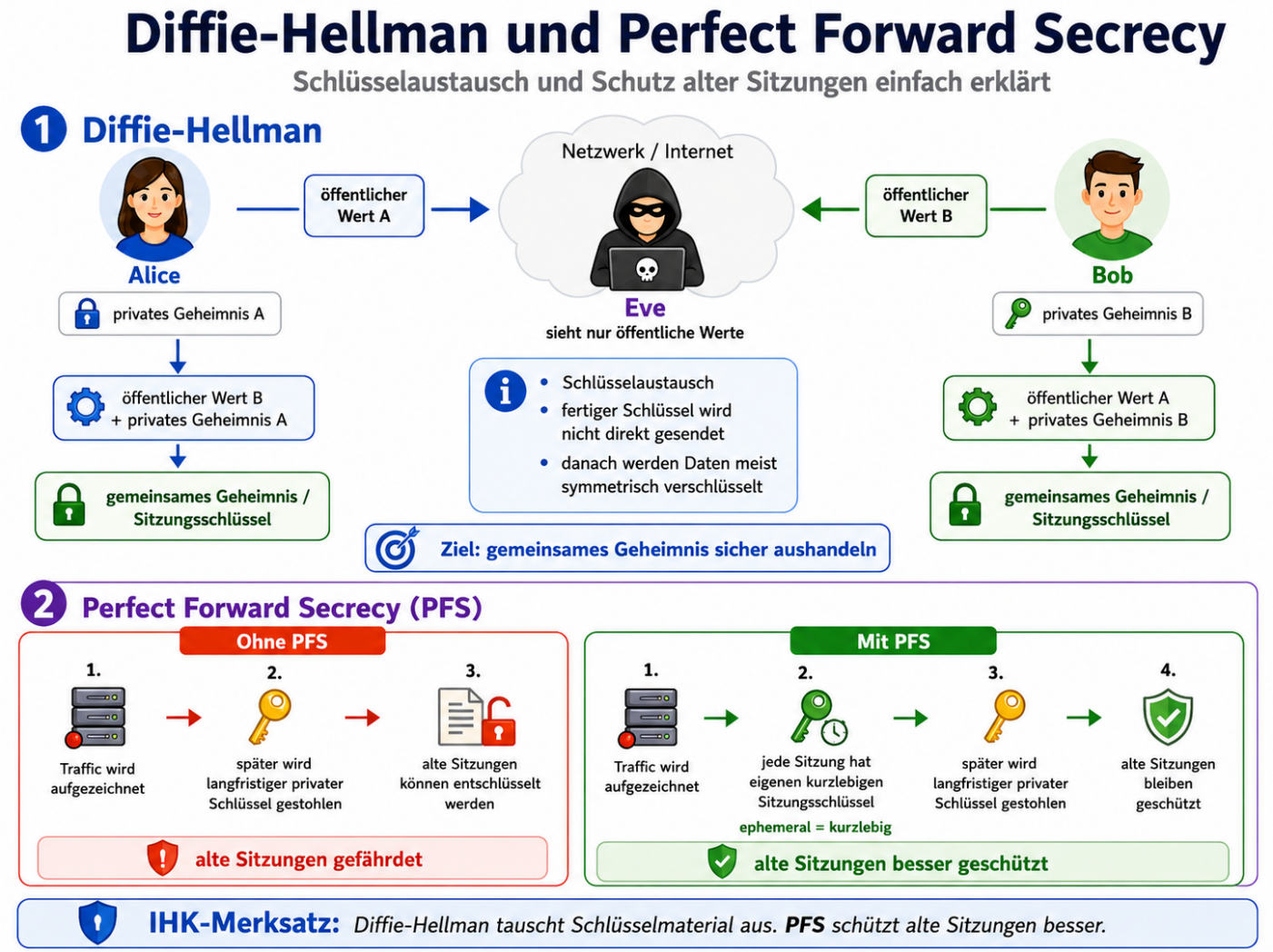
13.6 Diffie-Hellman und Perfect Forward Secrecy



Kurzüberblick

Diffie-Hellman ist ein Verfahren zum **Schlüsselaustausch**.

Es wird nicht dafür genutzt, große Datenmengen direkt zu verschlüsseln.

Die Grundidee ist:

Alice und Bob können über ein unsicheres Netzwerk ein gemeinsames Geheimnis erzeugen, ohne dieses Geheimnis direkt zu übertragen.

