

Informatik ⁹/₁₀



9/10 Informatik

Bearbeitet von
Andre Asschoff
Christian Bader
Carsten Dittich
Christian Pothmann

Informatik

Nordrhein-Westfalen

Informatik 9/10

Bearbeitet von André Aschoff, Christian Bader, Carsten Dittich und Christian Pothmann

Zu diesem Lehrwerk sind erhältlich:

► Digitales Lehrmaterial **click & teach** Einzellizenz, Bestell-Nr. 380431

Weitere Materialien finden Sie unter www.ccbuchner.de.

Dieser Titel ist auch als digitale Ausgabe **click & study** unter www.ccbuchner.de erhältlich.

Bitte beachten: An keiner Stelle im Schülerbuch dürfen Eintragungen vorgenommen werden.
Das gilt besonders für die Leerstellen in Aufgaben und Tabellen.

1. Auflage, 1. Druck 2024

Alle Drucke dieser Auflage sind, weil untereinander unverändert, nebeneinander benutzbar.

Dieses Werk folgt der reformierten Rechtschreibung und Zeichensetzung. Ausnahmen bilden Texte, bei denen künstlerische, philologische oder lizenzrechtliche Gründe einer Änderung entgegenstehen.

Die QR- und Mediacodes enthalten zusätzliche Unterrichtsmaterialien, die der Verlag in eigener Verantwortung zur Verfügung stellt. Auf verschiedenen Seiten dieses Buches finden sich Verweise (Links) auf Internetadressen. Haftungshinweis: Trotz sorgfältiger inhaltlicher Kontrolle wird die Haftung für die Inhalte externer Seiten ausgeschlossen.

© 2024, C.C.Buchner Verlag, Bamberg

Das Werk und seine Teile sind urheberrechtlich geschützt. Jede Nutzung in anderen als den gesetzlich zugelassenen Fällen bedarf der vorherigen schriftlichen Einwilligung des Verlags. Hinweis zu §§ 60a, 60b UrhG: Weder das Werk noch seine Teile dürfen ohne eine solche Einwilligung eingescannt und/oder in ein Netzwerk eingestellt werden. Dies gilt auch für Intranets von Schulen und sonstigen Bildungseinrichtungen. Fotomechanische, digitale oder andere Wiedergabeverfahren sowie jede öffentliche Vorführung, Sendung oder sonstige gewerbliche Nutzung oder deren Duldung sowie Vervielfältigung (z. B. Kopie, Download oder Streaming), Verleih und Vermietung nur mit ausdrücklicher Genehmigung des Verlags.

Layout und Satz: tiff.any GmbH & Co. KG, Berlin

Umschlag: Wildner + Designer GmbH, Fürth

Druck und Bindung:

www.ccbuchner.de

ISBN 978-3-661-38043-8

1	HTML und CSS	7
1.1	HTML: Die Sprache des Webs	8
1.2	HTML-Code strukturieren	10
1.3	Listen und Zeichencodierung	12
1.4	Bilder einbinden	14
1.5	Bildgrößen	16
1.6	Links im World Wide Web	18
1.7	Navigation	20
1.8	Vertiefung: Webseiten mit CSS gestalten	22
1.9	Projekt: Eigene Website erstellen	24
1.10	Das World Wide Web	28
1.11	Üben und Vertiefen	30
1.12	Am Ziel	33
1.13	Alles im Blick	34
2	Verschlüsselungsmethoden	35
2.1	Bedrohung für die Sicherheit durch Hacking	36
2.2	Kryptographie	38
2.3	Projekt: Einfache Geheimschriften	40
2.4	Kryptoanalyse	42
2.5	Polyalphabetische Substitution	44
2.6	Der Kasiski-Test	46
2.7	Die Enigma	48
2.8	Computergestützte Verschlüsselung	50
2.9	Üben und Vertiefen	52
2.10	Am Ziel	55
2.11	Alles im Blick	56

3	Algorithmen	57
3.1	Algorithmen	58
3.2	Darstellung von Algorithmen	60
3.3	Textbasiertes Programmieren	62
3.4	Bibliotheken	64
3.5	Schleifen in Python	66
3.6	Variablen in Python	68
3.7	Variablen und Parameter in Python	70
3.8	Verzweigungen	72
3.9	Üben und Vertiefen	74
3.10	Am Ziel	77
3.11	Alles im Blick	78
4	Projektkapitel – Calliope und Calli:Bot	79
4.1	Einführung Calliope	80
4.2	TigerJython und Calliope	82
4.3	Projekte für den Calliope	84
4.4	Der Calli:bot	86
4.5	Die Mars-Mission	88
5	Automaten	89
5.1	Rückblick Automaten	90
5.2	Zustände und Zustandsübergänge	92
5.3	Zustandsdiagramme und Tabellen	94
5.4	Erstellen von Automaten mit Flaci I	96
5.5	Erstellen von Automaten mit Flaci II	98
5.6	Erstellen von Automaten mit Kara I	100
5.7	Erstellen von Automaten mit Kara II	102
5.8	Üben und Vertiefen	104
5.9	Am Ziel	106
5.10	Alles im Blick	108

6	Logische Schaltungen	109
6.1	Logische Schaltungen und Simulation	110
6.2	UND-Schaltungen	112
6.3	ODER und NOT-Gatter	114
6.4	Weitere Gatter – NAND, NOR und XOR	116
6.5	Üben und Vertiefen	118
6.6	Am Ziel	121
6.7	Alles im Blick	122
7	KI und maschinelles Lernen	123
7.1	Künstliche Intelligenz: Begriff	124
7.2	Künstliche Intelligenz: Verfahren	126
7.3	Training von KI – Überwachtes Lernen	128
7.4	Training von KI – Unüberwachtes Lernen	130
7.5	Training von KI – Verstärkendes Lernen	132
7.6	Künstliche Intelligenz und das menschliche Gehirn	134
7.7	Projekt: Künstliche Neuronen und Neuronale Netze	136
7.8	Üben und Vertiefen	142
7.9	Am Ziel	145
7.10	Alles im Blick	146

8	Informatik, Mensch und Gesellschaft	147
8.1	Bits und Bytes	148
8.2	Codierung von Pixelgrafiken	150
8.3	Vektorgrafiken und Objektorientierung	152
8.4	Personenbezogene Daten	154
8.5	DSGVO	156
8.6	Datensicherheit	158
8.7	Lizenzen und Lizenzsysteme	160
8.8	Informatiksysteme in der Berufswelt	162
8.9	Üben und Vertiefen	164
8.10	Am Ziel	167
8.11	Alles im Blick	168
	Anhang	169
	Lösungen zu den Seiten „Am Ziel“	169
	Glossar	180
	Stichwortverzeichnis	184

HTML und CSS



Einstieg

Die folgenden Abbildungen zeigen das Gleiche, nur in unterschiedlichen Darstellungen.

- ▶ Beschreibe die Abbildungen kurz und erkläre, weshalb die Bilder das Gleiche zeigen.

```
<h1> Herzlich Willkommen  
</h1><br>  
Du bist auf der Homepage von <b>Anna</b>.  
Ich bin 13 Jahre alt und Schülerin des  
ABC-Gymnasiums. Mehr von mir erfährst du  
hier.
```

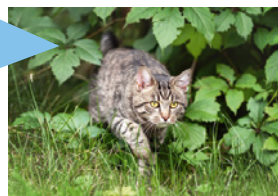
Herzlich Willkommen

Du bist auf der Homepage von **Anna**. Ich bin 15 Jahre alt und Schülerin des ABC-Gymnasiums. Auf dem Bild siehst du meine Katze Minna. Mehr von ihr erfährst du hier.

```
... ABC-Gymnasiums.  
<p>  
  
</p>  
<p>  
Auf dem Bild siehst du meine Katze Minna.  
</p>  
<p>  
Mehr von mir erfährst du  
<a href = "./Steckbrief.html" > hier  
</a>.  
</p>
```

Herzlich Willkommen

Du bist auf der Homepage von **Anna**. Ich bin 15 Jahre alt und Schülerin des ABC-Gymnasiums.



Auf dem Bild siehst du meine Katze Minna. Mehr von ihr erfährst du [hier](#).

Am Ende dieses Kapitels hast du gelernt, ...

- ▶ was die Dokumentenbeschreibungssprache HTML ist.
- ▶ wie man einen HTML-Code erstellt und strukturiert.
- ▶ wie man eine grundlegende Website erstellt.
- ▶ Webseiten mit Cascading Style Sheet (CSS) zu formatieren.
- ▶ Inhalte von Webseiten anzuordnen und responsiv zu formatieren.

EINSTIEG

Sieh dir Annas Webseite an.

- ▶ Aus welchen unterschiedlichen Elementen ist sie aufgebaut?
- ▶ Beschreibe, wie du den gezeigten Ausschnitt mit einem Textverarbeitungsprogramm umsetzen würdest.



ERARBEITUNG



Tim Berners Lee

h steht für „heading“
(engl. Überschrift)

p steht für „paragraph“
(engl. Abschnitt)

br steht für „break“
(engl. Umbruch)



P38043-003

abgebildete HTML-Seite

Die Sprache HTML

HTML steht für „Hypertext Markup Language“, auf Deutsch etwa „Hypertext Aufbau-sprache“. Mit HTML beschreibt man den Aufbau von Webseiten, es handelt sich also nicht um eine Programmiersprache. HTML wurde 1989 von Tim Berners Lee entwickelt, einem Wissenschaftler am CERN in Genf. Zunächst wollte er Texte mit anderen Texten verknüpfen („verlinken“). Er nannte diese Idee „Hypertext“.

A1 HTML-Elemente erkennen SPRACHE

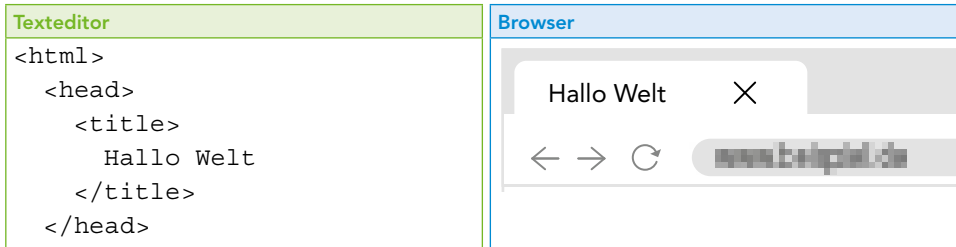
Im folgenden siehst du einen Ausschnitt einer HTML-Seite. Links ist die Ansicht in einem Texteditor zu sehen, rechts die Ansicht im Browser.

Texteditor	Browser
<pre><body> <h1> Hauptüberschrift </h1> <p> Einfacher Text
 Text nach Zeilenumbruch </p> <h2> Abschnitt </h2> <p> Einfacher Text </p> <h3> Unterabschnitt </h3> <p> Einfacher Text </p> </body></pre>	<p>Hauptüberschrift</p> <p>Einfacher Text Text nach Zeilenumbruch</p> <p>Abschnitt</p> <p>Einfacher Text</p> <p>Unterabschnitt</p> <p>Einfacher Text</p>

- Benenne unterschiedliche Elemente der Webseite im Browser (rechts).
- Beschreibe, wie diese Elemente in HTML (links) erstellt werden.
- Gib an, woran man den Anfang und das Ende eines Elements in HTML erkennt.

HTML-Elemente

Jede HTML-Datei beginnt mit dem Element **<html>**. Darin befinden sich jeweils genau einmal die Elemente **<head>** und **<body>**. Das Element **<head>** beschreibt übergeordnete Dinge wie den Titel der Seite. Das Element **<body>** enthält den gesamten Inhalt der Seite, der im Browser zu sehen ist. HTML-Elemente werden durch **Tags** gekennzeichnet. Sie besitzen ein einleitendes Tag (**<h1>**) und ein abschließendes Tag (**/h1>**).



A2 Fehler finden

Die im QR-Code verlinkte HTML-Datei codiert einen Text mit Überschriften. Lade sie herunter und öffne sie mit einem Texteditor. Dem Autor sind einige Fehler unterlaufen. Korrigiere die Fehler, speichere die Datei und prüfe sie mit dem Browser.



P38043-028

HTML-Datei zur Aufgabe

Editor und Browser

HTML-Dateien erstellt man mit einem einfachen **Texteditor**. Ein Texteditor speichert reinen Text, ohne Formatierungen wie Schriftart oder -größe im Gegensatz zu einem Textverarbeitungsprogramm. Einige Texteditoren erkennen, wenn mit HTML gearbeitet wird und stellen die HTML-Codes farbig dar.

HTML-Dateien haben die Dateiendung `.html`. Nach dem Speichern kann man die Datei auch mit einem Browser öffnen. Mit dem Browser prüft man, ob die Datei korrekt erstellt wurde.

Texteditoren (Beispiele):
Notepad++ (Windows)
Atom (MacOS)

Browser (Beispiele):
Edge (Microsoft)
Chrome (Google)
Safari (Apple)
Firefox (Mozilla)

A3 Die erste HTML-Datei erstellen

Schreibe einen kurzen Text mit einem Texteditor. Speichere die Datei als HTML-Datei ab und öffne sie mit einem Browser.

HTML steht für Hypertext Markup Language (Aufbausprache für Hypertext). Jede HTML-Datei beginnt mit dem Element `<html>`, dieses enthält je einmal die Elemente `<head>` und `<body>`. HTML-Code kann man mit einem **Texteditor** schreiben und das Ergebnis mit einem Browser anschauen. HTML-Elemente werden durch ein einleitendes und ein abschließendes Tag gekennzeichnet.

MERKE

- 1 a) Erstelle eine neue Textdatei und gib ihr im `<head>` den Titel „Steckbrief“.
- b) Im `<body>` soll ein Steckbrief zu deiner Person erstellt werden. Formatiere ihn so ähnlich wie im rechts abgebildeten Beispiel. Du kannst auch große und kleinere Überschriften verwenden.
Hinweis: Vor und nach Überschriften lässt der Browser automatisch etwas Platz. Bei einfachem Text erzeugst du Zeilenumbrüche mit `
`.
- c) Dein Steckbrief soll folgende Informationen enthalten:
 - ▶ Name, Klasse und Klassenlehrkraft
 - ▶ Steht dir ein Computer und eine Internetverbindung zur Verfügung?
 - ▶ Welche Vorkenntnisse in Informatik hast du?
 - ▶ Was möchtest du in Informatik lernen?
 - ▶ Was verbindest du mit dem Wort Informatik?
- d) Speichere die HTML-Datei unter dem Namen „Steckbrief.html“. Überprüfe deinen Steckbrief im Browser und korrigiere ihn gegebenenfalls.

AUFGABEN

Browser

Über mich
Name: Harry Potter
Klasse: 8b
Klassenlehrerin: Mrs. McGonnagal

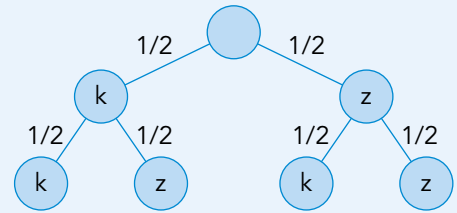
Computer & Co.
Computer: haben meine Eltern
Internet: haben wir zu Hause
Email-Adresse: harry@potter.de

Vorkenntnisse
Ich kenne mich mit Scratch aus und weiß etwas über den Aufbau eines Computers.

EINSTIEG

Baumstrukturen kennt man auch aus der Mathematik: Die Abbildung zeigt das Zufallsexperiment des doppelten Münzwurfs.

- ▶ Welche Baumstrukturen kennst du in der digitalen Welt bzw. in der Informatik?



ERARBEITUNG

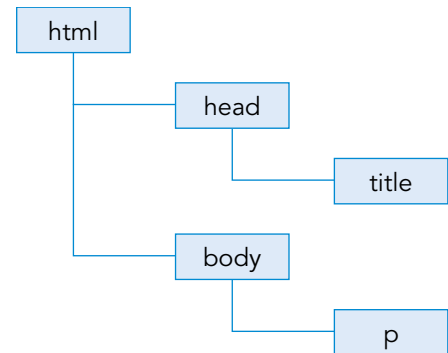
Baumstruktur des HTML-Codes

HTML-Code ist baumartig strukturiert: Elemente können sich in **Unterelemente** aufteilen. Die **Wurzel**, das Ausgangselement der Baumstruktur, ist `<html>`. Es hat die Unterelemente `<head>` und `<body>`, die weitere Unterelemente haben. Beispiel:

Website:
gesamter Webauftritt
Webseite:
einzelne Seite eines
Webauftrittes
Homepage:
Startseite einer Website

```

Texteditor
<html>
  <head>
    <title>
      Text für den Titel
    </title>
  </head>
  <body>
    <p>
      Text eines Abschnitts
    </p>
  </body>
</html>
  
```



A1 Baumstruktur zeichnen

Zeichne zu folgendem HTML-Code die entsprechende Baumstruktur:

```

Texteditor
<html>
  <head>
    <title> Rezept </title>
  </head>
  <body>
    <h1> Gurkensalat </h1>
    <h3> Zutaten </h3>
    <p>
      Eine Salatgurke <br>
      Etwas Dill, eine halbe Zitrone, Salz, Zucker
    </p>
    <h3> Zubereitung </h3>
    <p>
      Schneide die Gurke mit einem Hobel in Scheiben. <br>
      Würze mit Dill, Zitrone, Salz und Zucker.
    </p>
  </body>
</html>
  
```



P38043-004

Code der abgebildeten
HTML-Datei

HTML-Code einrücken

Die Baumstruktur des HTML-Codes mit Elementen und ihren Unterelemente erkennt man auch daran, dass Unterelemente nach rechts eingerückt werden. So kann man den Anfang und das Ende eines Elements leichter erkennen. Statt Leerzeichen einzufügen, verwendet man zum Einrücken den **Tabulator**, der meist auf eine Breite von vier Leerzeichen eingestellt ist.

Die Abbildung zeigt, dass die beiden Unterelemente von `<html>` einen Tabulator weit nach rechts eingerückt werden. Die Unterelemente von `<head>` und `<body>` werden noch weiter eingerückt.

Bei kürzeren Elementen, wie `<title>` und `<h1>` kann man Anfang, Inhalt und Ende auch in eine Zeile schreiben.

Browser stellen HTML-Code auch ohne Einrückung korrekt dar. Einrückungen verbessern aber die Lesbarkeit für den Menschen deutlich.

```

Texteditor
<html>
  <head>
    <title> Rezept </title>
  </head>
  <body>
    <h1> Gurkensalat </h1>
    <p>
      Schneide ...
      würze ...
    </p>
  </body>
</html>

```

Tabulator-Taste auf einer PC-Tastatur:



A2 Einrücken

Lade die im QR-Code verlinkte HTML-Datei herunter und öffne sie mit einem Texteditor. Der HTML-Code ist nicht eingerückt. Rücke jede Zeile mit der Tabulator-taste so weit ein wie nötig. Die Struktur der Unterelemente soll sich deutlicher erkennen lassen.




P38043-005

HTML-Datei zu A2

HTML-Elemente können **Unterelemente** haben, die wieder Unterelemente haben können. Dadurch ergibt sich eine **Baumstruktur**. Im Code sollten Unterelemente mit der Tabulator-Taste nach rechts eingerückt werden.

MERKE

1 Die hinterlegte HTML-Datei hat eine etwas komplexere Struktur. Sie enthält auch Elemente, die du möglicherweise noch nicht kennst. Die Baumstruktur kannst du aber bereits erkennen. 

