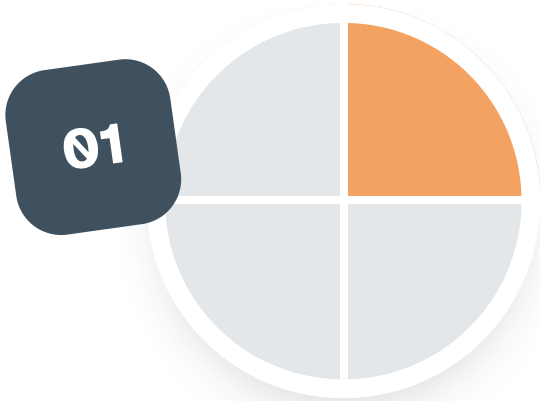
DYS+ Campus



Übungsheft · Informatik · Klasse 9

Datensicherheit und Verschlüsselung

Erklärungen, 44 Aufgaben in drei Stufen und alle Lösungen, viele mit Begründung.

Name _____ **Datum** _____

Das lernst du

- Ich ordne Fälle den Schutzzielen zu und nenne Maßnahmen.
- Ich verschlüssele und entschlüssele mit dem Caesar-Verfahren und erkläre Public Key.
- Ich beurteile Verfahren nach ihrer Sicherheit.

So arbeitest du mit dem Heft

●○○ **Basis** zum Einstieg

●●○ **Standard** zum Üben

●●● **Plus** zum Weiterdenken

Du musst nicht alles machen. Fang bei Basis an. Die Lösungen stehen hinten im Heft.

Noch unsicher?

Scanne den Code. Dort wird das Thema Schritt für Schritt erklärt.

dysplus.de/lernen/realschule/klasse-9/informatik/datensicherheit-verschluesselung/vertraulichkeit-integritaet-verfuegbarkeit

Kurz erklärt

Drei Schutzziele

Ziel	Frage	Maßnahme
Vertraulichkeit	Wer darf lesen?	Passwort, Verschlüsselung
Integrität	Ist es unverändert?	Schreibrechte
Verfügbarkeit	Ist es da?	Sicherungskopie

Caesar mit Schlüssel 3

1. H → K, A → D, L → O, L → O, O → R.
2. HALLO wird KDOOR.
3. Zum Entschlüsseln schiebt man 3 zurück.

Zahl der Schlüssel in einer Gruppe

1. 6 Personen, jedes Paar braucht einen Schlüssel.
2. $6 \cdot 5 : 2 = 15$.
3. Es sind 15 Schlüssel.

Merksatz: Symmetrisch: ein Schlüssel für beide. Public Key: öffentlich verschlüsselt, privat entschlüsselt.

Typischer Fehler: Der öffentliche Schlüssel entschlüsselt nicht. Entschlüsseln kann nur der private Schlüssel.

Tipp: Passwörter und private Schlüssel gibst du nie weiter. Nutze lange Passwörter, Zwei-Faktor-Anmeldung und Sicherungskopien.

●○○ Basis

Schutzziele und Sicherung

1 Welches Ziel ist verletzt? Kreuze an.

a) Fremde lesen eine private Nachricht: ☐ **Vertraulichkeit** ☐ **Verfügbarkeit**

_____

b) Eine Zahl in einer Tabelle wird heimlich geändert: ☐ **Integrität** ☐ **Vertraulichkeit**

_____

c) Der Server ist einen Tag lang nicht erreichbar: ☐ **Integrität** ☐ **Verfügbarkeit**

_____

d) Ein Stick ist kaputt, die Fotos sind weg: ☐ **Vertraulichkeit** ☐ **Verfügbarkeit**

_____

2 Ergänze.

a) Die drei Schutzziele sind Vertraulichkeit, Integrität und _____.

b) Bei der 3-2-1-Regel gibt es _____ Kopien.

c) Bei der 3-2-1-Regel gibt es _____ Speicherarten.

d) Bei der 3-2-1-Regel liegt _____ Kopie an einem anderen Ort.

