

### 1. Quiz: Kreuze jeweils alle richtigen Antworten an.

a) „Microsoft“ ist ...

☐

ein Betriebssystem

☒

ein Softwarehersteller

☐

ein Computer

☒

eine Firma

b) Die Datei „normalform.ggb“ mit einer Dateigröße von 1418 Bytes belegt auf einem Datenträger 4 KB. Woran liegt das?

☒

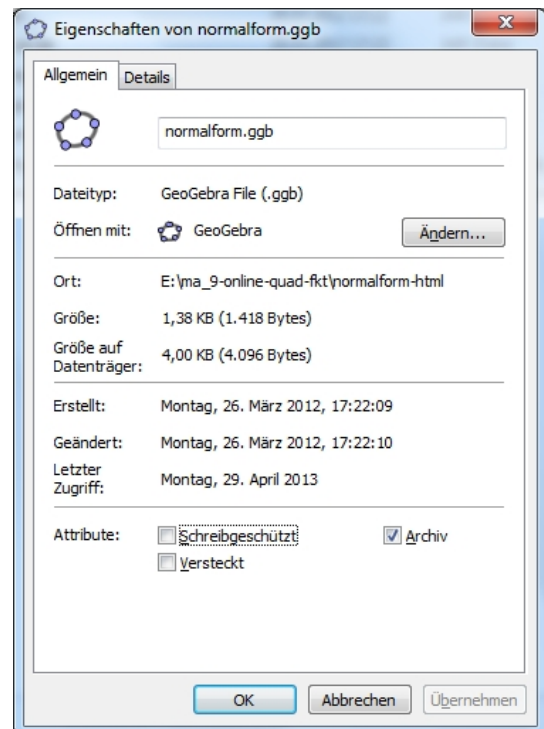
Der Datenträger hat eine Clustergröße von 4KB

☐

Die Dateigröße ist falsch angegeben

☐

Die Datei verbraucht wegen gesetztem Archiv-Bit mehr Speicherplatz



c) Welches Gerät befindet sich in dieser „black-box“?

☐

Monitor

☒

Switch

☐

Lautsprecher

☐

Scanner



d) Um sein Smartphone in das heimische WLAN einzubinden, soll Eric die MAC-Adresse in den Router eintragen. Bei welcher Angabe handelt es sich eine MAC-Adresse?

☒

00:80:41:ae:fd:7e

☐

192.168.1.25

☐

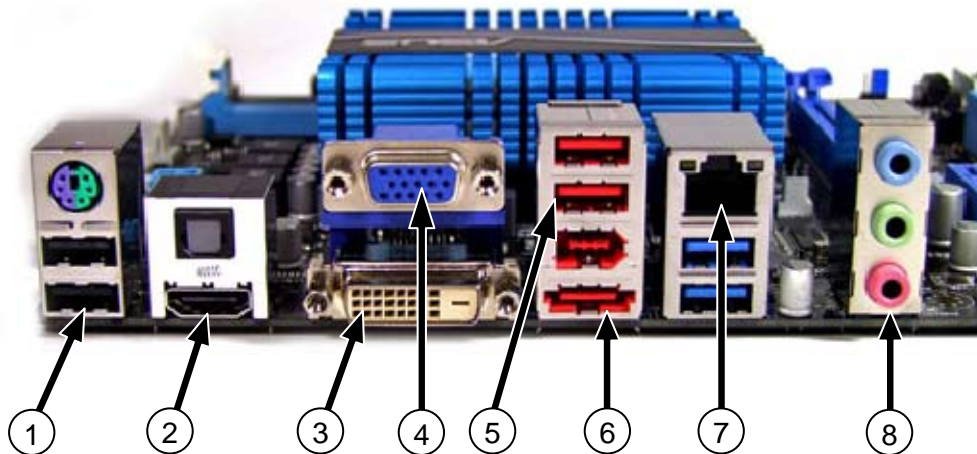
1920x1080

☐

iPhone0815S

**LÖSUNGEN:** Je richtig gelöster Aufgabe ein Punkt → 4 Punkte

## 2. Schnittstellen / Hardware



Bildquelle: [http://www.system68.com/computer/images/lian\\_li\\_v351\\_03.jpg](http://www.system68.com/computer/images/lian_li_v351_03.jpg) (©Stephan Bauer)