- Öffne die Datei mit dem Texteditor. Rücke jede Zeile mit Tabulatoren so ein, dass die Struktur der Unterelemente erkennbar wird.
- Stelle die HTML-Datei in einem Baumdiagramm dar.

2 Der folgende HTML-Code ist fehlerhaft, unvollständig und nicht korrekt eingerückt. Korrigiere und ergänze ihn.

```

<html>
  </title> Mein Haustier <title>
  <body>
    <h1> Charlie </h1>
    <p>
      Tierart: Chihuahua
      Alter: 5 Jahre
    </p>
    ...

```

AUFGABEN



P38043-006

HTML-Datei zu Aufgabe 1 und 2

EINSTIEG

Informationen werden oft in Form von Listen dargestellt, mit Punkten oder Nummerierung.

- ▶ Überlege, für welche Art von Informationen Listen nützlich sind.

Browser

Liste mit Stichpunkten

(„unordered list“)

- Prozessor
- Arbeitsspeicher
- Grafikkarte
- Soundkarte
- Netzwerkkarte

Nummerierte Liste

(„ordered list“)

1. Aufstehen
2. Schule
3. Hausaufgaben
4. Fernsehen
5. Schlafen

ERARBEITUNG

Listen in HTML

In HTML kann man **nummerierte** und **unnummerierte Listen** erstellen. Eine Liste wird mit dem Element `` bzw. `` erzeugt. Beide Listentypen können beliebig viele Elemente enthalten, welche die einzelnen Listenpunkte darstellen.

ul: unordered list
ol: ordered list
li: list item

Texteditor

```
<p> Werkzeuge: </p>
<ul>
  <li> Texteditor </li>
  <li> Browser </li>
</ul>

<p> Arbeitsschritte: </p>
<ol>
  <li> Codieren </li>
  <li> Prüfen </li>
</ol>
```

Browser

Werkzeuge:

- Texteditor
- Browser

Arbeitsschritte:

1. Codieren
2. Prüfen

A1 Liste codieren 

Erstelle eine HTML-Datei, mit der sich die Listen aus dem Einstieg darstellen lassen.

Unterpunkte

Manchmal benötigt man in Listen weitere Ebenen. Dafür fügt man HTML-Code innerhalb einer Liste eine weitere Liste ein.

Texteditor

```
<h1> Computerteile </h1>
<ul>
  <li> Prozessor </li>
  <ul>
    <li> AMD </li>
    <li> Intel </li>
  </ul>
  <li> Grafikkarte </li>
  <ul>
    <li> ATI </li>
    <li> nVidia </li>
  </ul>
</ul>
```

Browser

Computerteile:

- Prozessor
 - AMD
 - Intel
- Grafikkarte
 - ATI
 - nVidia

A2 ToDo-Liste in HTML erstellen SPRACHE

Erstelle eine HTML-Datei mit einer ToDo-Liste für die kommende Woche. Verwende mehrere Ebenen.

Ideen zur Gliederung der Liste:
Schule, Freizeit, Eltern,
Freunde

Zeichencodierung und Sonderzeichen

Werden Texte digital verarbeitet, wird jedes Zeichen codiert. Im Laufe der Jahrzehnte sind eine Vielzahl unterschiedlicher Codierungen für Texte, sogenannte **Zeichensätze** entstanden. Zwei bekannte Zeichensätze sind ASCII aus den 1960er Jahren und der moderne Unicode, der aktuell in der Form UTF-8 der am häufigsten verwendete Zeichensatz ist.

ASCII

- a, b, ..., z
- A, B, ..., Z
- 0, 1, ..., 9
- !, ? und ein paar Sonderzeichen
- insgesamt 128 Zeichen

Unicode (UTF-8)

- die ersten 128 Zeichen wie bei ASCII
- Schriftzeichen anderer Sprachen
- Symbole
- u. v. m
- insgesamt 1 114 112 Zeichen

ASCII enthält z. B. keine Umlaute (ä, ö, ü).

In Notepad++ kann man den Zeichensatz z. B. im Menü „Codierung“ einstellen.

Damit ein Browser eine HTML-Datei korrekt darstellen kann, muss darin vermerkt sein, welcher Zeichensatz verwendet wird. Dies wird im `<head>` der Datei vermerkt.

Texteditor

```
<head>
  <meta charset="UTF-8">
  <title> ... </title>
</head>
```

charset: character set
(Zeichensatz)

A3 Zeichensätze vergleichen

- a) Öffne die hinterlegte HTML-Datei in einem Browser und beschreibe deine Beobachtung.
- b) Korrigiere die HTML-Datei so, dass der Text richtig dargestellt wird.



P38043-007
QR-Code

Unnummerierte Listen werden mit dem Element ``, **nummerierte Listen** mit dem Element `` erzeugt. Einen Listenpunkt fügt man mit dem Element `` ein. Texte bestehen aus Zeichen, die mit **Zeichensätzen** codiert werden. Der Unicode-Zeichensatz (aktueller Standard: UTF-8) enthält alle für das World Wide Web relevanten Zeichen. In HTML-Dateien gibt man den Zeichensatz im Header mit dem Element `<meta>` an.

MERKE

- 1 a) Erstelle eine HTML-Seite mit mindestens drei nummerierten Listen. Zähle darin deine fünf Lieblingssportler, -musiker, -filme, -serien oder -bücher auf.
- b) Erstelle eine HTML-Seite, die eine Liste mit mehreren Ebenen zum Thema „Informatik in Klasse 5/6“ enthält. Führe als Oberpunkte Themen auf, an die du dich noch erinnern kannst. Formuliere eine Ebene tiefer stichpunktartig, welche Unterrichtsinhalte du innerhalb der einzelnen Themen kennengelernt hast.
- c) Wähle in deinen Dateien aus a) und b) als Zeichensatz UTF-8. Ergänze deine Dateien dazu an geeigneter Stelle.

AUFGABEN

Bücher

1. Der Hobbit
2. Momo
3. Tortilla Flat
4. Stardust
5. Wiseguy

Informatik in Kl. 6

- Codierungen
 - ASCII
 - Binärzahlen
 - QR-Code

EINSTIEG

Es gibt zahlreiche Dateiformate für Bilddateien.

- ▶ Finde heraus, in welchem Dateiformat die Bilder auf deinem Smartphone gespeichert werden. Vergleiche eure Ergebnisse.
- ▶ Recherchiere Eigenschaften einiger der gängigen Formate, die du in der Abbildung siehst.



ERARBEITUNG

Dateiformate für Bilder

Bilder werden in unterschiedlichen **Dateiformaten** gespeichert. Diese bestimmen unter anderem, wie stark die Bildinformationen komprimiert werden oder ob ein Bild aus mehreren Ebenen zusammengesetzt sein kann.

Welches Dateiformat ein Bild hat, erkennt man an der **Dateiendung**.

Im Internet sind die wichtigsten Dateiformate:

jupiter.**jpg** (oder **jpeg**): kann Bilder recht stark komprimieren

venus.**png**: unterstützt auch transparente Flächen in Bildern

mars.**gif**: unterstützt auch animierte (also bewegte) Bilder

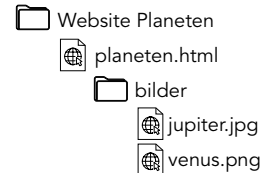
jpg: entwickelt von der Joint Photo Experts Group
 png: Portable Network Graphics
 gif: Graphics Interchange Format

A1 Dateiendungen anzeigen lassen 

Ändere die Einstellungen deines Computers so, dass Dateiendungen angezeigt werden.

Ordnung für Bilder

Webseiten mit Bildern bestehen oft aus vielen Dateien. Daher ist es wichtig, Ordnung zu halten. Die Webseite sollte einen eigenen Ordner auf dem Computer haben, und für Bilder sollte man einen Unterordner erstellen.

A2 HTML-Seite vorbereiten 

Im Folgenden sollst du eine kleine HTML-Seite mit Text und Bildern zu drei bis vier Planeten erstellen.

- Erstelle einen Ordner für die Webseite mit einem Unterordner „bilder“.
- Lade zu jedem Planeten ein Foto herunter und speichere es im Ordner „bilder“. Achte darauf, den Dateien sinnvolle, nicht zu lange Dateinamen zu geben, die du leicht in den HTML-Code übertragen kannst.

Bilder im HTML-Code

Mit dem Element `` wird eine Bilddatei in eine HTML-Seite integriert:

Beispiel: ``

Der Punkt gibt den Ordner an, in dem sich die HTML-Datei selbst befindet. Unterordner, in dem sich das Bild befindet Name der Datei inkl. Dateiendung

img: image (Bild)
 src: source (Quelle)

Das Element `` enthält ein sogenanntes Attribut: `src`. Mit Attributen kann man Elementen detailliertere Informationen „mitgeben“, in diesem Fall den Ordner und Dateinamen der Bilddatei.

Bilder kann man vor, nach oder zwischen anderen Elementen wie `<p>` oder `<h1>` in den `<body>` einfügen:

Texteditor

```
<h1> Der Jupiter </h1>

<p> Der größte Planet... </p>
```

A3 HTML-Seite umsetzen

Arbeite weiter in der Ordnerstruktur aus A2. Erstelle nun die HTML-Seite. Darin soll jeder Planet eine Überschrift, etwas Text sowie das passende Bild haben.

Spielregeln im Umgang mit Bildern

Bei der Veröffentlichung von HTML-Seiten im Internet (→ Webseite) müssen einige Gesetze beachtet werden. Das **Urheberrecht** bestimmt, in welchen Fällen man fremde Bilder (oder andere Werke) veröffentlichen darf.

- ▶ Sofern nichts anderes angegeben ist, gilt für Bilder das **Copyright**. Danach darf man diese nicht ohne Zustimmung des Urhebers veröffentlichen. Es können unter Umständen Lizenzgebühren fällig werden.
- ▶ **Creative-Commons-Lizenzen** bieten Urhebern die Möglichkeit, anderen die Veröffentlichung ihrer Werke unter festgelegten Bedingungen zu erlauben. Nebenstehend sind einige der Lizenzen abgebildet, aus denen Urheber selbst wählen können.

Für alle Werke, deren Autor man selbst nicht ist, müssen **Quellenangaben** gemacht werden. Dabei muss der Urheber und gegebenenfalls das Lizenzmodell angegeben werden.

Neben dem Urheberrecht gilt außerdem das **Recht am eigenen Bild**. In der EU dürfen Bilder von Personen nur mit deren Einverständnis veröffentlicht werden. Ausnahmen:

- ▶ Personen der Zeitgeschichte
- ▶ Bilder, auf denen Personen nur Beiwerk sind
- ▶ Bilder von Versammlungen

A4 Quellenangaben machen

- Recherchiere für jedes Bild aus A1 bzw. A2, ob es copyrightgeschützt ist oder unter einer Creative-Commons-Lizenz (o. ä.) veröffentlicht wurde.
- Füge an das Ende der Webseite einen Absatz ein, in dem du für jedes Bild den Urheber, die Quelle und das Lizenzmodell angibst. Webadressen kannst du einfach als Text einfügen.

Die wichtigsten **Dateiformate**, die auf Webseiten verwendet werden sind jpg, png und gif. Bilder werden auf HTML-Seiten mit dem Element `` eingebunden. Es hat ein **Attribut** namens `src`, das Ordner und Namen der Bilddatei angibt. Aus Gründen der Übersichtlichkeit sollten alle Bilder eine HTML-Seite in einem Unterordner gespeichert werden.

- Zwei wesentliche Bilddateiformate sind JPEG und PNG. Recherchiere die Unterschiede zwischen diesen Dateiformaten in Hinblick auf die Bedeutung der Abkürzungen, der Dateigröße und wann sich der jeweilige Einsatz anbietet.

Das Sonnensystem

Diese Webseite stellt einige Planeten vor.

1. Die Venus

Die Venus ist nach dem Merkur der Planet, der der Sonne am zweitnächsten ist. An manchen Tagen kann man die Venus mit bloßem Auge am Himmel erkennen.



Lizenzsymbole:



Copyright



Creative Commons



Urheber nennen



keine kommerzielle Verwendung



Veröffentlichung unter gleichen Bedingungen

→ Kapitel 8

Bei Webseiten gibt man immer das Datum des letzten Aufrufes an.

MERKE

AUFGABEN

EINSTIEG

Sicher kennst du das Gefühl der Ungeduld, wenn eine Webseite nur langsam lädt.

- ▶ Deine Internetverbindung hat eine Downloadgeschwindigkeit von 50 Mbit/s. Eine Webseite verwendet 10 Bilder von je 5 MB, eine andere 20 Bilder von je 250 kB. Wie viel schneller kann die zweite Seite geladen werden?



ERARBEITUNG

Bildgröße und Anzeigegröße

Die Größe eines digitalen Bildes wird in **Pixeln**, also Bildpunkten gemessen. Das derzeit wohl bekannteste Beispiel einer Auflösung ist Full-HD mit 1920×1080 Pixeln.

Im HTML-Code kann man die Größe, in der ein Bild im Browser angezeigt wird, unabhängig von seiner Originalgröße einstellen.

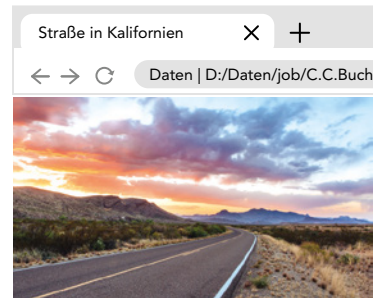
```

```



Breite der Originaldatei: 1600 Pixel

Höhe:
900
Pixel



width="800px"

width: Breite
height: Höhe

Man verwendet das Attribut **width**, um die Anzeigebreite eines Bildes einzustellen. Die Höhe passt sich automatisch der Breite (passend zum Seitenverhältnis) an. Das Attribut **height** benötigt man daher für Bilder in der Regel nicht.

A1 Auflösungen interpretieren

- Finde die Auflösung deines Smartphonebildschirms heraus.
- Nenne Konsequenzen, wenn ein Bild mit hoher (niedriger) Auflösung auf einer HTML-Seite sehr klein (groß) dargestellt werden soll.

Dateigröße und Übertragung von Bildern

Neben Breite und Höhe spielt für digitale Bilder auch der **Speicherplatz** einer Bilddatei eine Rolle. Ein RGB-Bild benötigt pro Pixel 3 Byte Speicherplatz. Durch Komprimierung kann man ein Bild mit einer Auflösung von 4000×3000 Pixeln auf ungefähr sechs Megabyte reduzieren, ohne allzu viel Bildqualität zu verlieren.

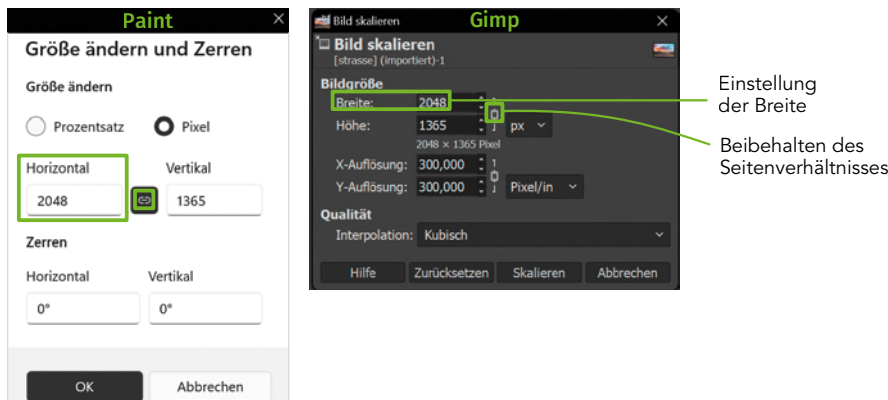
1 Kilobyte = 1000 Byte
1 Megabyte = 1000 kB
1 Gigabyte = 1000 MB
1 Terabyte = 1000 GB

	Bilder in Texten	Hintergrundbilder
Empfohlenes Bildformat in px	400 × 300 bzw. 800 × 600	1200 × 800 bzw. 1920 × 1080
Empfohlene Dateigröße	100–500 kB	100 kB–2 MB

Für Betreiber von Webseiten ist es bedeutsam, wie viel Zeit eine Datei braucht, um über das Internet übertragen zu werden.

Bildqualität reduzieren

Wenn man die Anzeigegröße eines Bildes auf einer Webseite mit dem Attribut `width` verkleinert, wird die Datei trotzdem in vollständiger Größe über das Internet übertragen. Deshalb sollte man zu große Dateien mit einem **Bildbearbeitungsprogramm** verkleinern.



Paint und Gimp (Gnu Image Manipulation) sind kostenlos verfügbare Bildbearbeitungsprogramme.

Paint: Start → Größe ändern
Gimp: Bild → Bild skalieren

Paint: Datei → Speichern unter → jpg auswählen
Gimp: Datei → Exportieren als → .jpg als Dateiendung eingeben → Qualität 90 Prozent

A2 Bild verkleinern

- Lade die hinterlegte HTML-Seite herunter.
- Öffne die Bilddatei mit einem Bildbearbeitungsprogramm.
- Verkleinere das Bild auf eine Breite von 1 200 Pixeln.
- Speichere das Bild im JPG-Format unter einem neuen Dateinamen ab. Wähle in Paint den Menüpunkt *Datei* → *Speichern unter*. Achte darauf, dass das JPG-Format ausgewählt ist. Die Qualität kannst du einstellen, nachdem du auf „Speichern“ geklickt hast.
- Notiere die Dateigrößen der Original- und der neuen Datei. Berechne, um wie viel Prozent die Dateigröße verringert werden konnte.
- Öffne die HTML-Datei mit dem Texteditor. Ändere das Element ``, sodass die verkleinerte Bilddatei verwendet wird. Füge das Attribut `width` hinzu, um das Bild mit einer Breite von 800 Pixeln anzuzeigen.



P38043-029

HTML-Seite zu Aufgabe A1

Breite und Höhe digitaler Bilder gibt man in **Pixeln** (Bildpunkten) an. Die Anzeigegröße eines Bildes kann man im HTML-Code mithilfe des Attributs `width` einstellen (ohne dass sich dadurch die Dateigröße ändert). Die **Dateigröße** einer Bilddatei gibt an, wie viel **Speicherplatz** (gemessen in Kilo- oder Megabyte) diese benötigt. Die Auflösung und damit auch die Dateigröße kann man mit einem **Bildbearbeitungsprogramm** verkleinern.

MERKE

- Bearbeite deine HTML-Seite aus dem vorherigen Kapitel zum Thema „Planeten“. Prüfe jede Bilddatei auf ihre Dateigröße sowie ihre Breite. Falls die Dateigröße mehr als 500kB beträgt, verkleinere das Bild. Falls die Breite weniger als 800 Pixel beträgt, lade ein neues, größeres Bild herunter.

AUFGABEN

EINSTIEG

In vielen Büchern findest du ein Stichwortverzeichnis mit Seitenzahlen.

- ▶ Beschreibe, was es damit auf sich hat.
- ▶ Nenne ähnliche Beispiele.

