Trainer – Verschlüsselung und Sicherheitsgrundlagen

50 Fragen und Antworten zum Ausklappen

Diese Fragen beziehen sich auf die behandelten Themen aus **13. Verschlüsselung und Sicherheitsgrundlagen**:

- symmetrische Verschlüsselung
- asymmetrische Verschlüsselung
- hybride Verschlüsselung
- digitale Signatur
- Hashfunktion
- Zertifikate
- Authentizität, Integrität und Vertraulichkeit
- Diffie-Hellman
- Perfect Forward Secrecy
- Brute Force
- Zufallszahlen
- One-Time-Pad
- Steganographie

---

1. Was bedeutet Verschlüsselung?

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

Aus Klartext wird Geheimtext beziehungsweise Chiffrat.

Beispiel:

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

Erst mit dem passenden Schlüssel kann der ursprüngliche Inhalt wiederhergestellt werden.

2. Was ist Klartext?

Klartext ist die ursprüngliche, lesbare Nachricht.

Beispiel:

Passwort: geheim123

Klartext ist also der Inhalt, bevor er verschlüsselt wurde oder nachdem er wieder entschlüsselt wurde.

3. Was ist Geheimtext oder Chiffrat?

Geheimtext oder Chiffrat ist die verschlüsselte Form einer Nachricht.

Der Inhalt ist ohne passenden Schlüssel nicht sinnvoll lesbar.

Beispiel:

A4$h!7k9%Lz@8mQ

4. Welche drei Sicherheitsziele sind besonders wichtig?

Die drei besonders wichtigen Sicherheitsziele sind:

- Vertraulichkeit
- Integrität
- Authentizität

Merksatz:

Vertraulichkeit = nur Berechtigte können lesen
Integrität = Daten wurden nicht verändert
Authentizität = Identität oder Absender ist echt

5. Was bedeutet Vertraulichkeit?

Vertraulichkeit bedeutet:

Nur berechtigte Personen oder Systeme können den Inhalt lesen.

Beispiele:

- Verschlüsselung
- HTTPS
- VPN

- WPA2 / WPA3
- verschlüsselte Festplatten
- verschlüsselte Backups

6. Was bedeutet Integrität?

Integrität bedeutet:

Daten wurden nicht verändert.

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

Beispiele für Techniken zur Integritätsprüfung:

- Hashfunktion
- digitale Signatur
- Prüfsumme
- Message Authentication Code

7. Was bedeutet Authentizität?

Authentizität bedeutet:

Die Identität ist echt.

Die Leitfrage lautet:

Bist du wirklich derjenige, für den du dich ausgibst?

Beispiele:

- Login mit Benutzername und Passwort
- Zertifikat
- digitale Signatur
- Zwei-Faktor-Authentifizierung
- Shared Secret

8. Was ist symmetrische Verschlüsselung?

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

Alice verschlüsselt mit diesem Schlüssel.
Bob entschlüsselt mit demselben Schlüssel.

Merksatz:

Symmetrisch = gleicher geheimer Schlüssel auf beiden Seiten.

9. Was ist der größte Vorteil symmetrischer Verschlüsselung?

Der größte Vorteil ist die Geschwindigkeit.

Symmetrische Verschlüsselung ist sehr schnell und eignet sich gut für große Datenmengen.

Beispiele:

- Dateien
- Datenströme
- VPN-Datenverkehr
- HTTPS-Nutzdaten
- WLAN-Datenverkehr
- Festplattenverschlüsselung

10. Was ist der größte Nachteil symmetrischer Verschlüsselung?

Der größte Nachteil ist die Schlüsselübergabe.

Alice und Bob brauchen denselben geheimen Schlüssel.

Die wichtige Frage lautet:

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

11. Was passiert, wenn Eve den symmetrischen Schlüssel bekommt?

Wenn Eve den gemeinsamen geheimen Schlüssel besitzt, kann sie die verschlüsselten Nachrichten entschlüsseln.

Dann ist die Sicherheit verloren.

Merksatz:

Der Schlüssel ist das eigentliche Geheimnis.

12. Warum ist symmetrische Verschlüsselung bei vielen Teilnehmern unpraktisch?

Weil viele Teilnehmer viele gemeinsame Schlüssel benötigen.