3 Stimmt der Satz? Schreibe falsche Sätze richtig auf.

a) Ein Passwort schützt vor allem die Vertraulichkeit. ☐ **stimmt** ☐ **stimmt nicht**

b) Eine Sicherungskopie auf demselben Gerät schützt vor einem Geräteausfall. ☐ **stimmt** ☐ **stimmt nicht**

c) Man sollte testen, ob man eine Sicherung zurückspielen kann. ☐ **stimmt** ☐ **stimmt nicht**

d) Passwörter gibt man gern an Freunde weiter. ☐ **stimmt** ☐ **stimmt nicht**

4 Rechne.

a) 40 GB pro Sicherung, 1000 GB frei: _____ Sicherungen

b) Original und 2 Sicherungen: _____ Kopien

c) 4 Fälle, in 2 davon ist die Vertraulichkeit verletzt. Andere Fälle: _____

d) Zahl der Schutzziele: _____

●●○ Standard

Verschlüsseln

5 **Verschlüssele mit Schlüssel 3 (Caesar). Trage die Buchstaben ein.**

a) A wird _____

b) B wird _____

c) Z wird _____

d) HALLO wird _____

6 **Entschlüssele mit Schlüssel 4.**

a) W wird _____

b) G wird _____

c) WGLYPI wird _____

d) E wird _____

7 **Symmetrisch oder Public Key? Kreuze an.**

a) Ein Schlüssel für beide Seiten: _____ ☐ **Public Key** ☐ **symmetrisch**

b) Öffentlicher und privater Schlüssel: _____ ☐ **Public Key** ☐ **symmetrisch**

c) Der Schlüssel muss vorher geheim übertragen werden: _____ ☐ **Public Key** ☐ **symmetrisch**

d) Jeder darf den Schlüssel zum Verschlüsseln kennen: _____ ☐ **symmetrisch** ☐ **Public Key**

8 Zahl der Schlüssel in einer Gruppe (symmetrisch).

a) 3 Personen: _____ Schlüssel

b) 5 Personen: _____ Schlüssel

c) 6 Personen: _____ Schlüssel

d) 10 Personen: _____ Schlüssel

●●● Plus

Public Key und Urteil

9 **Public-Key-Beispiel mit n = 33 und e = 3. Nimm den Rest bei Division durch 33.**

a) Klartext 2: 2^3 = _____

b) Geheimtext für Klartext 2: _____

c) Klartext 5: 5^3 = _____

d) Geheimtext für Klartext 5: _____

10 **Erkläre.**

a) Wozu dient der öffentliche Schlüssel, wozu der private?

b) Warum löst Public Key das Problem des Schlüsselaustauschs?

c) Wie viele Schlüsselpaare brauchen 10 Personen bei Public Key? Warum?

11 Beurteile Verfahren.

a) Warum ist das Caesar-Verfahren unsicher?

b) Ein Schlüsselwort hat 3 Buchstaben. Wie viele Möglichkeiten gibt es?

c) Was muss bei einem guten Verfahren geheim bleiben, was darf bekannt sein?

12 Sicherheitstipps.

a) Nenne drei Regeln für sicheres Verhalten mit Daten.

b) Was kannst du tun, wenn du Hilfe bei Datenproblemen brauchst?

Kannst du das schon?

Kreuze an, wie sicher du dich fühlst. Hier gibt es kein Richtig oder Falsch.

Ich kann …	sicher	fast	noch nicht
Ich ordne Fälle den Schutzzielen zu und nenne Maßnahmen.	☐	☐	☐
Ich verschlüssele und entschlüssele mit dem Caesar-Verfahren und erkläre Public Key.	☐	☐	☐
Ich beurteile Verfahren nach ihrer Sicherheit.	☐	☐	☐

Tipp: Bei „noch nicht“ schau dir „Kurz erklärt“ vorne im Heft noch einmal an oder scanne den Code auf dem Deckblatt. Dann probierst du die Aufgaben noch einmal.

Lösungen

Erst selbst lösen, dann vergleichen. Bei vielen Aufgaben steht die Begründung dabei.