E

Eindeutigkeit	80
Eingabealphabet	116
Ein- und Ausgabewerk	25
Empfänger	60

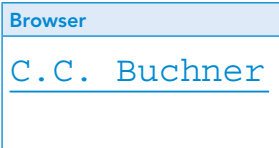
ERARBEITUNG

Links: Verknüpfungen im WWW

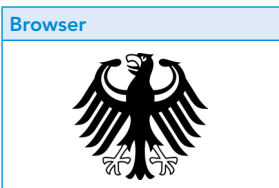
Ein **Link** ermöglicht eine Verbindung zwischen zwei HTML-Seiten. Links werden als Text oder Bild dargestellt, und man kann sie z. B. mit der Maus oder mit dem Finger „anklicken“. Dann zeigt der Browser die verknüpfte Webseite an. Dies kann auch eine beliebige Webseite im World Wide Web sein.

Links werden in HTML mit dem Element `<a>` erzeugt. Mit `href` gibt man die Adresse der verlinkten Seite an. Der Text, der zwischen `<a>` und `` steht, erscheint auf der Seite als anklickbarer Link, oft in blauer Schrift und unterstrichen.

a: anchor (Anker)
href: hyper reference
(Adresse einer Webseite)

Texteditor	Browser
<pre> C.C. Buchner </pre>	

Zwischen `<a>` und `` kann an Stelle eines Textes auch das Element `` eingefügt werden. Dann wird der Link als anklickbares Bild dargestellt:

Texteditor	Browser
<pre> </pre>	

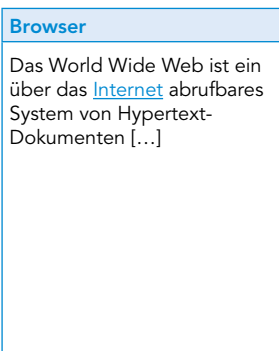
target: Ziel

Wenn man möchte, dass sich eine verlinkte Seite in einem neuen Tab öffnet, fügt man `target="new"` hinzu:

Texteditor
<pre> ... </pre>

Links können zwischen Elementen wie Überschriften und Absätzen eingefügt werden. Man kann aber auch Wörter innerhalb von Sätzen als Link codieren. Dies wird zum Beispiel in Wikipedia häufig angewendet:

Zeilenumbrüche im HTML-Code werden vom Browser ignoriert. Das Wort „Internet“ steht mitten im Satz:

Texteditor	Browser
<pre><p> Das World Wide Web ist ein über das Internet abrufbares System von Hypertext- Dokumenten [...] </p></pre>	

A1 Links als Text darstellen

Erstelle eine HTML-Datei, die den folgenden Text darstellt. Die unterstrichenen Begriffe sollen als Link auf die passende Wikipedia-Seite erscheinen:
Die Hypertext Markup Language ist eine Auszeichnungssprache zur Strukturierung elektronischer Dokumente wie Texte mit Hyperlinks, Bildern und anderen Inhalten. HTML-Dokumente sind die Grundlage des World Wide Web und werden von Webbrowsern dargestellt.

Webadressen

Adressen von Webseiten werden als **URL** angegeben:

https://de.wikipedia.org/wiki/HTML
 Protokoll Domainname Pfad

Das Protokoll https regelt die Übertragung von Webseiten vom Webserver zum Browser. Das „s“ in https bedeutet „secure“. Damit werden Daten verschlüsselt übertragen, um sie vor Missbrauch zu schützen.

Der Domainname „de.wikipedia.org“ beschreibt einen Computer, der mit dem Internet verbunden ist (→ Seite 28, 29).

Der Pfad am Ende der URLs beschreibt einen Ordner auf diesem Computer, in dem die gesuchte Webseite zu finden ist.

URL: uniform resource locator
(einheitlicher Ressourcen-
zeiger)

http: hypertext transfer
protocol (Übertragungs-
protokoll für Hypertext)

Es können auch mehrere
Computer sein.

A2 Link-Liste SPRACHE

Erstelle eine HTML-Datei, die eine nummerierte Liste von Links zu einigen Webseiten zeigt, die du häufig nutzt. Die verlinkten Seiten sollten sich jeweils in einem neuen Tab öffnen.

Mit **Links** kann man Texte oder Bilder mit anderen Webseiten verknüpfen. Dazu wird das Element `<a>` verwendet mit dem Attribut `href`, das die Adresse der verknüpften Webseite in Form einer **URL** angibt. Ein URL besteht aus einem Protokoll (z. B. https), einem Domainnamen und optional einem Pfad.

MERKE

- 1 a) Erstelle zunächst einen Ordner „Website“, welche den Unterordner „bilder“ enthält.
- b) Suche mehrere Logos oder Bilder von Vereinen, die du magst und speichere sie im Ordner „bilder“.
- c) Erstelle eine HTML-Datei mit den gefundenen Bildern. Verlinke jedes Bild mit der Homepage des entsprechenden Vereins.

AUFGABEN



- 2 SPRACHE Das Einbetten von Videos ist eine weitere Möglichkeit, deine HTML-Seiten attraktiver zu gestalten. So kannst du Videos direkt auf deiner Seite anzeigen lassen. Der HTML-Code zum Einbetten von Videos ist in der Regel unter oder neben dem Video zu finden.
Erstelle eine Webseite, in die du mindestens ein Video einbettest.

Beispiel: Video einbetten

Texteditor

```
<iframe width="560" height="315"
src="https://www.youtube.com/embed
/mztvStKHQRQ" title="YouTube video
player" frameborder="0"></iframe>
```

EINSTIEG

Rufe deine Lieblingswebsite auf.

- ▶ Aus wie vielen einzelnen Seiten besteht sie?
- ▶ Wie gelangt man als Benutzer von einer Seite auf die andere?



ERARBEITUNG

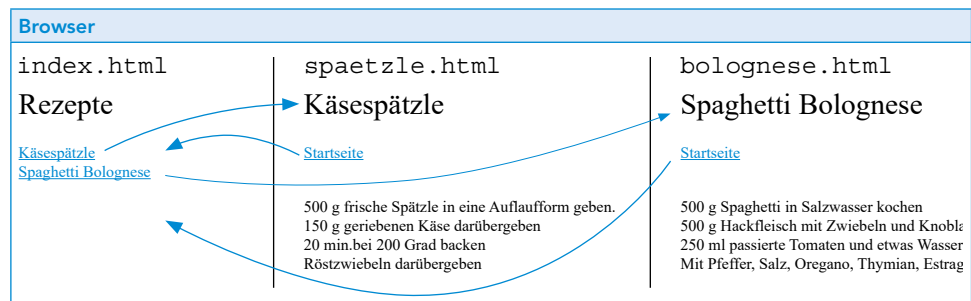
Mehrere HTML-Dateien

Eine Website besteht in der Regel nicht nur aus einer HTML-Datei. Meist wird der Inhalt auf mehrere **Unterseiten** verteilt. Jede davon wird in einer eigenen HTML-Datei gespeichert. Damit die Lesenden von einer Unterseite zur anderen wechseln können, werden diese HTML-Dateien miteinander verlinkt.

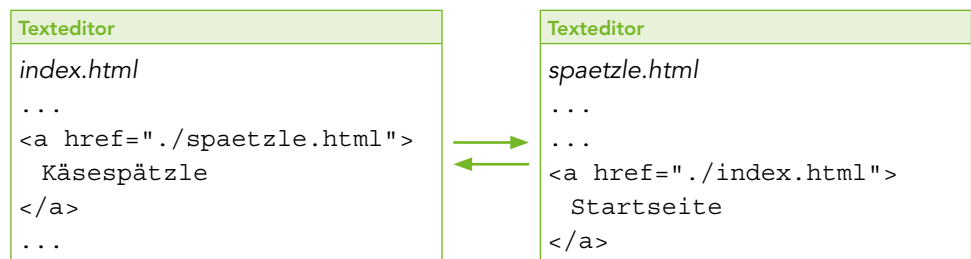
Möchte man beispielsweise eine Website für Rezepte erstellen, besteht diese aus einer Startseite, die den Überblick über die Rezepte gibt, und je einer Seite für jedes Rezept, etwa mit folgenden Dateinamen:

- ▶ index.html: Die Startseite (Homepage)
- ▶ spaetzle.html: Rezept für Käsespätzle
- ▶ bolognese.html: Rezept für Spaghetti Bolognese
- ▶ ...

Man kann die Seiten beispielsweise folgendermaßen verlinken:



Um HTML-Dateien miteinander zu verlinken, benutzt man ebenfalls das Element `<a>`. Im Attribut `href` gibt man die HTML-Datei an, zu der man navigieren möchte.



Der Punkt in `"/spaetzle.html"` bezeichnet den Ordner, in dem die HTML-Datei selbst liegt.

A1 HTML-Dateien verlinken 

- In den hinterlegten HTML-Dateien für die Rezept-Website fehlen die Verlinkungen. Füge die Links so hinzu, dass man von der Startseite jeweils zu den Rezept-Seiten und wieder zurück navigieren kann.
- Füge zwei weitere HTML-Dateien mit eigenen Rezepten hinzu. Verlinke die neuen HTML-Dateien ebenfalls mit der Startseite.



P38043-008

Webseite zu Aufgabe A1

Navigation

Um von einer Unterseiten zur anderen springen zu können, haben viele Websites eine **Navigation**. Eine Navigation besteht aus Links auf die wichtigsten HTML-Dateien des Webauftritts. Die Navigation ist üblicherweise auf jeder dieser HTML-Dateien zu sehen und sollte immer gleich aussehen.

Beispiel:

Browser		
<p>Leckere Rezepte</p> <ul style="list-style-type: none"> • Willkommen • Spargel mit Schweineschnitzel und Kartoffeln • Salat mit Dressing <p>Willkommen</p> <p>Hier findest Sie einfache Rezepte zum nachkochen und für jeden Geschmack. Entdecken Sie verschiedene Rezeptlisten und tauchen Sie in eine Welt des Genusses ein.</p> 	<p>Leckere Rezepte</p> <ul style="list-style-type: none"> • Willkommen • Spargel mit Schweineschnitzel und Kartoffeln • Salat mit Dressing <p>Salat mit Parmesan und Dressing</p> 	<p>Leckere Rezepte</p> <ul style="list-style-type: none"> • Willkommen • Spargel mit Schweineschnitzel und Kartoffeln • Salat mit Dressing <p>Spargel mit Kartoffeln und Schnitzel auf Sauce Hollandaise</p> 

A2 Navigation erstellen

In den hinterlegten Dateien findest du die oben dargestellte Webseite. Sie ist schon auf mehrere HTML-Dateien aufgeteilt, die Unterseiten sind jedoch nicht miteinander verlinkt.

- Erstelle in der Datei der Startseite (index.html) eine Navigation (als unnummerierte Liste) zu allen Seiten, einschließlich der Startseite selbst.
- Füge die Navigation an der gleichen Stelle in die anderen HTML-Dateien ein.



P38043-009

Webseite zu Aufgabe 1

Webauftritte bestehen oft aus mehreren Seiten, die in separaten HTML-Dateien gespeichert und miteinander verlinkt sind. Diejenige Startseite (Homepage) hat als Dateinamen üblicherweise **index.html**.

Eine **Navigation** besteht aus Links auf die wichtigsten Seiten der Website und sollte immer gleich aussehen.

MERKE

1 Für gewerbliche Webauftritte gilt das Telemediengesetz. Danach ist der Inhaber oder die Inhaberin verpflichtet, Namen und einige weitere Daten auf der Website zu veröffentlichen. Dies wird häufig „Impressum“ genannt.

- Informiere dich auf der verlinkten Webseite über das Telemediengesetz.
- Füge deinen Ergebnissen aus A2 eine weitere Unterseite hinzu, auf der du entsprechende Informationen über einen fiktiven Inhaber darstellst.

AUFGABEN



P38043-010

Link zum Telemediengesetz

EINSTIEG

Das Web wurde mit dem Gedanken entwickelt, Inhalte und ihre Darstellung voneinander zu trennen. Den Inhalt einer Webseite verfassen Autoren und verteilen ihn auf Teil-Seiten, Kapitel, Listen, Bilder usw. Die Darstellung gehört in den Bereich des (Web-) Designs: durch Farben, Schriftarten, Layout usw. wird der Inhalt ansprechend „verpackt“.

- Überlege, welche Vorteile diese Trennung hat.



ERARBEITUNG

Cascading Style Sheets

Für Websites geschieht die Trennung von Inhalt und Darstellung mit zwei Sprachen.

Inhalt wie Überschriften,
Absätze, Links mit HTML

Optische Gestaltung
der HTML-Inhalte mit CSS

Mit CSS können jedem HTML-Element, z. B. `<h1>`, `<p>` oder `` verschiedene Eigenschaften zugeordnet werden. Dadurch kann bestimmt werden, wie diese Elemente optisch dargestellt werden. In der folgenden Tabelle sind einige Beispiele für CSS-Eigenschaften aufgeführt.

CSS-Eigenschaft	Erläuterung	Mögliche Werte
font-family	Schriftart	Arial, Times New Roman, ...
text-decoration	Texteffekte	underline, blink, ...
color	Farben (Text, Linien)	red, green, blue, ...

Mit CSS können jedem HTML-Element beliebig viele CSS-Eigenschaften zugeordnet werden. Dabei wird in geschweiften Klammern die CSS-Eigenschaft geschrieben. Nach einem Doppelpunkt folgt der konkrete Wert dieser Eigenschaft. Mehrere CSS-Eigenschaften werden durch Semikolons getrennt.

Texteditor (CSS-Datei)	Browser
<pre>body { font-family: Arial; } h1 { font-size: 20 pt; color: blue; }</pre>	Hauptüberschrift

Je nachdem welches HTML-Element man mit CSS anspricht, kann das unterschiedliche Auswirkungen auf die Website haben. Wird eine CSS-Eigenschaft auf den `body` angewendet, so gilt das für den gesamten HTML-Inhalt innerhalb dieses HTML-Elements, beispielsweise wird auf der gesamten Website die Schriftart Arial genutzt. Wird für eine `<h1>`-Überschrift eine bestimmte Schriftgröße und -farbe festgelegt, so gilt dies nur für jede `<h1>`-Überschrift der gesamten HTML-Seite.

A1 CSS-Eigenschaften sehen 

- Öffne die hinterlegte Website und mache dich mit dem CSS-Code vertraut.
- Verändere die verschiedenen Eigenschaften des CSS-Codes und notiere dir die Beobachtungen.



P38043-011

CSS-Texteigenschaften

CSS-Datei

Um eine Website mit CSS zu formatieren, kann eine eigene CSS-Datei erstellt werden. Diese CSS-Datei kann einen beliebigen Namen haben, benötigt jedoch die Endung (z. B. Format.css). Außerdem muss sie im selben Ordner wie die HTML-Datei liegen. Der Vorteil einer eigenen Datei für den CSS-Code ist, dass dadurch der Code in der HTML-Datei übersichtlich und strukturiert bleibt, da nur die eigentlichen HTML-Elemente enthalten sind.



A2 CSS-Datei erstellen

- Öffne die hinterlegte HTML-Datei und verschaffe dir einen Überblick über den Code.
- Schreibe die CSS-Eigenschaften und Werte so, dass die nebenstehenden Formatierungen entstehen.



P38043-012
HTML-Datei

CSS-Datei mit HTML-Dateien verknüpfen

Damit die HTML-Datei auf die CSS-Datei zugreifen kann, müssen beide Dateien miteinander verknüpft werden. Die Verknüpfung wird in den `<head>` der HTML-Datei geschrieben.

Texteditor der HTML-Datei

```
<head>
  <meta charset = "UTF-8" />
  <title> ... </title>
  <link rel = "stylesheet" href = "./formate.css" />
</head>
```

Durch das Attribut `link rel="stylesheet"` wird die HTML- mit der CSS-Datei verknüpft.

Durch `href="./formate.css"` wird der Name und der Speicherort der CSS-Datei angegeben.

A3 CSS-Datei einbinden

- Verknüpfe deine HTML-Datei mit deiner CSS-Datei aus A2.
- Teste im Browser, ob die Seite wie gewünscht dargestellt wird. Verbessere etwaige Fehler in der CSS- bzw. HTML-Datei.

A4 Hintergrundfarbe einstellen

Häufig sieht man auf Webseiten auch eine Hintergrundfarbe. Recherchiere die dazugehörige CSS-Eigenschaft und füge deiner Webseite aus A3 eine passende Hintergrundfarbe hinzu.

EINSTIEG

Mit Tabellen kann man gleichartige Informationen übersichtlich darstellen.

- ▶ Welche Anwendungen für Tabellen fallen dir ein?

Subjekt	Verb	Objekt
Anna	spielt	Fußball
Bob	geht	schwimmen
Teresa	liebt	Tennis

ERARBEITUNG

Tabellen

Tabellen sind aus Zellen aufgebaut. Diese sind in Zeilen und Spalten angeordnet. In HTML werden Tabellen mit dem Element `<table>`, Zeilen mit `<tr>` und Zellen mit `<td>` erstellt. Standardmäßig werden im Browser keine Rahmen angezeigt.

table (engl.): Tabelle
tr (Abk.): table row
td (Abk.): table data

Texteditor	Browser						
<pre><table> <tr> <td> 29.11.23 </td> <td> Fußball </td> <td> 30,00 € </td> </tr> <tr> <td> 01.12.23 </td> <td> Schuhe </td> <td> 50,00 € </td> </tr> </table></pre>	<table border="1"> <tbody> <tr> <td>29.11.23</td> <td>Fußball</td> <td>30,00 €</td> </tr> <tr> <td>01.12.23</td> <td>Schuhe</td> <td>50,00 €</td> </tr> </tbody> </table>	29.11.23	Fußball	30,00 €	01.12.23	Schuhe	50,00 €
29.11.23	Fußball	30,00 €					
01.12.23	Schuhe	50,00 €					

A1 Tabellen mit HTML erstellen

Obiger HTML-Code wird im Browser als Tabelle angezeigt. Beschreibe anhand des Beispiels, wie man eine Tabelle erzeugt und die Zellen befüllt.

border-style: Rahmenlinie
border-width: Rahmenbreite
border-color: Rahmenfarbe

Tabellenlinien in CSS

Um Linien einer Tabelle zu formatieren, müssen für die HTML-Elemente `<table>` und `<td>` CSS-Eigenschaften vergeben werden. Mit den CSS-Befehlen `border-style`, `border-width` und `border-color` können die Rahmen der einzelnen Zellen angepasst werden. Mit `border-collapse` werden die Zellen verbunden dargestellt. Um den Inhalt der Zellen mit Abstand zu den Linien darzustellen, kann der Befehl `padding` genutzt werden. Die Pixelanzahl gibt an, wie groß der Abstand zwischen dem Text und den Tabellenlinien sein soll.

Texteditor (CSS-Datei)	Browser						
<pre>table { border-collapse: collapse; } td { border-style: solid; border-width: 2 px; border-color: grey; padding: 5px; }</pre>	<table border="1"> <tbody> <tr> <td>29.11.23</td> <td>Fußball</td> <td>30,00 €</td> </tr> <tr> <td>01.12.23</td> <td>Schuhe</td> <td>50,00 €</td> </tr> </tbody> </table>	29.11.23	Fußball	30,00 €	01.12.23	Schuhe	50,00 €
29.11.23	Fußball	30,00 €					
01.12.23	Schuhe	50,00 €					

A2 Tabellen mit CSS formatieren

- Öffne die hinterlegte Seite und verändere die Werte der Eigenschaften des Rahmens. Erstelle eine Übersicht über die verwendeten CSS-Eigenschaften und erläutere darin deren unterschiedliche Werte.
- Gehe dabei auch auf die Angabe von Farbwerten durch englische Wörter bzw. das RGB-System ein.