Ordne die Begriffe den Anschlüssen am Mainboard zu!  
(USB – DVI – VGA – LAN – HDMI – USB – SATA – Audio)

1	2	3	4	5	6	7	8
USB	HDMI	DVI	VGA	USB	SATA	LAN	Audio

**LÖSUNG:** je richtige Lösung 0,5 Punkte → 4 Punkte

## 3. Verschlüsselung

Zur Geheimhaltung der Kommunikation werden Informationen schon seit langer Zeit verschlüsselt. Das Cäsar-Verfahren ist eine klassische Substitutionsmethode.

Hier im Beispiel lautet der Schlüssel „D“.

Das heißt, beim Verschlüsseln schreibt man an Stelle des A in der Geheimschrift das D, statt B das E usw.

Klartextalphabet :    ABCDEFGHIJKLMNOPQRSTUVWXYZ  
Geheimtextalphabet:    DEFGHIJKLMNOPQRSTUVWXYZABC

a) Entschlüssele den Geheimtext    Kdoor gx Lqirupdwlnhu  
    Hallo du Informatiker

b) Man kann auch durch Transposition verschlüsseln. Alle Klartextzeichen erscheinen dabei lediglich in einer anderen Reihenfolge als Geheimtext.

Ein Beispiel ist die Zickzackschrift. Der Klartext wird dabei in der Mitte getrennt und untereinander geschrieben. Der Geheimtext ergibt sich dann aus dem „Zick-Zack“.

Bsp.: aus dem Klartext „GutenMorgen“ wird über

GutenM                    im Zick-Zack der Geheimtext „GourtgeennM“  
orgen

Verschlüssele nach diesem Prinzip das Wort „Informatik“

Infor                    Imnaftoirk  
matik

Modernere symmetrische Verfahren nutzen ein möglichst sicheres Passwort als Schlüssel. Ein vierstelliges Zahlenschloss (4 Ringe mit den Ziffern 0 bis 9) hat demzufolge ein „Passwort“ aus 4 Zeichen (Zeichenvorrat 10 Zeichen). Es gibt also  $10 \cdot 10 \cdot 10 \cdot 10 = 10^4 = 10000$  Möglichkeiten

- c) Wie viele Möglichkeiten hätte ein analog aufgebautes Zahlenschloss mit 8 Stellen?

---

$$10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 10^8 \text{ oder } 100\,000\,000 \text{ Möglichkeiten}$$

---

- d) Wie viele Möglichkeiten gibt es für ein sechstelliges Passwort aus den 26 Kleinbuchstaben? (Gib nur die Potenzschreibweise an)

---

$$26^6 \text{ Möglichkeiten}$$

---

- e) Man nutzt für seinen WLAN-Schlüssel Klein- und Großbuchstaben sowie die 10 Ziffern. Welche Potenz ergibt sich für die Anzahl der Möglichkeiten bei einem 40stelligen Passwort?

---

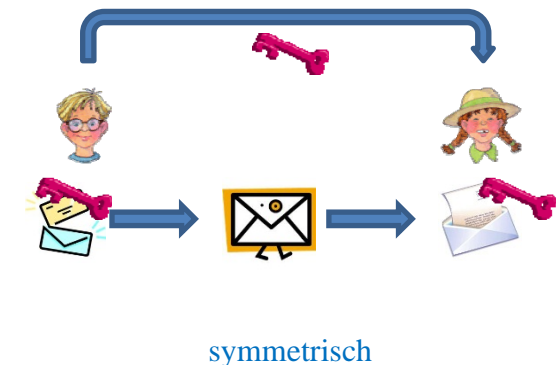
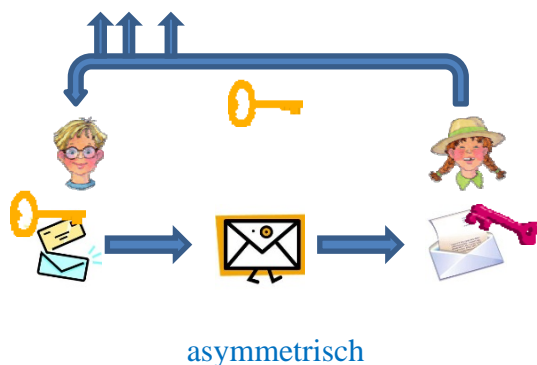
$$62^{40} \text{ Möglichkeiten}$$

---

Bei den genannten (symmetrischen) Verfahren besteht das Problem der sicheren Schlüsselübertragung. Hat ein Angreifer den Schlüssel abgefangen, kann er mitlesen.