●○○ Basis: Schutzziele und Sicherung

1 Welches Ziel ist verletzt? Kreuze an.

a) Vertraulichkeit

→ Eine unberechtigte Person hat gelesen.

b) Integrität

→ Die Daten sind nicht mehr unverändert.

c) Verfügbarkeit

→ Die Daten sind nicht zugänglich.

d) Verfügbarkeit

→ Die Daten sind nicht mehr da.

2 Ergänze.

a) Die drei Schutzziele sind Vertraulichkeit, Integrität und **Verfügbarkeit.**

b) Bei der 3-2-1-Regel gibt es **3** Kopien.

c) Bei der 3-2-1-Regel gibt es **2** Speicherarten.

d) Bei der 3-2-1-Regel liegt **1** Kopie an einem anderen Ort.

3 Stimmt der Satz? Schreibe falsche Sätze richtig auf.

a) Stimmt.

b) Stimmt nicht. Richtig: Fällt das Gerät aus, sind Original und Kopie weg. Die Kopie gehört auf ein anderes Gerät.

c) Stimmt.

d) Stimmt nicht. Richtig: Passwörter gibt man nie weiter.

4 Rechne.

a) 40 GB pro Sicherung, 1000 GB frei: 25 Sicherungen

b) Original und 2 Sicherungen: 3 Kopien

c) 4 Fälle, in 2 davon ist die Vertraulichkeit verletzt. Andere Fälle: 2

d) Zahl der Schutzziele: 3

●●○ Standard: Verschlüsseln

5 **Verschlüssele mit Schlüssel 3 (Caesar). Trage die Buchstaben ein.**

a) **A wird D**

b) **B wird E**

c) **Z wird C**

d) **HALLO wird KDOOR**

6 **Entschlüssele mit Schlüssel 4.**

a) **W wird S**

b) **G wird C**

c) **WGLYPI wird SCHULE**

d) **E wird A**

7 **Symmetrisch oder Public Key? Kreuze an.**

a) **symmetrisch**

→ Sender und Empfänger nutzen denselben Schlüssel.

b) **Public Key**

→ Es gibt zwei Schlüssel.

c) **symmetrisch**

→ Das ist das Problem des Schlüsselaustauschs.

d) **Public Key**

→ Der öffentliche Schlüssel darf bekannt sein.

8 **Zahl der Schlüssel in einer Gruppe (symmetrisch).**

a) **3 Personen: 3 Schlüssel**

b) **5 Personen: 10 Schlüssel**

c) **6 Personen: 15 Schlüssel**

d) **10 Personen: 45 Schlüssel**

●●● Plus: Public Key und Urteil

9 **Public-Key-Beispiel mit n = 33 und e = 3. Nimm den Rest bei Division durch 33.**

a) **Klartext 2: $2^3 = 8$**

b) **Geheimtext für Klartext 2: 8**

c) **Klartext 5: $5^3 = 125$**

d) **Geheimtext für Klartext 5: 26**

10 **Erkläre.**

a) **Der öffentliche verschlüsselt, der private entschlüsselt.**

→ Denke an Schloss und Schlüssel.

b) **Der öffentliche Schlüssel darf offen weitergegeben werden. Es muss kein Geheimnis übertragen werden.**

→ Was muss geheim bleiben?

c) **10 Paare, denn jede Person hat ein eigenes Paar.**

→ Jede Person hat ein Paar.

11 Beurteile Verfahren.

a) Es gibt nur 25 Schlüssel, die man alle ausprobieren kann, und Buchstabenmuster bleiben sichtbar.

→ Denke an Schlüsselzahl und Muster.

b) 26 · 26 · 26 = 17 576 Möglichkeiten.

→ 26 Möglichkeiten je Buchstabe.

c) Geheim bleibt nur der Schlüssel. Das Verfahren darf bekannt sein.

→ Sicherheit hängt vom Schlüssel ab.

12 Sicherheitstipps.

a) z. B. lange Passwörter, Zwei-Faktor-Anmeldung, Sicherungskopien, nichts weitergeben.

→ Denke an Passwort, Anmeldung und Sicherung.

b) Mit einem Erwachsenen sprechen, dem du vertraust, und bei Verdacht auf Missbrauch sofort das Passwort ändern.

→ Du bist nicht allein.