P38043-013

CSS-Tabellenbefehle

CSS-Klassen erstellen

Bisher werden gleiche HTML-Elemente mit dazugehörigen CSS-Eigenschaften immer gleich formatiert. Häufig möchte man auf Webseiten aber gleiche Elemente wie Überschriften, in unterschiedlichen Format darstellen, z. B. mit einer anderen Farbe oder Schriftart. In einer CSS-Datei kann man mehrere Klassen für ein HTML-Element definieren. Dabei werden Klassen mit einem Punkt nach dem angesprochenen HTML-Element erzeugt. So auch, um Tabellenzellen einzeln zu formatieren.

Texteditor (CSS-Datei)	
<code>td { font-family: Arial; }</code>	Schriftart Arial wird für jede Tabellenzelle genutzt
<code>td. Datum { background-color: blue; }</code>	Die Farbe blau wird nur für Zellen der Klasse „Datum“ verwendet.
<code>td. Preis { background-color: green; }</code>	Die Farbe grün wird nur für Zellen der Klasse „Preis“ verwendet.

Klassen eines Elementes werden durch einen Punkt, gefolgt vom gewünschten Klassennamen erzeugt.

CSS-Klassen nutzen

Im HTML-Code gibt man die CSS-Klasse mit dem Attribut `class` an.

Texteditor	Browser
<pre><table> <tr> <td class = "Datum" > 29.11.23</td> </tr> ... <tr> <td class = "Preis" 50,00 € </td> </tr> </table></pre>	

A3 Tabellen mit CSS formatieren II

- Erstelle eine HTML-Seite, auf der dein Stundenplan im Browser in Form einer Tabelle angezeigt wird.
- Erstelle eine CSS-Seite und verknüpfe sie mit der HTML-Seite aus a). Erzeuge darin mehrere CSS-Klassen, so dass jedes Fach in der Tabelle eine passende Hintergrundfarbe erhält.

Das Erstellen und Designen einer Website ist meistens ein großes Projekt. Um dabei die Übersicht zu behalten und eine Struktur zu schaffen, werden solche Projekte häufig in vier Phasen eingeteilt. Ein Projekt zeichnet sich durch einen Projektstart und ein Projektende aus.



P38043-014
Beispielwebsite

Projektanforderungen

Eure Website soll die folgenden Elemente beinhalten:

- ▶ eine Startseite mit den wichtigsten Informationen
- ▶ mehrere Unterseiten
- ▶ eine Navigationsleiste
- ▶ Bilder in geeigneter Größe
- ▶ Listen und Tabellen (➔ **Üben und Vertiefen**)
- ▶ Quellenangaben und Impressum



Es kann hilfreich sein, folgende vier Phasen zu durchlaufen:

PHASE 1

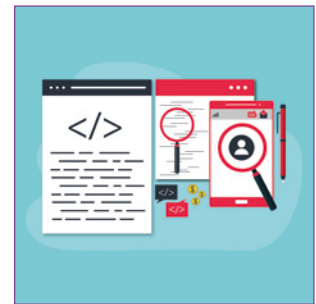
Definitionsphase

- ▶ Sammelt zunächst Ideen, über welches Thema ihr eine Website erstellen möchtet (z. B. Sportverein, ein gesellschaftliches oder politisches Thema).
- ▶ Notiert euch stichpunktartig die wesentlichen Inhalte eurer Website.

PHASE 2

Planungsphase

- ▶ Sammelt Vorschläge für das Layout und legt die Unterseiten der Website fest.
- ▶ Teilt die Aufgaben/Unterseiten in eurer Gruppe auf.
- ▶ Eventuell hilft es euch, die Struktur eurer Webseite zunächst handschriftlich aufzuzeichnen.
- ▶ Erstellt einen Zeitplan und prüft, ob das Projekt in der vorgegebenen Zeit zu schaffen ist.



PHASE 3

Durchführungsphase

- ▶ Setzt eure Planungen nun praktisch um, indem ihr sie in einen geeigneten HTML-Editor implementiert.
- ▶ Achtet darauf, eure Zwischenstände zu sichern.
- ▶ Haltet euch über den Projektfortschritt auf dem Laufenden.

PHASE 4

Abschluss

- ▶ Dokumentiert und präsentiert eure Ergebnisse.
- ▶ Bewertet und reflektiert eure Ergebnisse. Kontrolliert, ob ihr all eure Vorstellungen umsetzen konntet.

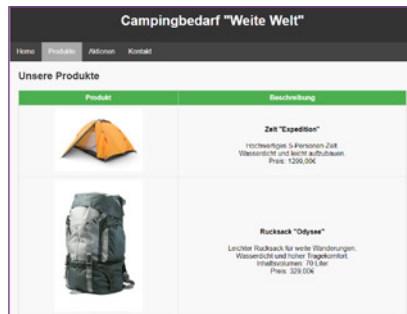
Projektideen für die eigene Website

Ihr habt keine gute Idee für eure eigene Website? Dann könnt ihr die folgenden Themenvorschläge als Grundlage für euer Projekt nutzen.

Campingwebsite

Camping ist in den letzten Jahre wieder in Mode gekommen. Die richtige Ausrüstung ist dabei entscheidend. Im Internet gibt es deshalb ein großes Angebot an Produkten. Eine Website für Campingbedarf sollte Folgendes enthalten:

- ▶ Einteilung der verschiedenen Produkte in Kategorien (z. B. Zelte, Rucksäcke, Kleidung, Zubehör)
- ▶ Bilder und eine Auflistung der Produkteigenschaften (z. B. Wasserfestigkeit oder Stabilität)
- ▶ Naturbilder auf allen Seiten



VORSCHLÄGE

Historie der eigenen Stadt

Viele Städte haben eine lange Geschichte. Gerade für die Einwohner ist die Historie ihrer Stadt ein sehr interessantes Thema. Eine Website über die Geschichte einer Stadt sollte u. a. folgende Inhalte haben:

- ▶ Historische Bilder der Stadt mit besonderen Sehenswürdigkeiten
- ▶ wichtige historische Ereignisse mit den dazugehörigen Jahreszahlen und einer kurzen Beschreibung der Ereignisse
- ▶ berühmte Einwohner (ggf. mit einem Steckbrief)



Modetrends

Die Mode ist stetig im Wandel und verändert sich von Jahr zu Jahr. Dabei ist es nicht immer einfach, genau den Trend im Blick zu behalten. Eine Website, welche die neusten Trends vorstellt, kann sehr informativ sein. Sie sollte Folgendes beinhalten:

- ▶ Modeartikel und Tipps und Ideen für Outfits
- ▶ die Geschichte der Mode
- ▶ DIY-Modeprojekte
- ▶ Fashion-News



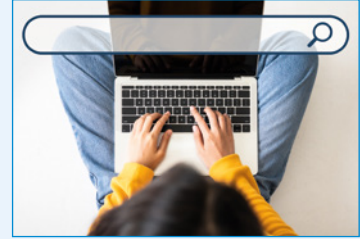
Website gestalten und designen

Das Gestalten einer Website mit HTML besitzt Grenzen. Für das Designen und Layouten von Webseiten nutzt man CSS (Cascading Style Sheets → Kapitel). Je nachdem, wie fit ihr im Umfang mit CSS seid, könnt ihr eure Webseite mit oder ohne CSS erstellen.

EINSTIEG

Jeden Tag wächst die Anzahl der Menschen, die über einen Zugang zum Internet verfügen. Auch die Nutzungszeiten und Anwendungsmöglichkeiten nehmen immer weiter zu.

- ▶ Welche konkreten Auswirkungen hätte es auf dein Leben/das Leben anderer Menschen, wenn es ab morgen kein Internet mehr geben würde?

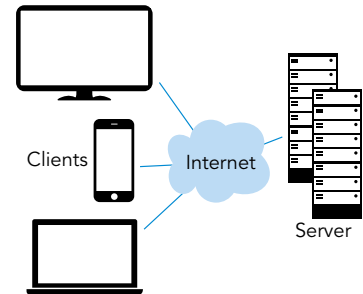


ERARBEITUNG

interconnected networks (engl.): zusammenschaltete Netzwerke

Was genau ist eigentlich das Internet?

Das **Internet** wird häufig auch das „Netz der Netze“ genannt und ist ein weltweites Computernetzwerk, das in den 1960er-Jahren in den Vereinigten Staaten entwickelt wurde. Heute ist das Internet inhaberlos. Einzelne Unternehmen oder Organisationen können einen eigenen Teil des Netzes verwalten und Nutzende können selbst Inhalte veröffentlichen.



A1 Internet nutzen

Die heutige Kommunikation unterscheidet sich sehr stark gegenüber früheren Zeiten, als es weder Computer noch Smartphones noch Internet gab. Vergleiche die Kommunikation von früher und heute. Nenne dabei Vor- und Nachteile.

Internetdienste

World Wide Web (engl.): weltweites Netz

Der Begriff **World Wide Web** (kurz: **WWW**) wird häufig fälschlicherweise mit dem Internet gleichgesetzt. Das World Wide Web ist ein Internetdienst und umfasst nur einen kleinen Teil des Internets, nämlich Webseiten mit Links und Multimedia-Inhalten. Das Internet bietet u. a. noch folgende weitere Dienste an:

Elektronische Post (E-Mail) @

Diskussionsforen und Chat

File Transfer Protocol (engl.): Dateiübertragungsprotokoll

Datenaustausch über FTP (File Transfer Protocol) FTP



Internet-Telefonie über VoIP (Voice over Internet Protocol) VoIP

Voice over Internet Protocol (engl.): Sprachübertragung über das Internetprotokoll

Fernsehen (Livestreams oder Video-on-Demand)

Internetradio

Die genannten Internetdienste sind eigenständig, funktionieren zugleich und es kommt häufig vor, dass Internetnutzer nur Teile des Internets in ihrem Alltag nutzen.

A2 Internetdienste

Recherchiert in Partnerarbeit Informationen für ein kurzes Referat zu einem der folgenden Internetdienste, das ihr anschließend in eurer Klasse präsentiert:

FTP

Secure Shell

Terminalsdiens

E-Mail

Instant Messenger

Cloud-Dienst

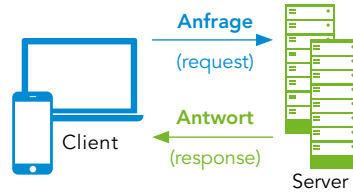
Videostreaming

Soziales Netzwerk

Online-Spiel

Client, Server, Service

Die Kommunikation zwischen Netzwerkkomponenten funktioniert nach dem **Client-Server-Prinzip**. Der Client braucht etwas und stellt deshalb eine Anfrage (= **request**) an einen **Server**. Der Server antwortet (= **response**) auf die Anfrage des Clients.



Server: Dienstleister
Client: Kunde
Service: Dienst

Ein **Server** stellt für alle, die Zugang zu ihm haben, etwas zur Verfügung. Im Internet gibt es unzählige Server.

A3 Das Client-Server-Prinzip

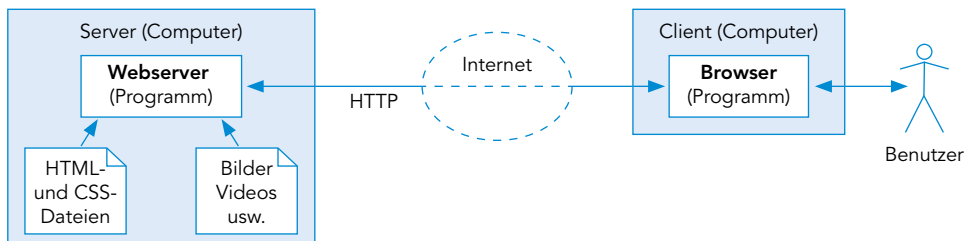
Erkläre das Client-Server-Prinzip am Beispiel eine Webseitenaufrufes.

Entwicklung des World Wide Web

Das **World Wide Web** wurde Anfang der 1990er Jahre von Tim Berners Lee und Robert Cailliau am CERN in Genf entwickelt. Sie wollten die Informationen ihrer Forschungseinrichtung, die auf vielen verschiedenen Computern verteilt waren, besser zugänglich machen. Berners Lee erfand dazu den (Hyper)link sowie den **Webserver**, ein Programm, das die Dateien einer Webseite zur Verfügung stellt. Er programmierte den ersten Browser und entwarf das Protokoll HTTP, das die Kommunikation zwischen Webserver und Browser beschreibt sowie die Sprache HTML. Statt dieses System nur für das CERN zu entwickeln, nutzte sein „Web“ das Internet, das zu dieser Zeit etwa zehn Jahre alt war. So konnten Texte in einem weltweiten Netzwerk miteinander verknüpft werden.

CERN: Europäische Organisation für Kernforschung

HTTP: hypertext transfer protocol



Das CERN entschied, das Protokoll HTTP lizenzfrei zu veröffentlichen. So konnten Universitäten und Unternehmen kostenfrei eigene Webserver und Browser entwickeln. Dadurch verbreitete sich das World Wide Web in wenigen Jahren sehr schnell, so dass heute (2024) mehr als die Hälfte der Weltbevölkerung das Web nutzt.

A4 Zeitstrahl erstellen SPRACHE

Stelle die Entwicklung des WWW mithilfe eines Zeitstrahls dar.

Das **Internet** ist ein weltweites Netzwerk aus kleineren Computernetzwerken. **Server** stellen Dienste zur Verfügung, **Clients** nutzen diese. Als **Dienst** bezeichnet man Anwendungen, an der viele Computer beteiligt sind, wie z. B. E-Mail oder das **World Wide Web**.

Letzteres ermöglicht die Verknüpfung von Texten (oder allgemein Inhalten) weltweit.

Webserver stellen Webseiten zur Verfügung.

MERKE


1 Erkläre den Unterschied zwischen dem Internet und dem World Wide Web.

AUFGABEN

- 1 HTML-Elemente werden genutzt, um Inhalte auf einer Website passend zu platzieren.

- Beschreibe, wie man in HTML Überschriften definiert.
- Erläutere, was man unter `<head>` bzw. `<body>` versteht.
- Nenne das Element zum Erzeugen eines Zeilenumbruchs.

Erstelle eine Übersicht wichtiger HTML-Elemente. Deine Übersicht soll u. a. Überschriften, `<head>` und `<body>` sowie Listen und Bilder enthalten.

- 2 Erstelle eine HTML-Seite mit folgendem Inhalt. Finde eine passende Überschrift und überprüfe dein Ergebnis im Browser. 

Browser

- 5x Weltmeister:
Brasilien
- 4x Weltmeister:
Deutschland, Italien
- 3x Weltmeister:
Argentinien
- 2x Weltmeister:
Frankreich, Uruguay
- 1x Weltmeister:
England, Spanien

Browser

- Seestraße
 - Farbe: pink
 - Preis: 140
- Opernplatz
 - Farbe: rot
 - Preis: 240
- Schlossallee
 - Farbe: blau
 - Preis: 400

- 3 Öffne die hinterlegte HTML-Datei mit einem Texteditor.

- Rücke den Code korrekt ein.
- Speichere die Datei ab und öffne sie in einem Browser.
- Erläutere die Bedeutung von `<meta charset="UTF-8">`.

- Zeichne die Baumstruktur der HTML-Datei und rücke den Code korrekt ein.
- Erläutere die einzelnen Bestandteile des HTML-Codes.
- Zeichne die ungefähre Darstellung der Seite im Browser in dein Heft. Überprüfe dein Ergebnis anschließend, indem du die Datei im Browser öffnest.



P38043-030
Mediencode

- 4 Bei der Erstellung von Webseiten muss das Copyright beachtet werden. Begründe jeweils, ob folgendes erlaubt ist:

Du möchtest folgendes Zitat von Albert Einstein auf deiner Website veröffentlichen: „Es ist schwieriger, eine vorgefasste Meinung zu zertrümmern als ein Atom.“

Du hast eine Website und möchtest, dass man dort dein Lieblingslied anhören kann. Dazu fügst du einen Verweis auf die Seite eines öffentlichen Radiosenders ein, wo das Lied zur Verfügung gestellt wird.

SPRACHE

5 Die Bilddatei „Katze.jpg“ hat eine Größe von 3 600 × 2 700 Pixeln und braucht 6 MB Speicherplatz. Sie soll auf einer Webseite neben Text (nicht als Hintergrund) verwendet werden.

- Erläutere, wie man mit der Datei umgehen sollte.
- Die Bilddatei befindet sich in einem Unterordner „bilder“. Gib den HTML-Code zum Einbinden der Bilddatei in einer angemessenen Größe an.
- Nenne weitere Dateiformate für Bilder, die im World Wide Web üblicherweise zum Einsatz kommen.



6 Auf einer Webseite soll das abgebildete Logo mit der URL <https://www.ccbuchner.de> verlinkt werden.

- Nenne die Bedeutung der Abkürzung URL.
- Erläutere die einzelnen Bestandteile der angegebenen URL unter Verwendung der entsprechenden Fachbegriffe.
- Das Logo liegt als Bilddatei in einem Unterordner „bilder“ und hat den Dateinamen buchner.png. Die verlinkte Seite soll sich in einem neuen Browser-Tab öffnen. Gib die Codierung des verlinkten Bildes in HTML an.



7 Tabellen sind ein wichtiger Bestandteil von HTML-Seiten.

<table> neue Tabelle
 <tr> neue Zeile in der Tabelle
 <td> neue Zelle in der jeweiligen Zeile

Texteditor			Browser								
<pre><table border=1> <tr> <td>Zelle 1</td> <td>Zelle 2</td> <td>Zelle 3</td> </tr> <tr> <td>Zelle 4</td> <td>Zelle 5</td> <td>Zelle 6</td> </tr> </table></pre>			<table border="1"> <tr> <td>Zelle 1</td> <td>Zelle 2</td> <td>Zelle 3</td> </tr> <tr> <td>Zelle 4</td> <td>Zelle 5</td> <td>Zelle 6</td> </tr> </table>			Zelle 1	Zelle 2	Zelle 3	Zelle 4	Zelle 5	Zelle 6
Zelle 1	Zelle 2	Zelle 3									
Zelle 4	Zelle 5	Zelle 6									

<table border=1> führt dazu, dass auch die Tabellenlinien angezeigt werden. 1 ist die Liniendicke und kann variiert werden.

a) Erstelle eine HTML-Datei und lasse folgende Sätze in einer Tabelle darstellen.

Anna spielt Fußball

Alejo geht schwimmen

Melek liebt Tennis

Jeder Satz soll in einer Zeile stehen und jede Zelle nur ein Wort enthalten.

b) Recherchiere, wie man einer Tabelle eine Kopfzeile hinzufügt. Ergänze in deiner Tabelle aus a) eine Kopfzeile. Trage darin passende Wörter zum Beschreiben der Sätze ein.

c) Bilde deinen Stundenplan in einer HTML-Datei ab. Verwende eine Tabelle mit Kopfzeile.

Stunde	Montag
1	Politik
2	Politik
3	Spanisch
4	Spanisch
5	Sport
6	Sport

8 Fortsetzung von ↪ Aufgabe 6

Arbeite weiter mit deinem Stundenplan aus Aufgabe 6c.

`style="background-color: red"` gibt HTML-Elementen die Hintergrundfarbe Rot.

<code><table style="background-color: blue"></code>	Tabelle mit Hintergrundfarbe
<code><tr style="background-color: green"></code>	jeweilige Zeile mit Hintergrundfarbe
<code><td style="background-color: yellow"></code>	jeweilige Zelle mit Hintergrundfarbe

- a) Farben können mit den englischen Wörtern oder im RGB-System eingegeben werden. Öffne den hinterlegten Link und mische dir für jedes Schulfach eine Farbe deiner Wahl. Notiere dir jeweils die Farben in folgendem Format.