Bei Alice und Bob reicht ein Schlüssel.

Bei vielen Benutzern müssen aber sehr viele sichere Schlüsselbeziehungen verwaltet werden.

Das skaliert schlecht.

13. Was ist asymmetrische Verschlüsselung?

Bei der asymmetrischen Verschlüsselung gibt es zwei verschiedene Schlüssel:

- öffentlicher Schlüssel
- privater Schlüssel

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

Merksatz:

Asymmetrisch = öffentlicher + privater Schlüssel.

14. Wer erzeugt bei asymmetrischer Verschlüsselung das Schlüsselpaar?

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

Beispiel:

Bob möchte geheime Nachrichten empfangen.
Also erzeugt Bob einen öffentlichen und einen privaten Schlüssel.

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

Alice nutzt Bobs öffentlichen Schlüssel.

Nur Bob kann die Nachricht anschließend mit seinem privaten Schlüssel entschlüsseln.

Merksatz:

Geheim an Bob senden = Bobs öffentlichen Schlüssel verwenden.

16. Welchen Schlüssel nutzt Bob zum Entschlüsseln?

Bob nutzt seinen privaten Schlüssel.

Der private Schlüssel darf nicht weitergegeben werden.

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

17. Warum darf der öffentliche Schlüssel öffentlich sein?

Der öffentliche Schlüssel ist dafür gedacht, verteilt zu werden.

Auch Eve darf ihn sehen.

Mit dem öffentlichen Schlüssel allein kann Eve aber nicht entschlüsseln.

Geheim bleiben muss der private Schlüssel.

18. Was ist der Vorteil asymmetrischer Verschlüsselung?

Der Vorteil ist, dass kein gemeinsamer geheimer Schlüssel vorher sicher übertragen werden muss.

Der öffentliche Schlüssel darf offen verteilt werden.

Dadurch hilft asymmetrische Verschlüsselung beim Problem der Schlüsselübergabe.

19. Was ist der Nachteil asymmetrischer Verschlüsselung?

Asymmetrische Verschlüsselung ist langsamer und rechenaufwendiger als symmetrische Verschlüsselung.

Deshalb verschlüsselt man große Datenmengen in der Praxis meistens nicht komplett asymmetrisch.

20. Was ist hybride Verschlüsselung?

Hybride Verschlüsselung kombiniert asymmetrische und symmetrische Verschlüsselung.

Asymmetrisch wird für den sicheren Schlüsselaustausch genutzt.
Symmetrisch wird für die schnelle Verschlüsselung der Nutzdaten genutzt.

Merksatz:

Hybrid = asymmetrisch für den Schlüssel, symmetrisch für die Daten.

21. Warum nutzt man hybride Verschlüsselung?

Man nutzt hybride Verschlüsselung, weil beide Verfahren unterschiedliche Vorteile haben.

Symmetrisch:

- schnell
- gut für große Datenmengen
- Problem: Schlüsselübergabe

Asymmetrisch:

- löst Schlüsselübergabe
- aber langsamer

Hybrid kombiniert beide Vorteile.

22. Was wird bei hybrider Verschlüsselung asymmetrisch verschlüsselt?

Der symmetrische Sitzungsschlüssel wird asymmetrisch geschützt oder übertragen.

Die eigentlichen Nutzdaten werden danach symmetrisch verschlüsselt.

23. Was wird bei hybrider Verschlüsselung symmetrisch verschlüsselt?

Die eigentlichen Nutzdaten werden symmetrisch verschlüsselt.

Beispiele:

- Dateien

- Webseiteninhalte
- VPN-Daten
- Login-Daten innerhalb einer sicheren Verbindung

24. Was ist ein Sitzungsschlüssel?

Ein Sitzungsschlüssel ist ein symmetrischer Schlüssel für eine bestimmte Verbindung oder Sitzung.

Er sollte:

- zufällig erzeugt werden
- nur für diese Sitzung gelten
- geheim bleiben
- nach der Nutzung verworfen werden

25. Wo wird hybride Verschlüsselung praktisch genutzt?

Hybride Verschlüsselung wird zum Beispiel genutzt bei:

- HTTPS
- TLS
- VPN
- sicherer Datenübertragung im Internet
- sicherer E-Mail-Kommunikation

26. Was ist eine digitale Signatur?

Eine digitale Signatur ist ein Verfahren, mit dem geprüft werden kann:

- ob der Absender echt ist
- ob die Daten unverändert sind

Eine digitale Signatur dient hauptsächlich Authentizität und Integrität.