Daher wurden asymmetrische Verfahren entwickelt, bei der der Empfänger E der Nachricht sich selbst zwei zusammenhängende Schlüssel erzeugt, einen geheimen (private key) und einen öffentlichen (public key). Jeder, der ihm eine Nachricht schicken möchte, nimmt sich den öffentlichen Schlüssel von E und verschlüsselt damit die Nachricht. Den Geheimtext schickt er an E. Empfänger E kann die Nachricht nur mit seinem privaten Schlüssel entschlüsseln. Da dieser Schlüssel nie übertragen werden muss, kann ihn ein Angreifer auch nicht abfangen.

- f) Ordne den Darstellungen die Begriffe *symmetrische* und *asymmetrische* Verschlüsselung zu.

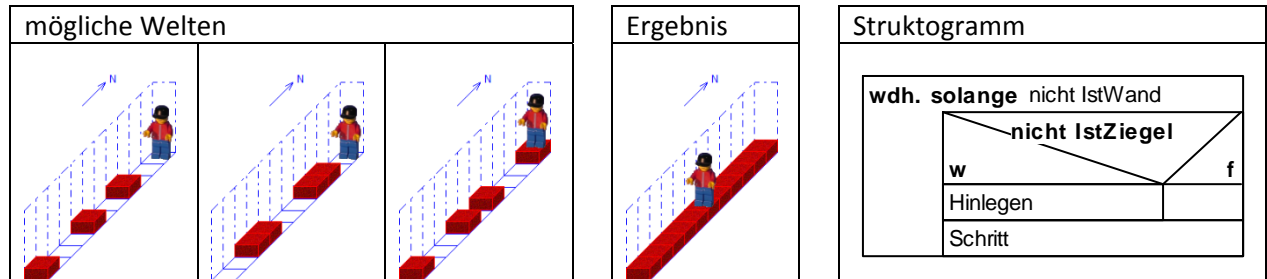


a) bis f) je Lösung ein Punkt → 6 Punkte

#### 4. Algorithmieren - Weg auslegen

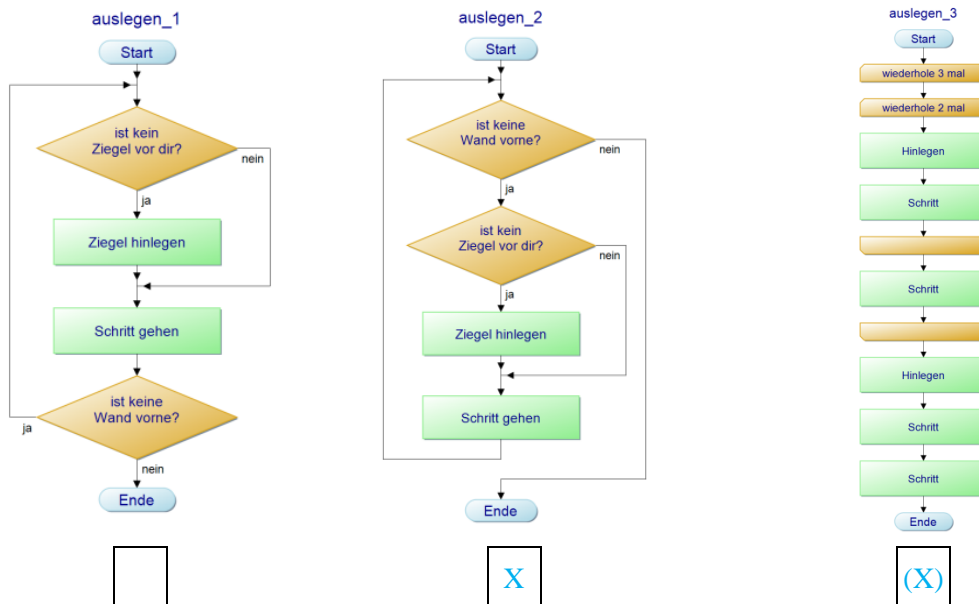
Roboter Karol kann Ziegel vor sich Hinlegen. Er nimmt seine Welt mit Sensoren wahr. Er kann zum Beispiel sehen, ob das Feld vor ihm leer ist oder ob er vor einer Wand steht. Natürlich kann er sich auch um 90 Grad nach links drehen