`rgb(200,200,200)` `rgb(225,180,36)` `rgb(150,190,60)` `rgb(195,20,60)`

- b) Verschönere deinen Stundenplan, indem du die in a) gewählten Farben als Hintergrundfarben für die verschiedenen Schulfächer verwendest.

9 Fortsetzung von ↪ Aufgabe 7

Für eine Website existieren bereits die HTML-Seiten `HTML.html`, `CSS.html`, `Javascript.html`, `PHP.html` und `SQL.html`.

- a) Erstelle eine HTML-Seite `index.html` für die Seite „Home“. Diese soll die folgende Tabelle zur Navigation beinhalten.

Home	HTML	CSS	Javascript	PHP	SQL
------	------	-----	------------	-----	-----

- b) Ändere die Hintergrundfarben, damit die Tabelle wie folgt aussieht.

Home	HTML	CSS	Javascript	PHP	SQL
------	------	-----	------------	-----	-----

- c) Füge Links ein, damit man per Klick auf die jeweilige Seite gelangt.

- 10 a) Bilder können durch das Copyright oder durch Creative-Commons-Lizenzen geschützt sein. Erläutere den Unterschied.

- b) Gib die Bedeutung der folgenden Abkürzungen für Creative Commons Lizenzen an. Wenn du dir unsicher bist, recherchiere ggf. im Web.

`CC BY-SA` `CC BY-SA-NC` `CC BY-ND`

- c) Du hast ein Foto deiner Klasse gemacht. Erläutere rechtlichen Aspekte, die du beachten musst, wenn du das Foto auf einer Webseite veröffentlichen möchtest.
- d) Du hast ein Bild mit einer Suchmaschine gefunden und möchtest es in deiner Webseite benutzen. Nenne mögliche Voraussetzungen, unter denen das erlaubt ist.

- 11 a) Gib eine Definition des Begriffs „World Wide Web“ an und grenze ihn vom Begriff „Internet“ ab.

- b) Recherchiere, welche Personen an der Entwicklung des World Wide Web beteiligt waren. Erstelle eine Tabelle (z. B. als HTML-Seite), die die wichtigsten Entwicklungsschritte und die zugehörige Person zeigt.

Das große Info-Quiz!

Hier sprechen Begriffe dieses Kapitels über sich selbst. Die Zahlen in Klammern geben den Buchstaben im erratenen Begriff an, den du für das Lösungswort brauchst.

1. „Ich kann die Struktur einer HTML-Seite darstellen.“ (1)
2. „Ich bearbeite HTML-Seiten, bevor sie im Browser dargestellt werden.“ (10)
3. „Ich bin eine Weiterentwicklung des ASCII-Codes.“ (5)
4. „Ich beinhalte eine riesige Zahl an Webseiten.“ (1)
5. „Ich bilde zusammen mit meinem Freund „Client“ ein wichtiges Prinzip des Internets.“ (1)
6. „Ich bin der Fachbegriff für einen Bildpunkt.“ (4)
7. „Ich kann vieles sein – z. B. WWW, E-Mail oder FTP.“ (5)



P38043-031
Info-Quiz

- 1 a) Erstelle eine HTML-Seite mit mindestens zwei verschiedenen Typen von Überschriften und einem manuellen Zeilenumbruch.
 - b) Gib der Seite einen Titel.
 - c) Lasse die Seite in einem Browser anzeigen.
- 2 Erstelle eine HTML-Seite, welche im Browser die rechts abgebildete Aufzählung zeigt.
- 3 Du sollst auf einer HTML-Seite mehrere Bilder darstellen. Beschreibe die Ordnerstruktur, die du dafür anlegst. Nenne den HTML-Befehl, der ein Bild mit einer Breite von 1024 Pixel einfügt.
- 4 a) Erstelle eine HTML-Seite, in der du die Überschriften der ersten sieben Doppelseiten dieses Kapitels als unnummerierte Liste aufzählst.
 - b) Erstelle für jeden der Listenpunkte eine Unterseite. Fasse darin die wesentlichen Erkenntnisse der jeweiligen Themen in deinen Worten zusammen.
 - c) Verlinke die Unterseiten mit der Seite aus a).
- 5 a) Grenze die Begriffe World Wide Web und Internet voneinander ab.
 - b) Gib drei Anwendungen an, die zum Internet aber nicht zum World Wide Web zählen.

Browser

1. Überschriften
 - h1
 - h2
2. Bilder
 - Bilder einfügen
 - Anzeigegröße
 - Bildbearbeitung
3. Navigation
 - Links

Ich kann ...	In Aufgabe	Hilfe
Überschriften und Zeilenumbrüche in HTML umsetzen und das Ergebnis mit einem Browser überprüfen.	1	1.1
nummerierte und unnummerierte Listen erzeugen.	2, 4	1.3
Bilder in eine HTML-Seite einbinden und sie in der gewünschten Größe anzeigen lassen.	3	1.4, 1.5
mehrere HTML-Seite verlinken.	4	1.6, 1.7
die Begriffe WWW und Internet voneinander abgrenzen.	5	1.9

HTML-Code ↪ 1.1, 1.2, 1.3

Mit HTML werden Dokumente erzeugt, die von Browsern dargestellt werden. HTML-Code ist in einzelne Elemente unterteilt, die mit einem Baumdiagramm veranschaulicht werden können.

Texteditor	Browser
<pre><body> <h1> Hauptüberschrift </h1> <p> Einfacher Text
 Text nach Zeilenumbruch </p> <h2> Abschnitt </h2> <p> Einfacher Text </p> <h3> Unterabschnitt </h3> <p> Einfacher Text </p> </body></pre>	<p>Hauptüberschrift</p> <p>Einfacher Text Text nach Zeilenumbruch</p> <p>Abschnitt</p> <p>Einfacher Text</p> <p>Unterabschnitt</p> <p>Einfacher Text</p>

Bilder auf Webseiten anzeigen ↪ 1.4, 1.5

Bilddateien werden in einem Unterordner gesammelt. Zu beachten sind Dateigröße, Anzeigegröße und Bildrechte.

HTML-Code:

```

```

Website Planeten	Das Sonnensystem
<ul style="list-style-type: none"> planeten.html <ul style="list-style-type: none"> bilder <ul style="list-style-type: none"> jupiter.jpg venus.png 	<p>Diese Webseite stellt einige Planeten vor.</p> <p>1. Die Venus</p> 

Links und Navigation ↪ 1.6, 1.7

Mit Links kann man beliebige Webseiten mit der eigenen verknüpfen. Mit einer Navigation werden mehrere Teilseiten der Webseite verlinkt.

<https://de.wikipedia.org/wiki/HTML>

Protokoll Domainname Pfad

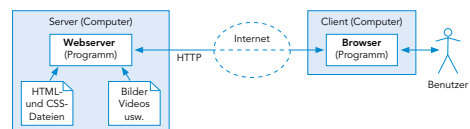
Grundlagen in CSS ↪ 1.8, 1.9

Während im HTML-Code der Inhalt einer Webseite codiert wird, wird die Darstellung des Inhalts mit CSS formatiert. Mit CSS-Klassen kann man HTML-Elemente unterschiedlich formatieren.

Texteditor (CSS-Datei)	Browser						
<pre>table { border-collapse: collapse; } td { border-style: solid; border-width: 2 px; border-color: grey; padding: 5px; }</pre>	<table border="1"> <tr> <td>29.11.23</td> <td>Fußball</td> <td>30,00 €</td> </tr> <tr> <td>01.12.23</td> <td>Schuhe</td> <td>50,00 €</td> </tr> </table>	29.11.23	Fußball	30,00 €	01.12.23	Schuhe	50,00 €
29.11.23	Fußball	30,00 €					
01.12.23	Schuhe	50,00 €					

Das World Wide Web ↪ 1.10

Der Begriff Internet bezeichnet das Netzwerk, das Computer auf der ganzen Welt miteinander verbindet. Das World Wide Web ist die Gesamtheit aller über das Internet aufrufbaren Webseiten.

**FACHBEGRIFFE**

Hier findest du die wichtigsten Begriffe aus diesem Kapitel:

HTML	Dateiformat	Bildbearbeitungsprogramm	Client-Server-Prinzip
Browser	Urheberrecht	Link	Internet
Texteditor	Creative-Commons-Lizenz	URL	World Wide Web
Baumstruktur	Recht am eigenen Bild	Navigation	Internetdienst
Zeichensatz	Pixel		

Verschlüsselungs- methoden

2

Einstieg

Wie kann man geheime Informationen geheim halten? Im modernen Informationszeitalter wird es immer schwieriger, bestimmte Informationen zu verschlüsseln und vor unbefugtem Zugriff zu schützen.

- ▶ Finde Situationen, in denen es wichtig ist, Informationen zu schützen.
- ▶ Nenne mögliche Verschlüsselungen, die du aus den Jahrgangsstufen 5/6 bereits kennst.

Am Ende dieses Kapitels hast du gelernt, ...

- ▶ was man unter dem Begriff „hacken“ versteht.
- ▶ welche unterschiedlichen Verschlüsselungsmethoden es gibt.
- ▶ worauf es bei modernen Verschlüsselungsmethoden ankommt.

EINSTIEG



P38043-015

Grafik zum Lagebericht des BSI

Das Bundesamt für Sicherheit in der Informationstechnik erstellt jährlich einen Bericht zur Lage der IT-Sicherheit in Deutschland. In der hinterlegten Grafik wird dieser Bericht in einer Grafik zusammengefasst.

- Verschaffe dir damit einen Überblick über Bedrohungen, die gerade aktuell sind.



Bundesamt
für Sicherheit in der
Informationstechnik

ERARBEITUNG

Auch sogenannte Whistle-Blower verschaffen sich (zum Teil illegal) Zugriff auf Daten, wobei ihre Absicht aber das Bloßstellen unlauterer bzw. krimineller Machenschaften ist.

pen: Abk. für penetration (engl. für Eindringen in Informatiksysteme)

Hacker und Pentester

Während **Hacking** ursprünglich dafür steht, Lösungen für knifflige Probleme (durch Programmierung von Computern) zu finden, wird der Begriff heute meist für das illegale Eindringen in Informatiksysteme verwendet. Dabei können z. B. Daten gestohlen oder die Verfügbarkeit eines Systems außer Kraft gesetzt werden. Hinter Hacking-Angriffen stehen unterschiedliche Absichten, u. a. Bereicherung durch Diebstahl oder Erpressung, Manipulation der öffentlichen Meinung, Behinderung eines Gegners in Konflikten oder Kriegen, Spionage und manchmal auch einfach Abenteuerlust.

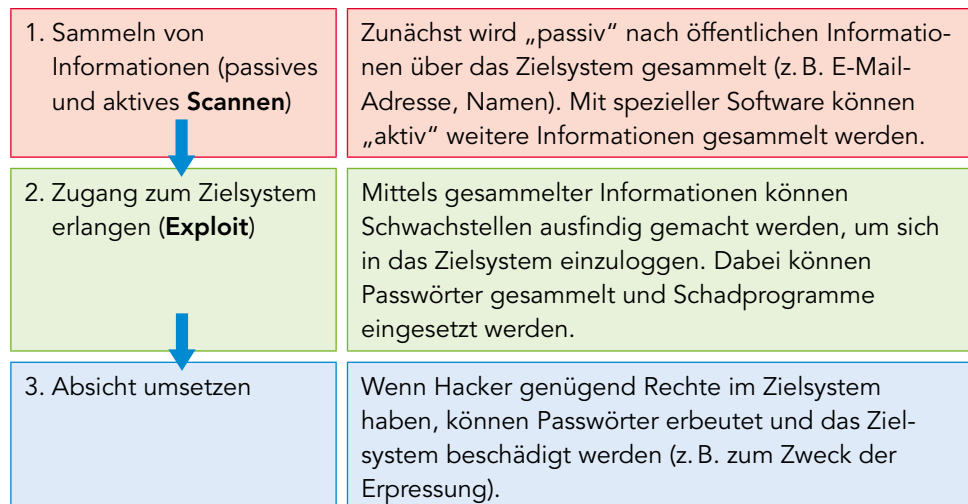
Hacker müssen nicht kriminell sein: **Pentester** werden von Unternehmen engagiert, um gezielt nach Schwachstellen in der Sicherheit ihrer Informatiksysteme zu suchen, damit Sicherheitslücken geschlossen werden können.

A1 Pentester beschreiben 

Recherchiere im Web und erstelle eine kurze Beschreibung des Berufs „Pentester“.

Ablauf eines Hacks

Das Eindringen in ein Informatiksystem, um sich z. B. Zugang zu Daten zu verschaffen oder anderen Schaden anzurichten, geschieht in der Regel in drei Phasen:



Da Hacking illegal ist, macht man sich durch aktives Scannen bereits strafbar.

to exploit: ausnutzen (von Schwachstellen)

A2 Passiv nach Informationen scannen  SPRACHE

- Nenne Daten über Schulangehörige (Namen, E-Mailadressen), die auf der Webseite deiner Schule zu finden sind.
- Ermittle, z. B. mit dem Browser-Plugin Wappalizer, welche Softwarepakete der Webserver deiner Schule verwendet.

Passwörter „erbeuten“

Ein großer Teil von Hacking-Aktivitäten zielt auf das Ermitteln von Zugangsdaten. Informatiksysteme müssen prüfen, ob ein Benutzer das richtige Passwort eingegeben hat. Sie speichern aber so gut wie nie die Passwörter selbst, denn dann hätte ein Hacker, der eine Liste von Passwörtern findet, sehr leichtes Spiel.

Stattdessen wird eine **Hashfunktion** verwendet. Damit wird jedem beliebigen Passwort eine Zeichenkette (der „Hashwert“) zugeordnet, die üblicherweise gleich lang ist, egal wie lang das Passwort ist:


Passwort	Hashwert (MD5)
Marienkäfer2000	d4db139e605347949a3348ace5356be9
Passwort123	fe6fa98138ffab6339e4adeee157538c

Man kann aus einem Hashwert das ursprüngliche Passwort nicht einfach wiederherstellen. Man kann nur prüfen, ob ein eingegebenes Passwort den gleichen Hashwert produziert. Wenn Hacker eine Liste mit Hashwerten erbeuten, haben sie daher nur die Möglichkeit einer **Brute-Force-Attacke**, d. h. mögliche Passwörter nacheinander auszuprobieren. Dazu verwenden sie Listen häufig benutzter Passwörter. Ein simples Passwort kann so nach einigen Stunden ermittelt werden, für ein sicheres Passwort würde diese Methode Jahrhunderte benötigen.

A3 Passwörter und Hashwerte verknüpfen

- Recherchiere und erkläre die Brute-Force-Attacke.
- Recherchiere nach einer Liste mit häufig genutzten Passwörtern.
- Erzeuge die MD5- bzw. SHA-Hashwerte einiger der unter b) gefundenen Passwörter mithilfe eines Generators.

Mit **Hacking** bezeichnet man das unbefugte Eindringen in Informatiksysteme. **Pentester** werden häufig von Firmen engagiert, um Sicherheitslücken in Systemen aufzudecken. Hacking geschieht in mehreren Phasen, zu denen **Scannen** und **Exploits** gehören. Um in Systeme einzudringen, werden Passwörter benötigt, die mithilfe von **Hashfunktionen** sicher gespeichert und nur durch **Brute-Force-Attacken** geknackt werden können.

- Recherchiere und halte ein kurzes Referat zu einem der folgenden Themen bzw. Begriffe aus a), b) oder c). 

- Stelle die Geschichte eines Hacking-Angriffs vor (eine Liste bekannter Angriffe findest du hinterlegt).
- Begriffe aus dem Bereich Hacking:
 - Privilege Escalation • Social Engineering • Phishing • Malware, z. B. Virus oder Trojaner • Botnetz • DDOS
- Schutzmaßnahmen gegen Hacking-Angriffe:
 - Passwortrichtlinien • Single Sign On • Zwei-Faktor-Authentifizierung • Klassifizierung von Informationen in Sicherheitsstufen • Mitarbeitersensibilisierung, z. B. „Think before you click“ • Principle of least privilege • Netzwerksegmentierung • Firewall • Patch-Management (hält Software in Systemen auf dem neuesten Stand) • SIEM (Security Information and Event Management) • Pentesting

Der deutsche Begriff für Hashfunktion ist „Streuwertfunktion“.

Als Hashfunktion werden heute meist MD5 (message digest algorithm) und SHA (secure hash algorithm) verwendet.



P38043-016

MD5- und SHA-Generatoren

MERKE

AUFGABEN



P38043-017

Liste bekannter Hacking-Angriffe

EINSTIEG

Pakitas Eltern haben wichtige Bankdokumente digitalisiert und abgespeichert. Jedoch sorgen sie sich, dass diese Dokumente möglicherweise jemand anderes einsehen könnte oder die Dateien bei einem Hackerangriff verschwinden könnten.



- ▶ Mache Pakitas Eltern Vorschläge, wie sie ihre Dokumente schützen könnten.

ERARBEITUNG

Schutz vertraulicher Daten

Vertraulichkeit von Daten ist nicht nur Geheimdiensten vorbehalten. Jeder Mensch hat Daten, auf die nicht jeder Zugriff haben sollte, wie zum Beispiel Kontoauszüge oder Unterlagen über ärztliche Behandlungen. Die Sicherheit solcher Daten muss bei deren Aufbewahrung und Versendung gewährleistet sein.



A1 Daten schützen

Nenne mindestens fünf verschiedene Daten, die deiner Meinung nach schützenswert sind.

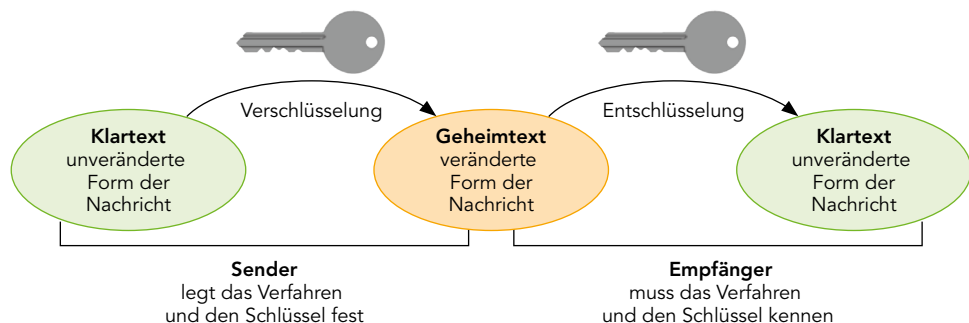
Verschlüsselung von Daten

Kryptographie stammt von den griechischen Wörtern *kryptós* (verborgen, geheim) und *gráphein* (schreiben).

Kryptographische Verfahren, die den gleichen Schlüssel zum Ver- und Entschlüsseln benutzen, nennt man „symmetrisch“.

Es gibt auch asymmetrische Verfahren, die Schlüsselpaare verwenden. Dabei wird ein Teil des Paares zum Verschlüsseln, der andere zum Entschlüsseln benutzt.

Kryptographie ist eine Wissenschaft, die sich mit Verschlüsselungen beschäftigt. Um die Vertraulichkeit und Sicherheit von Daten zu gewährleisten, können Verschlüsselungsverfahren genutzt werden. Bei einem solchen Verfahren wird ein sogenannter **Klartext** in einen **Geheimtext** umgewandelt. Für die Ver- und Entschlüsselungen ist der passende **Schlüssel** notwendig.