27. Bietet eine digitale Signatur automatisch Vertraulichkeit?

Nein.

Eine digitale Signatur macht den Inhalt nicht automatisch geheim.

Sie prüft vor allem:

- Absender-Echtheit
- Unveränderheit der Daten

Für Vertraulichkeit braucht man Verschlüsselung.

28. Welchen Schlüssel nutzt der Absender zum Signieren?

Der Absender nutzt seinen privaten Schlüssel.

Beispiel:

Bob signiert mit Bobs privatem Schlüssel.

29. Welchen Schlüssel nutzt der Empfänger zum Prüfen einer Signatur?

Der Empfänger nutzt den öffentlichen Schlüssel des Absenders.

Beispiel:

Alice prüft Bobs Signatur mit Bobs öffentlichem Schlüssel.

30. Was ist der Unterschied zwischen Verschlüsselung und Signatur?

Verschlüsselung schützt den Inhalt vor Mitlesen.

Digitale Signatur prüft Absender und Unveränderheit.

Vergleich:

Verschlüsselung = Vertraulichkeit
Signatur = Authentizität + Integrität

31. Was ist eine Hashfunktion?

Eine Hashfunktion erzeugt aus Daten einen Prüfwert fester Länge.

Dieser Prüfwert heißt Hash oder Hashwert.

Ein Hash ist wie ein digitaler Fingerabdruck von Daten.

32. Ist ein Hash eine Verschlüsselung?

Nein.

Ein Hash ist keine Verschlüsselung.

Ein Hash wird normalerweise nicht entschlüsselt.

Stattdessen berechnet man den Hash neu und vergleicht ihn mit einem bekannten Hashwert.

33. Wozu dient ein Hash?

Ein Hash dient vor allem zur Integritätsprüfung.

Man kann damit erkennen, ob Daten verändert wurden.

Beispiele:

- Datei prüfen
- Download prüfen
- Nachricht prüfen
- Grundlage für digitale Signaturen

34. Was passiert mit dem Hash, wenn sich eine Datei leicht ändert?

Schon eine kleine Änderung an der Datei verändert den Hashwert stark.

Beispiel:

Hallo → a1b2c3d4...
Halla → 9f8e7d6c...

Merksatz:

Kleine Änderung an den Daten = großer Unterschied beim Hash.

35. Was ist ein Zertifikat?

Ein Zertifikat ist ein digitaler Nachweis.

Es verbindet eine Identität mit einem öffentlichen Schlüssel.

Beispiel:

Ein Zertifikat kann bestätigen, dass ein öffentlicher Schlüssel wirklich zu www.beispiel.de gehört.

36. Wozu braucht man Zertifikate?

Zertifikate helfen dabei, die Identität zu prüfen.

Sie beantworten zum Beispiel die Frage:

Gehört dieser öffentliche Schlüssel wirklich zu dieser Webseite oder Person?

Typische Nutzung:

- HTTPS
- TLS
- VPN
- digitale Signaturen
- sichere Serveridentifikation

37. Welches Sicherheitsziel passt besonders zu Zertifikaten?

Zertifikate gehören besonders zur Authentizität.

Sie helfen zu prüfen, ob eine Identität echt ist.

Merksatz:

Zertifikat = Identität + öffentlicher Schlüssel.

38. Was ist Diffie-Hellman?

Diffie-Hellman ist ein Verfahren zum Schlüsselaustausch.

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

39. Verschlüsselt Diffie-Hellman direkt große Datenmengen?

Nein.

Diffie-Hellman dient dem Schlüsselaustausch.

Die eigentlichen Daten werden danach meistens symmetrisch verschlüsselt.

Merksatz:

Diffie-Hellman = Schlüsselaustausch, nicht Nutzdatenverschlüsselung.

40. Was sieht Eve bei Diffie-Hellman?

Eve kann öffentliche Austauschwerte sehen.

Eve sieht aber nicht:

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

Dadurch kann Eve den gemeinsamen Schlüssel nicht einfach berechnen.