> **IHK-Merksatz:**
> Diffie-Hellman = Schlüsselaustausch
> Nicht: direkte Verschlüsselung großer Datenmengen

Quelle 11.1 – Einordnung

In der Quelle wird Diffie-Hellman bei den Unterscheidungsmerkmalen der Verschlüsselungsverfahren genannt.

Es gehört in den Bereich:

- Schlüsselaustausch
- asymmetrische Kryptografie
- sichere Verbindungsaufnahme
- Grundlage für sichere Protokolle
- Perfect Forward Secrecy

Wichtig ist:

Diffie-Hellman ist kein Ersatz für symmetrische Verschlüsselung.

Es hilft dabei, einen gemeinsamen Schlüssel zu erzeugen oder auszuhandeln.

Warum braucht man Diffie-Hellman?

Bei der symmetrischen Verschlüsselung gab es ein Problem:

Alice und Bob brauchen denselben geheimen Schlüssel.

Aber:

Wie bekommen beide denselben Schlüssel, ohne dass Eve ihn einfach kopiert?

Diffie-Hellman löst genau dieses Problem.

> **Kurz gesagt:**
> Alice und Bob einigen sich auf ein gemeinsames Geheimnis, ohne dieses Geheimnis direkt über das Netzwerk zu senden.

Grundidee ohne Mathematik

Alice und Bob wollen einen gemeinsamen Sitzungsschlüssel erhalten.

Eve kann den Netzwerkverkehr mithören.

Trotzdem soll Eve den fertigen Sitzungsschlüssel nicht kennen.

Vereinfacht passiert Folgendes:

Schritt	Erklärung
1	Alice und Bob tauschen öffentliche Informationen aus.
2	Alice kombiniert diese Informationen mit ihrem privaten Geheimnis.
3	Bob kombiniert diese Informationen mit seinem privaten Geheimnis.
4	Beide kommen dadurch auf dasselbe gemeinsame Geheimnis.
5	Eve sieht nur die öffentlichen Informationen, aber nicht die privaten Geheimnisse.

Was sieht Eve?

Eve kann den Datenverkehr beobachten.

Sie sieht zum Beispiel:

- öffentliche Austauschwerte
- Protokollinformationen
- eventuell Zertifikate
- verschlüsselte Daten

Eve sieht aber nicht:

- Alices privaten Anteil
- Bobs privaten Anteil
- den fertigen gemeinsamen Sitzungsschlüssel

Bestandteil	Sichtbar für Eve?	Kritisch?
öffentliche Austauschwerte	ja	normalerweise nein
privater Anteil von Alice	nein	ja, muss geheim bleiben
privater Anteil von Bob	nein	ja, muss geheim bleiben
fertiger Sitzungsschlüssel	nein	ja, muss geheim bleiben

Wichtig: Diffie-Hellman verschlüsselt nicht die Nutzdaten

Ein häufiger Fehler ist:

Diffie-Hellman mit normaler Verschlüsselung zu verwechseln.

Das ist falsch.

Thema	Aufgabe
Diffie-Hellman	gemeinsamen Schlüssel aushandeln
symmetrische Verschlüsselung	Nutzdaten verschlüsseln
asymmetrische Verschlüsselung	Schlüssel schützen, Signaturen, Zertifikate
Hashfunktion	Integrität prüfen
Zertifikat	Identität prüfen

> **Achtung Prüfungsfalle:**
> Diffie-Hellman ist ein Verfahren zum Schlüsselaustausch, nicht die eigentliche Datenverschlüsselung.

Bezug zur hybriden Verschlüsselung

Diffie-Hellman passt gut zum hybriden Prinzip.

Bei der hybriden Verschlüsselung gilt:

- asymmetrische Technik hilft beim sicheren Schlüsselaustausch
- symmetrische Technik verschlüsselt danach die Nutzdaten

Diffie-Hellman kann dabei helfen, den gemeinsamen Sitzungsschlüssel sicher auszuhandeln.

Danach wird dieser Sitzungsschlüssel für symmetrische Verschlüsselung genutzt.

Phase	Technik
Verbindungsaufbau	Schlüsselaustausch, zum Beispiel Diffie-Hellman
danach	symmetrische Verschlüsselung der Nutzdaten
zusätzlich	Zertifikate / Signaturen zur Identitätsprüfung

Einfaches Beispiel

Alice und Bob wollen sicher kommunizieren.