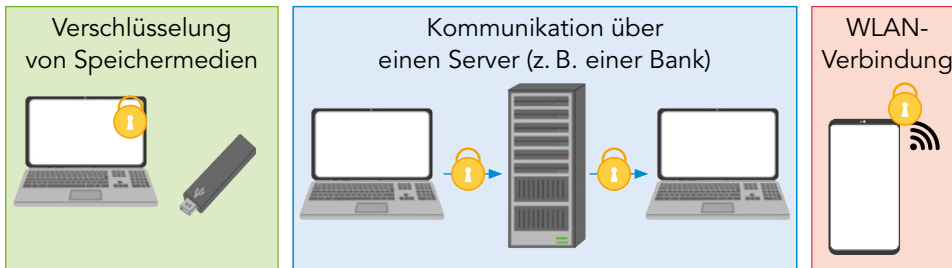


A2 Schlüssel übertragen

- E-Mails sind keine sichere Kommunikationsmöglichkeit. Du möchtest eine verschlüsselte Datei per E-Mail an einen Freund oder eine Freundin schicken. Erkläre Möglichkeiten, dieser Person den Schlüssel gefahrlos mitzuteilen.
- Luca meint: „Wenn mein Weg, den Schlüssel zu übertragen, sicher ist, dann kann ich auch alle Nachrichten über diesen Weg übertragen.“ Beurteile Lucas Aussage.

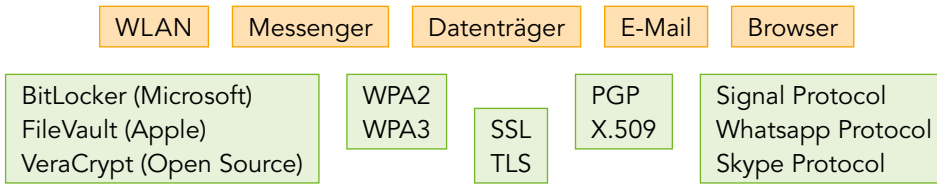
Anwendungen von Verschlüsselungstechnologie

Verschlüsselungen werden in vielen Situationen eingesetzt, in denen Daten digital gespeichert und übertragen werden:



Die Art der Verschlüsselung hängt dabei vom Anwendungsfall ab. Die Sicherheit einer Verschlüsselung hängt jedoch immer von der Anzahl der möglichen Schlüsselkombinationen ab. Die Nutzung des Internets würde ohne Verschlüsselung nicht funktionieren.

A3 Verschlüsselungstechnologien zuordnen



Kryptographie beschäftigt sich mit Methoden, Daten zu **verschlüsseln**, um deren Vertraulichkeit zu schützen. Eine Verschlüsselung wandelt **Klartext** mithilfe eines **Schlüssels** in einen **Geheimtext** um. Die Originaldaten können nur mithilfe des passenden **Schlüssels** wiederhergestellt werden können.

MERKE

- 1 a) Wähle dich mit einem Endgerät, z. B. deinem Handy, in ein WLAN ein. Prüfe und nenne die verwendete Verschlüsselungsmethode.
- b) Recherchiere die Verbesserungen der Sicherheit bei der WPA3-Methode gegenüber der WPA2-Methode.
- c) Recherchiere und erkläre die Rolle eines Radius-Servers im Zusammenhang mit der Verschlüsselung eines WLANs.
- 2 a) Viele Messenger-Dienste verwenden eine „Ende-zu-Ende-Verschlüsselung“. Recherchiere und erkläre diese Verschlüsselungsmethode.
- b) Erläutere auf Grundlage deiner Recherche, wie sich Ende-zu-Ende von der Verschlüsselung zwischen Browser und Webserver unterscheidet.
- 3 Bei modernen Verschlüsselungsverfahren ist das automatisierte Durchprobieren aller Schlüssel die einzig mögliche Angriffsmethode. Gehe von einem modernen PC aus, der rund 2 Milliarden Schlüssel pro Sekunde testen kann. Berechne die Zeit, die zum Testen aller Schlüssel benötigt wird:
 - a) Der Schlüssel besteht aus sieben Kleinbuchstaben.
 - b) Der Schlüssel besteht aus acht Großbuchstaben.
 - c) Der Schlüssel besteht aus acht Zeichen (Klein- und Großbuchstaben und die Ziffern von 0 bis 9).

AUFGABEN

Verschlüsselungen werden seit Jahrtausenden eingesetzt, um vertrauliche Nachrichten zu schützen. Heutige Verfahren sind sehr komplex, aber sie beruhen in ihren Grundlagen auf historischen Verfahren. Um sich an digitale Kryptographie heranzutasten, ist es daher nützlich, sich zuerst mit älteren, einfachen Verfahren zu beschäftigen.

Arbeitet für die folgenden Projekte in Zweiergruppen. Probiert einige der vorgestellten Verfahren mit Papier und Bleistift aus, indem ihr jeweils eine kurze Botschaft an eure Partnerin bzw. euren Partner verschlüsselt, und die erhaltene Nachricht entschlüsselt.



P38043-018

Bastelvorlage Skytale

Skytale

Diese Geheimschrift entstand vor ca. 2500 Jahren in der griechischen Stadt Sparta. Die Skytale ist ein achtkantiger Stab, um den früher ein Leder- oder Pergamentstreifen gewickelt wurde.

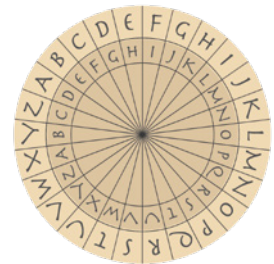
Die Nachricht wird der Länge nach auf den umwickelten Stab geschrieben. Wenn der beschriftete Streifen abgewickelt wird, ergeben die Zeichen keinen Sinn mehr.



Verwende als Ersatz für eine echte Skytale einen dicken Buntstift und anstatt eines Lederstreifens einen schmalen Streifen Papier (eine Kästchenbreite).

Cäsar-Verschlüsselung

Bei dieser Methode, die z. B. von Julius Cäsar angewendet wurde, wird jedem Buchstaben ein anderer Buchstabe zugeordnet. Man schreibt unter das Alphabet für den Originaltext ein weiteres Alphabet für den Geheimtext, das um einige Stellen verschoben ist. Jeden Buchstaben des Originaltextes ersetzt man dann durch den entsprechenden Geheimbuchstaben. Beispiel:



Originalalphabet: **A**BCDEFGHIJKLMNOPQRSTUVWXYZ

Geheimalphabet: DEFGHIJKLMNOPQRSTUVWXYZ**A**BC

Aus „MORGEN UM ACHT“ wird der Geheimtext „PRUJHQ XP DFKW“.

Um das Verfahren zu unterstützen kann man eine Drehscheibe mit zwei Alphabeten verwenden.



P38043-019

Bastelvorlage
Cäsar-Scheibe

Geheimschrift mit Zitronensaft

Wenn man Zitronensaft mit etwas Zucker mischt, erhält man eine Geheimtinte. Mit einem Federhalter (oder einem Wattestäbchen) schreibt man damit eine Botschaft auf Papier. Sobald die „Tinte“ getrocknet ist, ist sie unsichtbar.

Der Empfänger der Botschaft kann sie durch Erhitzen, z. B. im Ofen oder mit einem Bügeleisen wieder sichtbar machen.

Freimaurer-Geheimschrift

Diese Geheimschrift wurde vermutlich schon im Mittelalter von jüdischen Rabbis und den Tempelrittern, später dann von den Freimaurern benutzt. Jedem Buchstaben des Alphabets wird ein Zeichen zugeordnet, das sich aus dem abgebildeten Schema ergibt: **┘** wird für A verwendet, **┐** für B usw. **┘┐┘┐┘┘┘┘┘┘┘┘** codiert beispielsweise das Wort „FREIMAUER“.

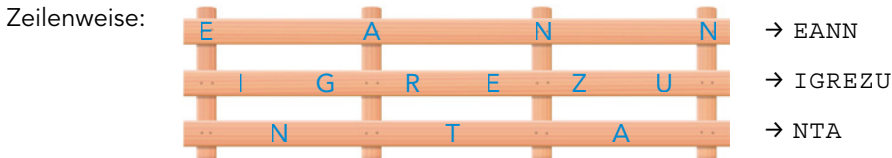
A	B	C	J	K	L
D	E	F	M	N	O
G	H	I	P	Q	R
T	S	U	X	W	Y
	V			Z	

Gartenzaun

Die Buchstaben der Botschaft werden zickzackartig auf mehrere Zeilen geschrieben: der erste Buchstabe auf die oberste Zeile, der zweite auf die zweite Zeile, usw. Wenn man die unterste Zeile erreicht hat, geht es wieder nach oben. Leerzeichen werden weggelassen. Anschließend wird der Text Zeile für Zeile zusammengefasst und hintereinandergeschrieben.

Beispiel mit drei Zeilen

Originaltext: EIN GARTENZAUN



Geheimtext: EANNIGREZUNTA

Internationales Signalbuch

Das internationale Signalbuch ist ein weltweit akzeptierter Standard für die Kommunikation in der Seefahrt. Es ist nicht geheim, hat aber die Eigenschaften einer Geheimschrift. Signale wie „Vorsicht, wir haben Taucher im Wasser“ werden durch Buchstaben codiert. Die Buchstaben können auf verschiedene Weise übertragen werden, z. B. durch Flaggen-, Funk- oder Lichtsignale.

Stellt euch vor, dass ihr Kapitäne zweier Schiffe seid, von denen eins Schwierigkeiten hat und das andere um Hilfe bittet. Stellt eine „Unterhaltung“ der beiden Kapitäne mithilfe der Signale zusammen, die ihr im Signalbuch findet.



P38043-020

Internationales Signalbuch
(Auszug)

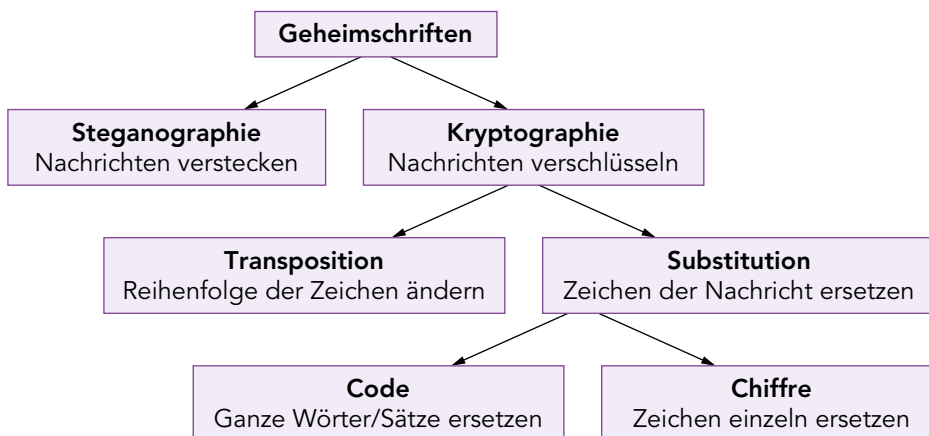
Geheimschriften recherchieren

Recherchiert weitere Geheimschriften und probiert sie aus:

Atbash, die Geheimschrift Karls des Großen, das Alphabetum Kaldeorum

Geheimschriften einordnen

Geheimschriften lassen sich in folgende Struktur einordnen:



Entscheide für die von euch durchgeführten Verschlüsselungen, ob es sich um eine Methode der Steganographie, eine Transposition, einen Code oder eine Chiffre handelt.

EINSTIEG

Du hast einen geheimen Text erhalten, von dem du nicht weißt, wie er verschlüsselt wurde.

- Beschreibe Möglichkeiten, um die Verschlüsselung zu knacken und an die geheime Botschaft zu gelangen.



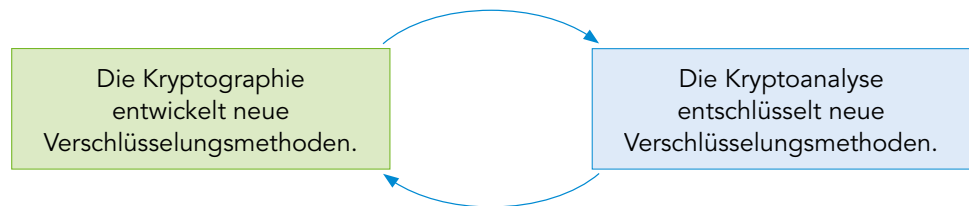
ERARBEITUNG



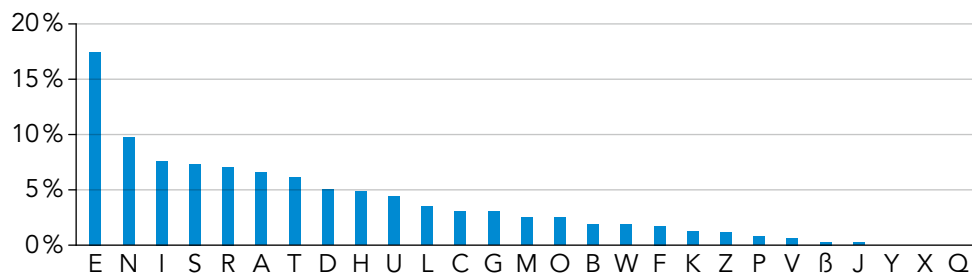
Maria Stuart

Die Häufigkeitsanalyse

Wenn jemand Geheimnisse hat, gibt es auch Personen, die diese Geheimnisse erfahren möchten: Maria Stuart, Königin von Schottland, verschlüsselte ihre Briefe, in denen sie einem Attentat auf ihre Cousine, Königin Elisabeth I. zustimmte. Diese Briefe wurden später entschlüsselt und Maria Stuart wurde zum Tode verurteilt. Geheimschriften entwickeln sich in einem Wechselspiel von Kryptographie und **Kryptoanalyse**:



Die erste wesentliche Methode der Kryptoanalyse wurde von dem arabischen Wissenschaftler Ya'qūb al-Kindī (800–873 n. Chr.) entwickelt. Dabei untersuchte er Texte anhand ihrer Buchstabenhäufigkeit.



Buchstabenhäufigkeit in deutschen Texten

Die Buchstaben ä, ö, ü werden wie ae, oe, ue gezählt; β als eigenes Zeichen.

Mit der **Häufigkeitsanalyse** lassen sich Geheimtexte entschlüsseln. Wenn zum Beispiel in einem Text, der mit Cäsar verschlüsselt wurde, Q der häufigste Buchstabe ist, liegt es nahe, dass Q im Original dem E entspricht.

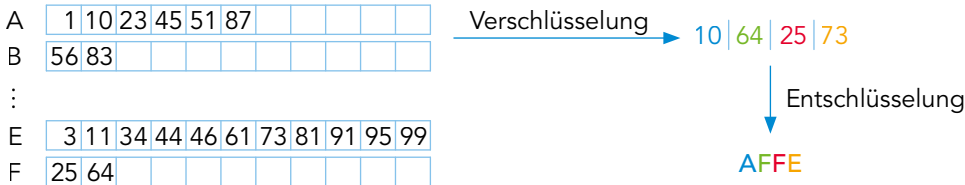
A1 Häufigkeiten analysieren

Entschlüssele den folgenden Geheimtext mithilfe einer Häufigkeitsanalyse. Es handelt sich dabei um eine Cäsar-Verschlüsselung – Schlüssel unbekannt.
 QMPMQUBMFBM SVIKSMV QAB UIVKPUIT TMQKPBZ ITA UIV LMVSB

Erschweren der Häufigkeitsanalyse

Die Entdeckung der Häufigkeitsanalyse machte auf einen Schlag viele Verschlüsselungsmethoden nutzlos. Eine Lösung bestand darin, häufigen Buchstaben (z. B. E) mehrere Geheimzeichen, sogenannte **Homophone** zuzuordnen. Beim Verschlüsseln wird dann jedes Mal ein Homophon zufällig ausgewählt. Man könnte beispielsweise die 26 Buchstaben auf 100 Zahlen von 0 bis 99 aufteilen. Je häufiger ein Buchstabe dabei vorkommt, umso mehr Zahlen erhält dieser.

Die „Große Chiffre“ von Ludwig XIV, ein Zahlen-Code, war sicher gegen die Häufigkeitsanalyse.



A2 Texte mit Homophonen verschlüsseln

Erstelle eine Tabelle, in der du jedem Buchstaben des Alphabets eine oder mehrere Zahlen zwischen 0 und 99 zuordnest. Nutze die Übersicht der Buchstabenhäufigkeit, um die Zahlen so zu verteilen, dass jede Geheimzahl etwa gleich oft im Geheimtext vorkommt.

Die **Kryptoanalyse** entwickelt Methoden, um verschlüsselte Botschaften ohne Kenntnis des Schlüssels zu entschlüsseln.

Eine solche Methode ist die **Häufigkeitsanalyse**, mit der man über die statistische Häufigkeit von Buchstaben die Bedeutung von Geheimzeichen erraten kann.

Die Verwendung von **Homophonen** erschwert die Häufigkeitsanalyse.

MERKE

1 Der folgende Geheimtext wurde mit dem Cäsar-Verfahren verschlüsselt. Knacke den Text mithilfe der Häufigkeitsanalyse:

ZLOYBYL, XU CWB OHYLZUBLYH OHX VYMWBXCXYL QUL UFM BYONY,
 BUNNYH GYCHY BIYWBMNY UWBNOHA UHXLY FYONY.
 MJUYNL NLUZ CWB UOZ XYL QYCYX UOMMYL GCL HIWB GYBL EUYFVYL,
 OHX HOH MWBUYNT CWB, MITOMUAYH, YLMN GCWB MYFVYL.

AUFGABEN

2 Öffne den hinterlegten, mit Symbolen verschlüsselten Text. Darin ist die Entschlüsselung schwieriger als bei einer Cäsar-Verschlüsselung. Überlegt in Partnerarbeit, mit welchen Mitteln man auch hier die Verschlüsselung brechen kann und entschlüsselt den Text. 👥



P38043-021

Kryptogramm für Aufgabe 2

3 Begründe, warum es nicht möglich ist, den folgenden Text mit der Häufigkeitsanalyse zu entschlüsseln:



4 Man kann die Häufigkeitsanalyse erschweren, indem man sich für jeden Buchstaben eine Zufallszahl ausdenkt. Dieser Buchstabe wird dann um die entsprechende Zahl verschoben. Der neue Buchstabe wird zur Verschlüsselung genutzt. Verschlüssele damit die Nachricht „TREFFEN AM SEE UM ZWEI!“ mit den folgenden Zufallszahlen: 6, 2, 9, 4, 8, 1, 7, 5, 3, 10, 2, 6, 9, 8, 4, 7, 1, 5

EINSTIEG

Obwohl mit der Häufigkeitsanalyse einfache Verschlüsselungen wie Cäsar gebrochen werden konnten, wurden diese trotzdem weiter verwendet. Erst mit dem Aufkommen der Telegrafie im 19. Jahrhundert, mit der ständig verschlüsselte Nachrichten versendet wurden, entstand der Bedarf für sicherere kryptographische Verfahren.



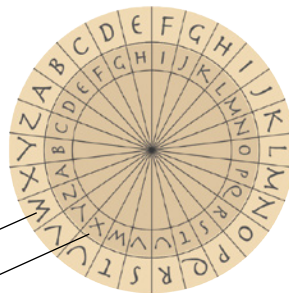
- Finde Gründe, warum man telegraphierte Botschaften verschlüsseln musste.