41. Was bedeutet Perfect Forward Secrecy?

Perfect Forward Secrecy bedeutet:

Alte Sitzungen sollen besser geschützt bleiben, auch wenn später ein langfristiger privater Schlüssel kompromittiert wird.

Merksatz:

PFS schützt alte Sitzungen besser.

42. Was bedeutet ephemeral?

Ephemeral bedeutet kurzlebig.

Im Zusammenhang mit Kryptografie bedeutet es:

Schlüsselmaterial wird nur für eine bestimmte Sitzung genutzt und danach verworfen.

Das hilft bei Perfect Forward Secrecy.

43. Was ist Brute Force?

Brute Force bedeutet:

Ein Angreifer probiert systematisch viele Möglichkeiten aus, bis etwas passt.

Beispiele:

- Passwörter ausprobieren
- PINs ausprobieren
- Schlüssel ausprobieren
- Hashes testen

Merksatz:

Brute Force = ausprobieren, bis es passt.

44. Was schützt gegen Brute Force?

Gegen Brute Force helfen:

- lange Passwörter
- zufällige Passwörter
- Passwortmanager
- Multi-Faktor-Authentifizierung
- Rate Limiting
- Account-Sperren
- starke Schlüssel
- moderne Algorithmen

45. Warum sind Zufallszahlen in der Kryptografie wichtig?

Zufallszahlen sind wichtig, weil Schlüssel nicht vorhersehbar sein dürfen.

Wenn ein Schlüssel aus schlechtem Zufall entsteht, kann er leichter erraten oder berechnet werden.

Merksatz:

Starker Algorithmus + schlechter Zufall = unsicheres System.

46. Was ist ein One-Time-Pad?

Das One-Time-Pad ist ein besonderer Fall der Verschlüsselung.

Es gilt theoretisch als nicht knackbar, wenn alle Bedingungen erfüllt sind.

47. Welche Bedingungen braucht ein sicheres One-Time-Pad?

Ein sicheres One-Time-Pad braucht:

- Schlüssel ist wirklich zufällig
- Schlüssel ist mindestens so lang wie die Nachricht
- Schlüssel wird nur einmal verwendet
- Schlüssel bleibt geheim
- Schlüssel wird sicher übertragen

Wenn eine Bedingung verletzt wird, ist die besondere Sicherheit nicht mehr gegeben.

48. Warum ist One-Time-Pad praktisch schwierig?

Das größte Problem ist die Schlüsselverteilung.

Der Schlüssel muss mindestens so lang wie die Nachricht sein und vorher sicher an den Empfänger übertragen werden.

Das ist in der Praxis oft unpraktisch.

49. Was ist Steganographie?

Steganographie bedeutet:

Informationen werden in unauffälligen Daten versteckt.

Das Ziel ist, zu verbergen, dass überhaupt eine geheime Nachricht existiert.

Beispiel:

Eine Nachricht wird in einem Bild versteckt.

50. Was ist der Unterschied zwischen Verschlüsselung und Steganographie?

Verschlüsselung macht den Inhalt unlesbar.

Steganographie versteckt die Existenz der Nachricht.

Beste Kombination:

Erst verschlüsseln, dann verstecken.

Dann ist der Inhalt geschützt und zusätzlich unauffälliger.

Abschluss-Spickzettel

Thema	Kurzantwort
symmetrisch	gleicher geheimer Schlüssel
asymmetrisch	öffentlicher + privater Schlüssel
hybrid	asymmetrisch für Schlüssel, symmetrisch für Daten
Signatur	Authentizität + Integrität
Hash	Integrität prüfen
Zertifikat	Identität + öffentlicher Schlüssel
Diffie-Hellman	Schlüsselaustausch
PFS	alte Sitzungen besser geschützt
Brute Force	systematisches Ausprobieren
Zufallszahlen	wichtig für sichere Schlüssel
One-Time-Pad	theoretisch sicher bei perfekten Bedingungen
Steganographie	Nachricht verstecken
Vertraulichkeit	nur Berechtigte können lesen
Integrität	Daten unverändert
Authentizität	Identität echt

Revision #1
Created 3 June 2026 06:08:25 by Admin
Updated 3 June 2026 06:18:12 by Admin