Sie nutzen Diffie-Hellman, um einen gemeinsamen Sitzungsschlüssel zu erzeugen.

Danach verwenden sie diesen Sitzungsschlüssel für die symmetrische Verschlüsselung.

Ablauf:

Schritt	Erklärung
1	Alice und Bob starten den Schlüsselaustausch.
2	Beide tauschen öffentliche Werte aus.
3	Beide nutzen zusätzlich ihr eigenes privates Geheimnis.
4	Beide berechnen denselben Sitzungsschlüssel.
5	Die Nutzdaten werden mit diesem Sitzungsschlüssel symmetrisch verschlüsselt.

Warum ist das sicherer als einfaches Senden des Schlüssels?

Beim einfachen Senden würde Alice den Schlüssel direkt an Bob übertragen.

Dann könnte Eve ihn kopieren.

Bei Diffie-Hellman wird der fertige Schlüssel nicht direkt gesendet.

Stattdessen wird er auf beiden Seiten berechnet.

Direkte Schlüsselübergabe	Diffie-Hellman
Schlüssel wird übertragen	Schlüssel wird auf beiden Seiten berechnet
Eve könnte den Schlüssel kopieren	Eve sieht nur öffentliche Austauschwerte
riskant bei unsicherem Netzwerk	besser für unsichere Netzwerke
einfach zu verstehen	mathematisch komplexer

Perfect Forward Secrecy

Perfect Forward Secrecy bedeutet:

Alte Verbindungen sollen auch dann geschützt bleiben, wenn ein langfristiger privater Schlüssel später kompromittiert wird.

Anders gesagt:

Wenn ein Angreifer heute einen privaten Schlüssel stiehlt, soll er damit nicht automatisch alte aufgezeichnete Sitzungen entschlüsseln können.

> **IHK-Merksatz:**
> Perfect Forward Secrecy schützt alte Sitzungen besser, weil Sitzungsschlüssel nicht dauerhaft gleich bleiben.

Warum ist Perfect Forward Secrecy wichtig?

Eve könnte Datenverkehr heute mitschneiden und speichern.

Später könnte Eve versuchen, einen privaten Schlüssel zu stehlen.

Ohne Perfect Forward Secrecy wäre das gefährlicher.

Mit Perfect Forward Secrecy soll gelten:

- alte Sitzungsschlüssel waren nur kurzzeitig gültig
- alte Sitzungsschlüssel wurden nicht dauerhaft gespeichert
- ein später gestohlener Langzeitschlüssel reicht nicht aus, um alte Sitzungen zu entschlüsseln

---

Beispiel ohne Perfect Forward Secrecy

Eve macht Folgendes:

1. Eve zeichnet heute verschlüsselten Datenverkehr auf.
2. Eve stiehlt später den privaten Schlüssel eines Servers.
3. Eve versucht, alte Verbindungen nachträglich zu entschlüsseln.

Wenn alte Sitzungen vom langfristigen Schlüssel abhängig waren, wäre das problematisch.

Beispiel mit Perfect Forward Secrecy

Bei Perfect Forward Secrecy wird für Sitzungen eigenes, kurzlebiges Schlüsselmaterial verwendet.

Das bedeutet:

1. Jede Sitzung bekommt eigene Schlüssel.
2. Die Sitzungsschlüssel werden später verworfen.
3. Ein später gestohlener Langzeitschlüssel reicht nicht aus, um alte Sitzungen zu entschlüsseln.

Ohne PFS	Mit PFS
alte Sitzungen können stärker vom Langzeitschlüssel abhängen	jede Sitzung nutzt kurzlebige Schlüssel
späterer Schlüsselverlust kann alte Daten gefährden	alte Sitzungen bleiben besser geschützt
weniger Schutz bei aufgezeichnetem Datenverkehr	besserer Schutz gegen nachträgliches Entschlüsseln

---

Ephemeral Diffie-Hellman

Im Zusammenhang mit Perfect Forward Secrecy taucht häufig der Begriff **ephemeral** auf.

Ephemeral bedeutet:

kurzlebig oder nur vorübergehend.

Bei ephemeral Diffie-Hellman werden für einzelne Sitzungen kurzlebige Schlüsselwerte verwendet.

Diese werden nach der Sitzung verworfen.

> **Kurz gesagt:**
> Ephemeral = nur für diese Sitzung gedacht.
> Dadurch werden alte Sitzungen besser geschützt.