ERARBEITUNG

Die dargestellte Cäsar-Scheibe dient zur Verschlüsselung von Texten mit der Verschiebung um jeweils 3 Buchstaben.

Entwicklung der polyalphabetischen Substitution

Bei einer monoalphabetischen Verschlüsselung ordnet man jedem Buchstaben aus einem **Klartextalphabet** einen Buchstaben aus dem **Geheimtextalphabet** zu.



Klartextalphabet
Geheimtextalphabet

Verschlüsselungsverfahren	Jeder Buchstabe wird um einen festgelegten Wert im Alphabet nach vorne verschoben. Dadurch wird z. B. der Klartextbuchstabe A zum Geheimbuchstaben D.
Schlüssel	ein festgelegter Wert (Cäsar verwendete den Schlüssel 3.)

Das Verfahren und der Schlüssel müssen vor der Verschlüsselung festgelegt werden und sowohl Sender als auch Empfänger bekannt sein. So ist es möglich, Informationen vor unbefugten Personen zu schützen. Für „INFORMATIK“ ergibt sich im Beispiel:

Klartext	I	N	F	O	R	M	A	T	I	K
Verschlüsselung um 3 Stellen	L	Q	I	R	U	P	D	W	L	N

Schlüssel 3 bedeutet, dass jeder Buchstabe um 3 Stellen im Alphabet verschoben wird.

A1 Wie die Römer verschlüsseln

- Verschlüsse das Wort „ROEMERLAGER“ mit dem Schlüssel 3.
- Der folgende Satz ist mit Cäsar (Schlüssel: 4) verschlüsselt: „HMI KEPPMIV WMRH EYJ AMPHWGLAIMRNEKH“. Ermittle den Klartext.

Bei einer **polyalphabetischen** Substitution werden mehrere Geheimalphabete genutzt. Eine der ältesten Ideen ist die Alberti-Verschlüsselung. Dabei nutzt man abwechselnd zwei verschiedene Schlüssel. Beispiel für Cäsar:

Klartextalphabet	ABCDEF ³ FGHIJKLMNOPQRS ¹⁵ TUVWXYZ
1. Verschiebung (Schlüssel: 3)	DEF ³ GH ³ IJKLMNOPQRSTUVWXYZABC
2. Verschiebung (Schlüssel: 15)	PQRSTUVWXYZABCDEF ¹⁵ GH ¹⁵ IJKLMNO

Beim ersten Buchstaben wird der erste Schlüssel verwendet, beim zweiten Buchstaben der zweite Schlüssel. Danach wird immer abgewechselt.

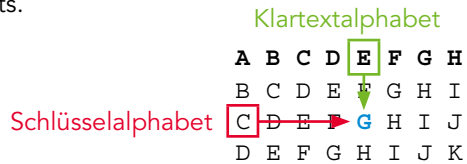
A2 Alberti-Verschlüsselung knacken

Durch Spionage konnte eine geheime Botschaft abgefangen werden, welche mit Alberti verschlüsselt wurde: UFJQVUHKQIDPJ. Die Kryptologen fanden außerdem heraus, dass die Schlüssel 3 und 15 sind. Entschlüsse die Nachricht.

Verschlüsseln mit Vigenère

Blaise de Vigenère entwickelte eine weitere polyalphabetische Verschlüsselung. Dabei legt ein Schlüsselwort fest, um wie viele Stellen ein Buchstabe eines Geheimtextes zur Verschlüsselung verschoben wird. Um einen Text mit dem **Vigenère-Verfahren** zu verschlüsseln, muss das Codewort zunächst wiederholt unter den Text geschrieben werden. Buchstabe für Buchstabe verschlüsselt man dann den Text mithilfe des nachfolgend rechts abgebildeten Vigenère-Quadrats.

Klartext **E**INVERSTANDEN
 Schlüsselwort **C**ODECODECODEC
 Geheimtext **G**WQZGFVXCBGIP



P38043-022

Vigenère – Schritt für Schritt und Vigenère-Quadrat

Vigenère entwickelte im 16. Jahrhundert dieses Verfahren. Es stellt eine Weiterentwicklung der Alberti-Methode dar.

A3 Vigenère-Chiffre ausprobieren

Verschlüsselt jeweils eine Botschaft mithilfe des Vigenère-Verfahrens. Nutzt für die Verschlüsselung ein „Vigenère-Quadrat“. Übergebt eurer Partnerin bzw. eurem Partner den Geheimtext und das Schlüsselwort, um die Botschaft zu entschlüsseln.

Varianten der Vigenère-Methode

Die Autokey-Verschlüsselung wurde ebenfalls von Vigenère entwickelt. Statt das Schlüsselwort zu wiederholen, wird es bei diesem Verschlüsselungsverfahren nur einmal aufgeschrieben und um den Klartext ergänzt.

Klartext	E	I	N	V	E	R	S	T	A	N	D	E	N
Schlüsselwort	C	O	D	E	E	I	N	V	E	R	S	T	A
Geheimtext				Z	I	Z	F		E	E		X	

A4 Autokey-Verschlüsselung nutzen

- a) Nutze das Vigenère-Quadrat, um den vollständigen Geheimtext anzugeben.
- b) Verschlüsse den Klartext TREFFEN UM DREI mit der Autokey-Verschlüsselung. Nutze ein selbst gewähltes Schlüsselwort.



P38043-023

Autokey-Chiffre

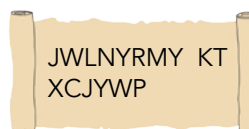
Bei einer **monoalphabetischen** Verschlüsselung ordnet man jedem Klartextbuchstaben aus einem Klartextalphabet einen festen Buchstaben aus dem Geheimtextalphabeten zu. Für **polyalphabetische** Verschlüsselungen (wie z.B. der **Vigenère-Verschlüsselung**) werden mehrere Geheimtextalphabete verwendet.

MERKE

1 Begründe, warum man einen mit Vigenère verschlüsselten Text nicht wie bei der Cäsar-Verschlüsselung mit der Häufigkeitsanalyse knacken kann.

AUFGABEN

2 Die folgende Botschaft konnte abgefangen werden. Eine Analyse ergab das Schlüsselwort SCHLOSS. Es ist jedoch unklar, welche Vigenère-Methode verwendet wurde. Entschlüssele die Nachricht und nenne die genutzte Vigenère-Methode.



Vigenère oder Autokey

EINSTIEG

Betrachte die folgende Geheimbotschaft.
 VHVS SP QUCE MRVBV BBB VHVS URQ
 GIBDU GRNICJ QUCE RVUAX SSR

- Kannst du ein Muster erkennen?



ERARBEITUNG

le chiffre indechiffable (franz.):
 die unknackbare Geheimschrift



Charles Babbage (1791–1871)
 erfand neben seinen Beiträgen
 zur Kryptographie auch
 den ersten programmierbaren
 Computer, die Analytical
 Engine.

Berechnen der Vigenère-Verschlüsselung

Die Methode von Vigenère wurde die unknackbare Chiffre genannt. Etwa 200 Jahre lang galt sie als sicher. Doch im 19. Jahrhundert entwickelten der englische Mathematiker Charles Babbage und der preußische Kryptoanalytiker Friedrich Wilhelm Kasiski unabhängig voneinander ein Verfahren, mit dem sich Vigenères Verschlüsselung unter bestimmten Voraussetzungen sogar recht leicht knacken lässt. Da Babbage seine Entdeckung geheim halten musste, wurde die Methode „Kasiski-Test“ genannt.

A1 Vigenère-Kryptogramm entschlüsseln

Mit der Methode von Babbage bzw. Kasiski ermittelt man die Länge des Schlüsselwortes eines mit Vigenère verschlüsselten Textes. Nimm an, dass du bereits weißt, dass für den folgenden Text ein Schlüsselwort mit zwei Buchstaben benutzt wurde – der erste Buchstabe für die blauen, der zweite für die roten Buchstaben:

LNM LMISSJV XQSL KZJQ BMW SFVS ANM JZWIYMS
 ANM KTNMMS DTZGMN ENM SIJKMBQQHPJ AHPFBYMS
 SJQS UJVXKM SFVS ANM BQXAJV PMNV OIJOJZ JZXMQJAXMS
 MX JQMNJJB IIGMN LNM LMISSJV XQSL KZJQ

- Erkläre, wie du die Häufigkeitsanalyse einsetzen kannst, um Informationen über die beiden verwendeten Alphabetverschiebungen zu erhalten.
- Entschlüssele die Botschaft und gib das Schlüsselwort an.

Der Kasiski-Test

Mit dem **Kasiki-Test** kann die Länge des Schlüsselwortes der Vigenère-Verschlüsselung ermittelt werden. Dies beruht auf der Wiederholung häufiger Wörter, wie „der“, „die“ oder „das“. Bei einem längeren Text ist es wahrscheinlich, dass diese an einigen Stellen gleich verschlüsselt werden, da sich das Schlüsselwort an anderer Stelle wiederholt. Zum Beispiel wiederholt sich die Verschlüsselung des Wortes „ich“ nach 12, die des Wortes „Was“ nach 15 Buchstaben, weil das Schlüsselwort in beiden Fällen die gleiche Position hat:

Klartext: ICH DENK AN WAS ICH WILL SOWIE WAS MICH BEGLUECKT
 Schlüsselwort: MIT MITM IT MIT MIT MITM ITMIT MIT MITM ITMITMITM
 Geheimtext: UKA PMGW IG IIL UKA IQEX AHIQX IIL YQVT JXSTNQKDF
 12 Buchstaben 15 Buchstaben

Aus der Analyse des Geheimtextes kann man schließen, dass das Schlüsselwort 3 Buchstaben lang ist. Die Wiederholung kann nur entstehen, wenn sich das Schlüsselwort in beiden Fällen an der gleichen Stelle wiederholt. Das kann nur der Fall sein, wenn sich sowohl 12 wie 15 durch die Länge des Schlüsselwortes teilen lassen.

Allgemein ist das Vorgehen wie folgt:

① Man sucht mindestens zwei Wiederholungen im Geheimtext, die jeweils mindestens drei Buchstaben lang sind.

② Man zählt, nach wie vielen Buchstaben sich diese Wörter wiederholen.

③ Der größte gemeinsame Teiler (ggT) dieser Abstände ist vermutlich die Länge des Schlüsselwortes (auch ein kleinerer Teiler ist möglich).

④ Die Buchstaben des Geheimtextes teilt man in so viele Gruppen ein, wie das Schlüsselwort Buchstaben hat. Für jede dieser Gruppen wird der Buchstabe ermittelt, der am wahrscheinlichsten dem E entspricht.

⑤ Die Bedeutung der restlichen Geheimbuchstaben ergibt sich, da jede der Buchstabengruppen mit einer Alphabetverschiebung verschlüsselt wurde.

A2 Den Kasiki-Test anwenden

Öffne den hinterlegten, mit Vigenère verschlüsselten Text. Entschlüssele ihn mithilfe des Kasiki-Tests.



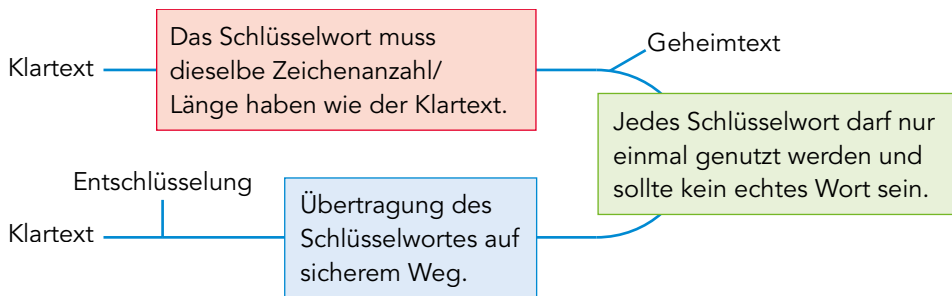
P38043-024

Geheimtext und Hilfestellung für A2

One-Time-Pad (Vernam-Chiffre)

1919 patentierte der Amerikaner Gilbert Vernam eine kryptographische Methode, von der mathematisch nachgewiesen ist, dass sie unmöglich geknackt werden kann. Man verwendet ein Schlüsselwort, das genauso lang ist wie die Botschaft selbst und aus zufällig gewählten Buchstaben besteht.

One-Time-Pads wurden im 20. Jahrhundert von Diplomaten und Geheimdiensten eingesetzt.



Mit dem **Kasiki-Test** kann man die Länge des Schlüsselwortes eines mit der Vigenère-Methode verschlüsselten Textes ermitteln. Basierend darauf kann man den Text durch mehrmalige Häufigkeitsanalyse entschlüsseln.

Ein **One-Time-Pad** ist ein Schlüsselwort, das aus zufälligen Buchstaben besteht, genauso lang ist wie die Botschaft und nur einmal verwendet wird.

MERKE

1 Ein weiteres Verfahren zum Brechen der Vigenère-Verschlüsselung ist die Auto-Korrelation. Informiere dich auf der hinterlegten Website über diese Methode und erstelle einen kurzen Steckbrief.

SPRACHE

2 Das von Vernam entwickelte One-Time-Pad ist zwar hundertprozentig sicher, aber das Verfahren hat auch gravierende Nachteile. Recherchiere die Verwendung von One-Time-Pads und erläutere entsprechende Nachteile.

AUFGABEN



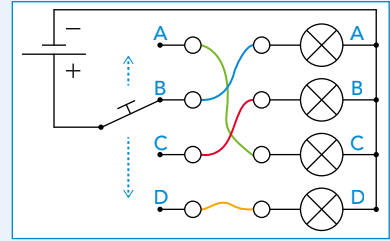
P38043-025

Aufgabe 1

EINSTIEG

Rechts ist eine elektrische Schaltung abgebildet.

- ▶ Was bedeuten die einzelnen Symbole?
- ▶ Wie fließt hier der Strom?
- ▶ Nimm an, dass man die farbigen Drähte in der Mitte der Schaltung unterschiedlich verknüpfen kann. Wie könnte man die Schaltung für eine Verschlüsselung einsetzen?



ERARBEITUNG

Die Entwicklung maschineller Verschlüsselung

Fortschritte in der Kryptoanalyse erforderten immer bessere Verschlüsselungsmethoden. Doch schon Vigenères Chiffre war mit Papier und Bleistift so zeitraubend, dass sie kaum in der Praxis eingesetzt wurde – und auch diese Methode erwies sich als unsicher.

1918 entwickelte Arthur Scherbius die **Enigma**. Die Enigma ist eine komplexe Chiffrenmaschine zur Verschlüsselung von Nachrichten. Im Gegensatz zu früheren Verschlüsselungen nutzt die Enigma Rotoren. Sie wurde von der Wehrmacht im Zweiten Weltkrieg eingesetzt. Die spannende Geschichte ihrer Entschlüsselung und ihr Name machten sie zur vielleicht bekanntesten Chiffriermaschine.



Die spannende Geschichte ihrer Entschlüsselung und ihr Name machten sie zur vielleicht bekanntesten Chiffriermaschine.

A1 Schlüssel täglich wechseln

Die deutsche Wehrmacht nutzte für die Entschlüsselung von Enigma-Nachrichten täglich geänderte Schlüssel. Erkläre die Bedeutung dieser Änderungen.

Der Aufbau

Die Enigma besteht aus einer Tastatur, einer Reihe von Walzen (Rotorwalzen), einem Steckbrett und einer Anzeigetafel. Diese Elemente ermöglichen die Verschlüsselung.

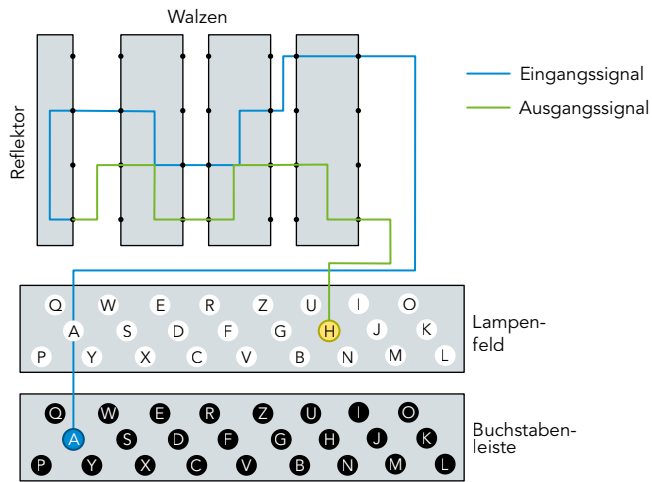
A2 Aufbau Enigma _____

- a) Recherchiere die Funktion der einzelnen Bestandteile einer Enigma, die in der Abbildung zu sehen sind.
- b) In der Abbildung sind die Reflektoren nicht zu sehen. Recherchiere deren Funktion in der Enigma.



Die Verschlüsselungstechnik

Jede Walze hat 26 Metallkontakte auf beiden Seiten, einen pro Buchstaben des Alphabets. Im Inneren sind diese Kontakte mit Drähten verbunden. Wenn ein Buchstabe auf der Tastatur gedrückt wird, wird der Strom durch die drei Walzen geleitet. Der Reflektor hinter der dritten Walze hat ebenfalls 26 Kontakte, aber nur auf einer Seite, von denen je zwei miteinander verdrahtet sind. Er leitet den Strom wieder zurück durch die drei Walzen und dann an das Lampenfeld, wo der chiffrierte Buchstabe aufleuchtet.



Damit die Buchstaben nicht immer gleich verschlüsselt werden, dreht sich die erste Walze nach jedem eingetippten Buchstaben eine Position weiter. Wenn die erste Walze sich 26-mal gedreht hat, dreht sich die zweite eine Position weiter, und wenn die sich einmal ganz herumgedreht hat, die dritte. So erzeugt die Enigma eine polyalphabetische Chiffre. Ein großer Vorteil der Enigma ist, dass sie auf die gleiche Art auch entschlüsselt. Wenn man einen Geheimtext eintippt, erscheint auf dem Lampenfeld der Originaltext.

Entschlüsselung der Enigma

Obwohl die Enigma zunächst völlig sicher zu sein schien, gelang es dem polnischen Mathematiker Marian Rejewski in den 1930er Jahren, die damalige Version der Enigma zu knacken. Die Enigma wurde jedoch verbessert, und mit dem deutschen Angriff auf Polen konnte er seine Arbeit nicht fortsetzen. Seine Forschungsergebnisse wurden aber an die Alliierten weitergegeben, so dass es dem Briten Alan Turing und seinen Mitarbeitern gelang, auch die späteren Versionen der Enigma zu entschlüsseln und so entscheidend zu einem früheren Ende des Zweiten Weltkriegs beizutragen.



Alan Turing (1902–1954) leistete wichtige Beiträge zur Entwicklung moderner Computer. Er gilt als einer der „Väter“ der Informatik.

Die **Enigma** ist eine elektrische Chiffriermaschine. Auf ihrer **Tastatur** wird der Originaltext oder der Geheimtext eingetippt. Die Buchstaben werden elektrisch mithilfe von drehbaren **Walzen** und einem **Reflektor** in andere Buchstaben umgewandelt und können auf einem **Lampenfeld** abgelesen werden.