Die abgebildeten Welten sollen vollständig mit Ziegeln ausgelegt werden (siehe Ergebnis). Dabei ist es egal, wo der Roboter am Ende steht.



Mit dem Struktogramm ist ein Programm gegeben.

- a) Entscheide, welcher der gegebenen Programmlaufpläne dem Ergebnis des Programms entspricht.



wenn auslegen\_2 → 2 Punkte

wenn auslegen\_3 (füllt NUR die erste Welt vollständig aus – nicht allgemeingültig) → 1 Punkt

- b) Das im Struktogramm gegebene Programm enthält einen Fehler. Notiere diesen hier.

das erste Feld wird nicht mit einem Ziegel belegt, es bleibt frei

→ 1 Punkt

- c) Verbessere den Fehler. Zeichne ein entsprechendes Struktogramm oder einen Programmlaufplan

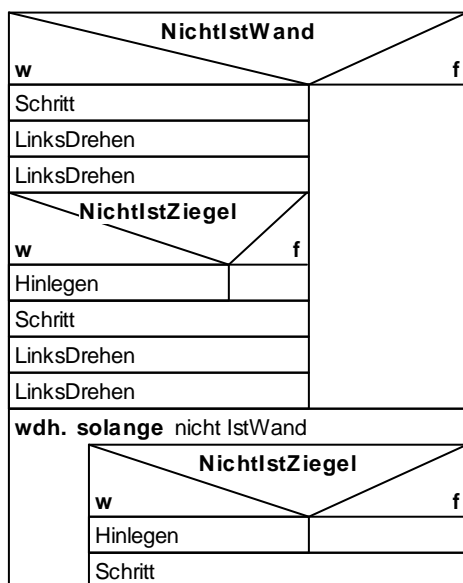
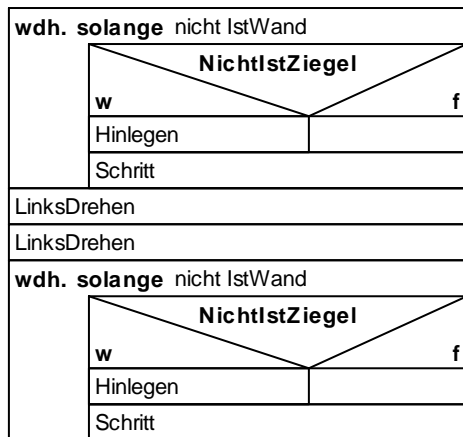
geg. Struktogramm oder PAP verwendet → 1

Lücke gefüllt (gleich zu Beginn, oder auf Rückweg) → 1

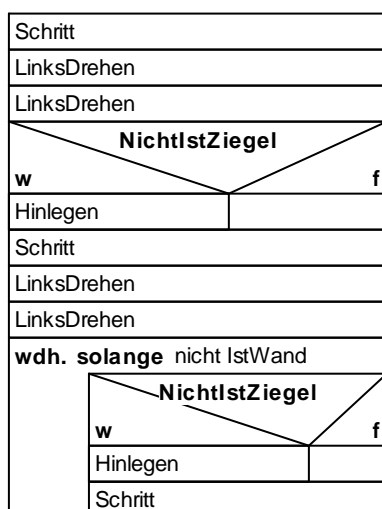
Saubere/ordentliche Darstellung → 1

insgesamt 3 Punkte

## mögliche Lösungen:



## Bei Annahme Welt >1:



usw.