Bezug zu HTTPS / TLS

Bei HTTPS beziehungsweise TLS ist das wichtig.

Vereinfacht:

Schritt	Erklärung
1	Browser verbindet sich mit einem Server.
2	Zertifikat hilft bei der Prüfung der Serveridentität.
3	Ein Schlüsselaustauschverfahren hilft beim Erzeugen eines Sitzungsschlüssels.
4	Danach werden die Nutzdaten symmetrisch verschlüsselt.
5	Bei PFS werden alte Sitzungen besser gegen späteren Schlüsselverlust geschützt.

Bezug zu VPN

Auch bei VPNs ist die Idee wichtig.

Ein VPN braucht:

- sichere Identitätsprüfung
- sicheren Schlüsselaustausch
- symmetrische Verschlüsselung der Nutzdaten
- möglichst kurzlebige Sitzungsschlüssel
- Schutz gegen nachträgliches Entschlüsseln alter Sitzungen

Darum passt dieses Thema gut vor das spätere Kapitel:

14. VPN, Intranet und Extranet

Diffie-Hellman, PFS und Sitzungsschlüssel

Begriff	Bedeutung
Diffie-Hellman	Verfahren zum Schlüsselaustausch
Sitzungsschlüssel	symmetrischer Schlüssel für eine bestimmte Verbindung
PFS	Schutz alter Sitzungen bei späterem Schlüsselverlust
ephemeral	kurzlebig, nur für eine Sitzung
symmetrische Verschlüsselung	verschlüsselt danach die eigentlichen Daten

---

Typische IHK-Fragen

Was ist Diffie-Hellman?

Diffie-Hellman ist ein Verfahren zum Schlüsselaustausch.

Wozu dient Diffie-Hellman?

Es dient dazu, über ein unsicheres Netzwerk ein gemeinsames Geheimnis beziehungsweise Schlüsselmaterial auszuhandeln.

Verschlüsselt Diffie-Hellman große Datenmengen direkt?

Nein. Es dient dem Schlüsselaustausch. Die eigentlichen Daten werden danach meist symmetrisch verschlüsselt.

Was ist Perfect Forward Secrecy?

Perfect Forward Secrecy bedeutet, dass alte Sitzungen auch dann besser geschützt bleiben sollen, wenn ein langfristiger privater Schlüssel später kompromittiert wird.

Warum sind Sitzungsschlüssel wichtig?

Sie schützen eine konkrete Verbindung oder Sitzung und können danach verworfen werden.

Was bedeutet ephemeral?

Ephemeral bedeutet kurzlebig oder nur für eine Sitzung gültig.

Prüfungsfalle: Diffie-Hellman ist nicht dasselbe wie Verschlüsselung der Nutzdaten

Aussage	Richtig oder falsch?
Diffie-Hellman verschlüsselt große Dateien direkt.	falsch
Diffie-Hellman hilft beim Schlüsselaustausch.	richtig
Danach kann symmetrisch verschlüsselt werden.	richtig
PFS schützt alte Sitzungen besser.	richtig
Der öffentliche Schlüssel muss geheim bleiben.	falsch

> **Merksatz:**
> Diffie-Hellman erzeugt oder vereinbart Schlüsselmaterial.
> Die Datenverschlüsselung passiert danach mit einem symmetrischen Verfahren.

Zusammenfassung

Diffie-Hellman ist ein Verfahren zum sicheren Schlüsselaustausch.

Alice und Bob können damit über ein unsicheres Netzwerk ein gemeinsames Geheimnis erzeugen, ohne dieses Geheimnis direkt zu übertragen.

Dieses gemeinsame Geheimnis kann anschließend als Grundlage für einen symmetrischen Sitzungsschlüssel dienen.

Perfect Forward Secrecy sorgt dafür, dass alte Sitzungen besser geschützt bleiben, selbst wenn später ein langfristiger privater Schlüssel kompromittiert wird.

> **IHK-Spickzettel:**
> Diffie-Hellman = Schlüsselaustausch
> nicht direkte Nutzdatenverschlüsselung
> Sitzungsschlüssel = symmetrischer Schlüssel für eine Verbindung
> PFS = schützt alte Sitzungen besser
> ephemeral = kurzlebig / nur für diese Sitzung
> Praxis = HTTPS / TLS / VPN

Revision #4
Created 2 June 2026 23:44:05 by Admin
Updated 3 June 2026 06:18:12 by Admin