderungen.

Authentizität

Authentizität bedeutet:

Die Identität ist echt.

Die Leitfrage lautet:

```
Bist du wirklich derjenige, für den du dich ausgibst?
```

Beispiele:

- Benutzer meldet sich mit Passwort an.
- Webseite weist sich mit Zertifikat aus.
- Absender signiert eine Nachricht digital.
- Zwei-Faktor-Authentifizierung bestätigt zusätzlich die Identität.

> **Merksatz:**
> Authentizität prüft Echtheit.

Was Verschlüsselung leisten kann

Verschlüsselung kann helfen bei:

Ziel	Erklärung
Schutz vor Mitlesen	Geheimtext ist ohne Schlüssel nicht verständlich
Schutz gespeicherter Daten	Daten auf Datenträgern oder in der Cloud werden geschützt
sichere Übertragung	Daten können über unsichere Netze übertragen werden
Grundlage für VPN	VPNs nutzen Verschlüsselung für sichere Tunnel
Grundlage für HTTPS	Webseitenverbindungen werden geschützt

Was Verschlüsselung allein nicht automatisch leistet

Verschlüsselung ist wichtig, aber sie löst nicht jedes Sicherheitsproblem automatisch.

Problem	Warum Verschlüsselung allein nicht reicht
falscher Empfänger	Daten können an die falsche Person gesendet werden
gestohlener Schlüssel	Angreifer kann entschlüsseln
unsicheres Passwort	Schlüssel oder Zugang kann erraten werden
manipulierte Software	Daten können vor oder nach der Verschlüsselung abgegriffen werden
unsicheres Endgerät	Klartext kann direkt am Gerät gelesen werden
fehlende Authentizität	Man weiß nicht sicher, mit wem man spricht

> **Achtung Prüfungsfalle:**
> Verschlüsselung schützt den Inhalt, aber nicht automatisch vor allen Angriffen.

Wichtige Verfahren im Überblick

Verfahren	Grundidee
symmetrische Verschlüsselung	gleicher geheimer Schlüssel auf beiden Seiten
asymmetrische Verschlüsselung	öffentlicher und privater Schlüssel
hybride Verschlüsselung	asymmetrisch für Schlüsselaustausch, symmetrisch für Daten
digitale Signatur	Absender und Unveränderheit prüfen
Hashfunktion	Prüfwert zur Integritätsprüfung
Zertifikat	Identität mit öffentlichem Schlüssel verbinden
Diffie-Hellman	gemeinsames Schlüsselmaterial aushandeln
One-Time-Pad	theoretisch sicher bei perfekten Bedingungen
Steganographie	Nachricht in unauffälligen Daten verstecken

Symmetrisch, asymmetrisch und hybrid im Kurzvergleich

Merkmal	Symmetrisch	Asymmetrisch	Hybrid
Schlüsselprinzip	ein gemeinsamer geheimer Schlüssel	öffentlicher + privater Schlüssel	Kombination aus beiden
Geschwindigkeit	schnell	langsamer	praktisch schnell
Hauptvorteil	gut für große Datenmengen	löst Schlüsselübergabe	kombiniert beide Vorteile
Hauptproblem	sichere Schlüsselübergabe	höherer Rechenaufwand	komplexerer Ablauf
typischer Einsatz	Nutzdaten	Schlüssel, Signatur, Zertifikate	HTTPS, TLS, VPN

> **Kurzform:**
> Symmetrisch = schnell
> Asymmetrisch = Schlüsselübergabe lösen
> Hybrid = Praxislösung

Beispiel aus dem Alltag: HTTPS

Wenn du eine Webseite über HTTPS aufrufst, spielen mehrere Sicherheitsbausteine zusammen.

Vereinfacht:

Baustein	Aufgabe
Zertifikat	Browser prüft die Identität der Webseite
asymmetrische Verfahren	helfen beim sicheren Verbindungsaufbau
Sitzungsschlüssel	wird für diese Verbindung genutzt
symmetrische Verschlüsselung	schützt danach die eigentlichen Nutzdaten
Hash / Signatur	helfen bei Prüfung von Integrität und Vertrauen

Das genaue Verfahren ist technisch komplexer, aber für die Grundlagen reicht:

> **“ HTTPS nutzt mehrere Sicherheitsbausteine zusammen.**

Typische Prüfungsfragen zu den Grundlagen

Was bedeutet Verschlüsselung?

Verschlüsselung bedeutet, dass lesbare Daten mit einem Schlüssel in eine unlesbare Form umgewandelt werden.

Was ist Klartext?

Klartext ist die lesbare ursprüngliche Nachricht.

Was ist Geheimtext?

Geheimtext ist die verschlüsselte Form einer Nachricht.

Was ist ein Schlüssel?

Ein Schlüssel ist ein Wert, mit dem Daten ver- oder entschlüsselt werden.

Was bedeutet Vertraulichkeit?

Nur Berechtigte können die Daten lesen.

Was bedeutet Integrität?

Daten wurden nicht verändert.

Was bedeutet Authentizität?

Identität oder Absender ist echt.

Warum ist Verschlüsselung im Netzwerk wichtig?

Weil Daten über unsichere Netze übertragen werden können und vor Mitlesen geschützt werden sollen.

Prüfungsfalle: Verschlüsselung, Hash und Signatur nicht verwechseln

Begriff	Aufgabe
Verschlüsselung	Inhalt unlesbar machen
Hash	Veränderung an Daten erkennen
digitale Signatur	Absender und Integrität prüfen
Zertifikat	Identität und öffentlichen Schlüssel verbinden
Steganographie	Existenz einer Nachricht verstecken

> **Merksatz:**
> Verschlüsselung schützt den Inhalt.
> Hash prüft Daten.
> Signatur prüft Absender und Daten.
> Zertifikat prüft Identität.
> Steganographie versteckt Nachrichten.

Zusammenfassung

Verschlüsselung ist ein Grundbaustein der Netzwerksicherheit.

Sie wandelt lesbare Daten in eine unlesbare Form um.

Nur mit dem passenden Schlüssel können die Daten wieder entschlüsselt werden.

Für die IHK sind besonders wichtig:

- Vertraulichkeit
- Integrität
- Authentizität
- symmetrische Verschlüsselung
- asymmetrische Verschlüsselung
- hybride Verschlüsselung

- Hashfunktion
- digitale Signatur
- Zertifikate
- Diffie-Hellman
- Perfect Forward Secrecy
- Brute Force
- Zufallszahlen
- One-Time-Pad
- Steganographie

> **IHK-Spickzettel:**
> Verschlüsselung = Inhalt schützen
> Vertraulichkeit = nur Berechtigte lesen
> Integrität = Daten unverändert
> Authentizität = Identität echt
> Symmetrisch = gleicher Schlüssel
> Asymmetrisch = öffentlicher + privater Schlüssel
> Hybrid = asymmetrisch für Schlüssel, symmetrisch für Daten

Revision #1
Created 3 June 2026 06:15:29 by Admin
Updated 3 June 2026 06:18:12 by Admin