MERKE

1 Arbeitet im Zweierteam. Hinterlegt findet ihr eine Bastelvorlage (mit Anleitung), auf der Walzen und Reflektoren der Enigma als Papierstreifen abgedruckt sind. Verschlüsselt damit jeweils eine Botschaft und lasst sie von der anderen Person entschlüsseln. 👤👤

2 Das Knacken der Verschlüsselung der Enigma hatte einen entscheidenden Einfluss auf den Verlauf des Zweiten Weltkrieges. Recherchiere wie es Alan Turing und seinem Team gelang, das Verschlüsselungsverfahren der Enigma zu entschlüsseln. Fasse deine Ergebnisse zusammen. 🖥️

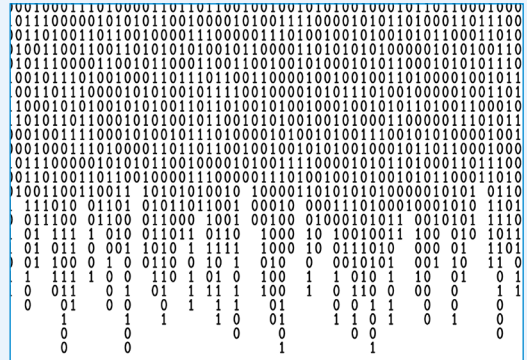
AUFGABEN



P38043-026
Aufgabe 1

EINSTIEG

Neben der Enigma wurden viele weitere Verschlüsselungsmaschinen gebaut. Eine davon ist die 1943 von Siemens & Halske entwickelte T43 mit dem englischen Codenamen „Thrasher“. Sie benutzte Lochstreifen für binär codierte Nachrichten und Schlüssel. Als Schlüssel war theoretisch ein One-Time-Pad möglich, womit die Verschlüsselung unmöglich zu brechen wäre.



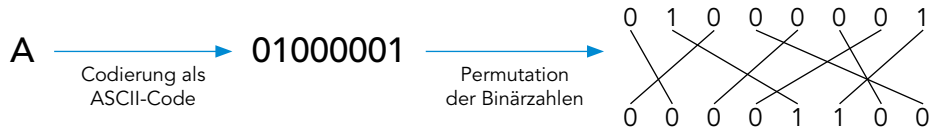
- ▶ Recherchiere die Geschichte dieser Maschine und erkläre die Verschlüsselungsmethode kurz.

ERARBEITUNG

Binärzahlen verschlüsseln

Ein Computer verarbeitet und speichert Daten mithilfe von Binärzahlen. Für einen Buchstaben braucht man im ASCII-Code z. B. eine achtstellige Binärzahl (acht Bits bzw. ein Byte). Moderne Verschlüsselungsmethoden verarbeiten Binärzahlen und wenden dabei Transpositionen und Substitutionen an.

Eine Transposition ist mathematisch eine sogenannte **Permutation**. Das folgende Beispiel zeigt die Permutation (2, 5, 1, 8, 3, 7, 4, 6) für eine achtstellige Bitfolge:



A1 Permutationen durchführen

- Beschreibe für obiges Beispiel, wie die Permutation durchgeführt wird.
- Bilde die Permutation (2, 4, 6, 8, 1, 3, 5, 7) der Binärzahl 1 1 0 0 1 1 0 0.

Transposition = Änderung der Reihenfolge der einzelnen Bits
 Substitution = Ersetzen von Bits durch andere

Für die Substitution von Binärzahlen wird in computergestützten Verschlüsselungen meist eine weitere Binärzahl als Schlüssel verwendet. Die zu verschlüsselnde Zahl und der Schlüssel werden mithilfe der **XOR-Operation** verrechnet. a XOR b ist 1, wenn entweder a oder b den Wert 1 hat, ansonsten ist a XOR b = 0 (siehe Tabelle).

XOR: exclusive or (ausschließendes oder bzw. „entweder – oder“)

a	b	a XOR b
0	0	0
0	1	1
1	0	1
1	1	0

Verschlüsselung

Zahl 1 1 0 0 1 0 0 1
 Schlüssel 1 0 1 0 1 0 1 0
 XOR
 Geheimtext 0 1 1 0 0 0 1 1

Entschlüsselung

Zahl 1 1 0 0 1 0 0 1
 XOR
 Schlüssel 1 0 1 0 1 0 1 0
 Geheimtext 0 1 1 0 0 0 1 1

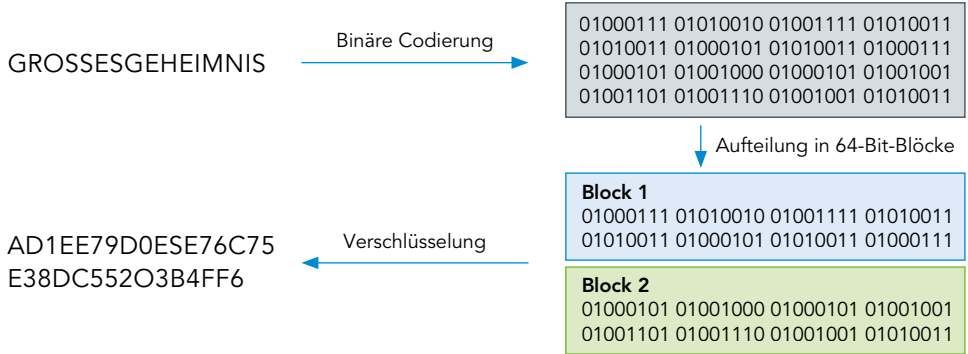
Man bildet für jede Stelle der zu verschlüsselnden Zahl und des Schlüssels das XOR. Der Schlüssel kann zufällig generiert oder eine vom Benutzer bestimmte Zahl sein.

A2 Binäre Transposition und Substitution anwenden

- Verschlüsse die Zahl 1 1 0 0 1 1 0 0 mit XOR und dem Schlüssel 1 0 0 1 0 0 1 0.
- Entschlüsse 1 0 1 1 1 0 0 0 mit XOR und dem Schlüssel 1 0 0 1 0 0 1 0.

Blockchiffren

Moderne Verschlüsselungsverfahren sind Blockchiffren. Mit ihnen verschlüsselt man nicht jeden Buchstaben einzeln, sondern mehrere Buchstaben gemeinsam. Die Grundlage für heutige Blockchiffren war der Data-Encryption-Standard (DES). Dieser nutzte zur Verschlüsselung einen 64 Bit langen Schlüssel. Dabei wird ein Text in 64-Bit-Blöcke eingeteilt – wenn ein Buchstabe 8 Bits benötigt, sind dies jeweils 8 Buchstaben.



Durch die immer stärker werdende Rechenleistung kann diese Verschlüsselung mit der Brute-Force-Methode gebrochen werden. Daher wird heute das **Advanced Encryption Standard (AES)** verwendet. AES ist heute die am häufigsten verwendete Verschlüsselungsmethode für digitale Daten.

A3 AES-Verfahren recherchieren

- a) Recherchiere Merkmale dieses Verfahrens. Gehe dabei auch auf die Schlüssellänge ein.
- b) Finde heraus, in welchen Bereichen AES eingesetzt wird.

Mit einer **Permutation** kann man binär codierte Nachrichten durch eine Transposition verschlüsseln. Eine Substitution kann mithilfe eines Schlüssels und der **XOR-Operation** durchgeführt werden.

Für eine **Blockchiffre** wird eine binär codierte Nachricht in Blöcke fester Länge (z. B. 64 Bit) geteilt, die dann jeweils als Block verschlüsselt werden. Der aktuelle Standard zur Verschlüsselung heißt **Advanced Encryption Standard (AES)**.

MERKE

1 Mithilfe von Permutation und Substitution lässt sich beispielhaft folgende Verschlüsselungsmethode konstruieren.

- ① Teile den Originaltext, der binär codiert ist, in 16-Bit-Blöcke ein. Falls für den letzten Block nicht genügend Bits übrig sind, fülle ihn mit Nullen auf.
- ② Wende auf jeden Block eine immer gleiche Permutation an: (4, 14, 10, 2, 16, 6, 7, 3, 1, 15, 13, 5, 8, 12, 9, 11)
- ③ Codiere ein Schlüsselwort als Binärzahl und nutze diesen als Schlüssel für die XOR-Operation.
 - a) Stelle die Botschaft „KIEL“ mit dem ASCII-Code als Binärzahl dar.
 - b) Verschlüsse sie mit der beschriebenen Methode und dem Schlüssel „IF“.
 - c) Entschlüsse folgenden Geheimtext mit dem Schlüssel „BV“, indem du die Substitution umkehrst und anschließend die Permutation rückgängig machst:
0 1 0 0 0 0 1 0 0 1 1 0 0 0 0 1 0 1 0 0 0 1 1 0 0 1 0 0 0 0 0 1

AUFGABEN

D	68	0100	0100
E	69	0100	0101
F	70	0100	0110
G	71	0100	0111
H	72	0100	1000
I	73	0100	1001
J	74	0100	1010
K	75	0100	1011
L	76	0100	1100

ASCII (Ausschnitt)

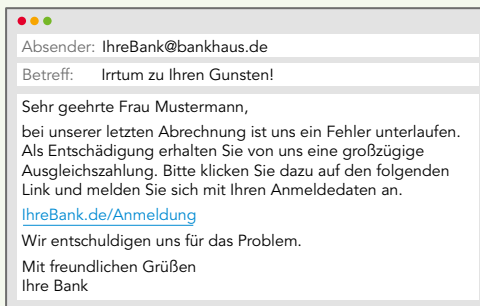
1 Verschlüsselungen gewährleisten die Sicherheit von Daten und sind heute unerlässlich.

- Erkläre den Unterschied zwischen einer monoalphabetischen und einer polyalphabetischen Verschlüsselung.
- Nenne und erkläre jeweils ein Beispiel.

- Gib die binäre Darstellung der Buchstabenfolge „IF“ (codiert mit ASCII) an.
- Wende die Permutation (16, 1, 15, 2, 14, 3, 13, 4, 12, 5, 11, 6, 10, 7, 9, 8) auf die Binärzahl aus Aufgabe a) an.
- Nach der Transposition wird die XOR-Operation angewendet. Erkläre den Vorteil dieses Vorgehens.

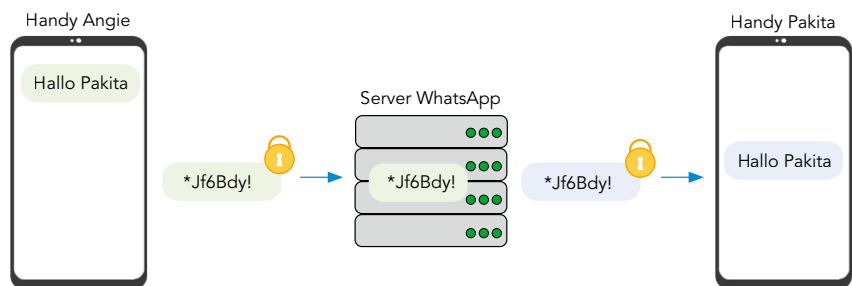
2 Hackerangriffe und deren Gefahren sind in den letzten Jahren immer häufiger geworden.

Silvia hat folgende E-Mail von ihrer Bank erhalten. Beurteile die Situation und gib Silvia Ratschläge.



- Erläutere die Gemeinsamkeiten und Unterschiede zwischen Hackern und Pentestern.
- Erläutere, wie ein Hacker mithilfe einer Liste von Hash-Werten Passwörter erbeuten kann.
- Liste die Phasen eines Hacks auf und erläutere diese kurz.

3 Die Ende-zu-Ende-Verschlüsselung ist eines der wichtigsten Verschlüsselungsverfahren im Bereich Social Media.



- Erkläre die obige Grafik und gehe dabei auf die einzelnen Schritte ein.
- Recherchiere die Datenschutzfunktionen von WhatsApp und erstelle eine Übersicht.

- Neben der Ende-zu-Ende-Verschlüsselung findet man auch die Punkt-zu-Punkt-Verschlüsselung. Informiere dich mit geeigneten Quellen über diese Verschlüsselungsmethode.
- Beurteile die Sicherheit der Punkt-zu-Punkt-Verschlüsselung gegenüber der Ende-zu-Ende-Verschlüsselung.

4 Vergleiche das Brute-Force-Verfahren mit der Häufigkeitsanalyse. Erläutere, in welchen Situationen welches Verfahren verwendet wird.

SPRACHE

5 a) Nutze die Vigenère-Verschlüsselung zur Verschlüsselung des Klartextes „ZAHLENSCHLOSS“ mit dem Schlüssel „CODE“.


b) Die geheime Botschaft „JIGOCIAIV“ wurde abgefangen. Durch Spionage konnte herausgefunden werden, dass der Schlüssel „TEIG“ lautet. Entschlüssele die abgefangene Nachricht.

c) Begründe die höhere Sicherheit im Vergleich zum Cäsar-Verfahren.

6 Valentina und Cem einigen sich darauf, ihre Kommunikation mit Morsezeichen zu verschlüsseln, indem sie einfach lange und kurze Signale vertauschen. So werden zum Beispiel U (.-) und G (--.) miteinander vertauscht.


- a) Entschlüssele die Nachricht ONGDTEEK.
- b) Begründe, dass die Gesamtzahl der für eine Nachricht zu sendenden Signale (kurze oder lange Impulse) durch diese Verschlüsselung gleich bleibt.
- c) Begründe, dass durch die Verschlüsselung in der Regel mehr Zeit benötigt wird, um die Nachrichten zu versenden.
- d) Begründe, warum diese Verschlüsselung nicht immer durchführbar ist.

7 a) Verschlüssele mit deiner Enigma eine beliebige Nachricht.

b) Tausche deinen Geheimtext mit einer anderen Person aus und entschlüssele deren Geheimtext. 


8 a) Erläutere, warum ein längeres Schlüsselwort die Vigenère-Methode sicherer macht.

b) Beschreibe, wie du ein beliebiges Buch einsetzen könntest, um eine Botschaft mit der Vigenère-Methode zu verschlüsseln. Dabei soll nur jemand, der über das gleiche Buch verfügt, die Botschaft wieder entschlüsseln können. Nenne den Schlüssel.

c) Recherchiere, warum man ein One-Time-Pad nur ein einziges Mal benutzen darf, um eine Entschlüsselung unmöglich zu machen. 

SPRACHE

9 Das Advanced Encryption Standard (AES) ist ein Verschlüsselungsverfahren, das zur sicheren Übertragung von Daten verwendet wird. Es basiert auf einer symmetrischen Blockchiffre. Sowohl der Sender als auch der Empfänger verwenden denselben Schlüssel. Das AES-Verfahren verwendet eine Netzwerkstruktur, bei der die Daten in Blöcke von 128 Bit aufgeteilt werden. Diese Blöcke werden dann durch eine Reihe von Operationen verschlüsselt. AES bietet verschiedene Schlüssellängen, nämlich 128, 192 und 256 Bit.

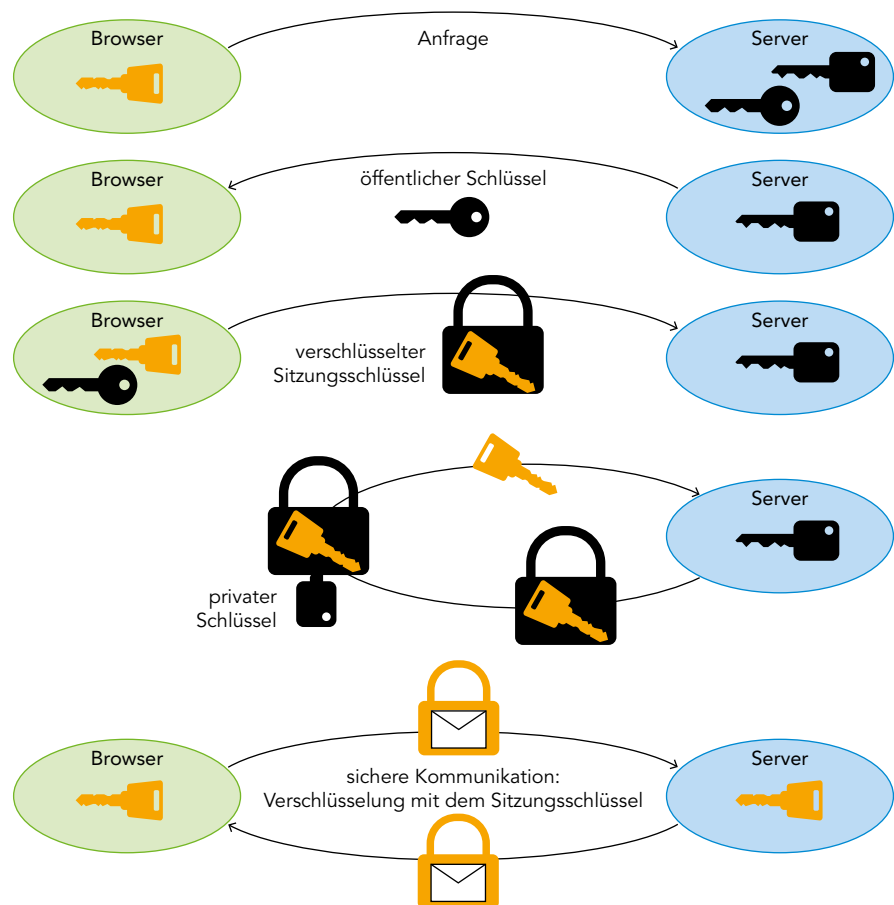
- a) Recherchiere, wie viele Schlüsselkombinationen es bei AES mit einer Schlüssellänge von 128 (192, 256) Bit gibt. Gib die Ergebnisse als Potenzen an. 
- b) Mit welcher dir bekannten Methoden könnte man einen Schlüssel der Länge 128 Bit knacken?

SPRACHE

10 Recherchiere und erläutere die Bedeutung von „Security through Obscurity“. Nenne und erkläre zudem kurz das passende Gegenkonzept.

HTTPS: Hypertext Transfer Protocol Secure

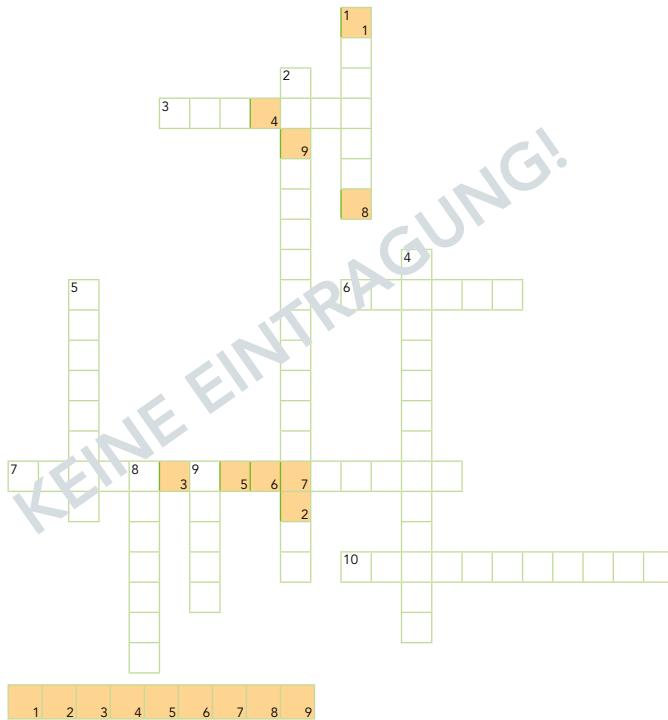
- 11 Neben der symmetrischen Verschlüsselung gibt es auch die Möglichkeit der asymmetrischen Verschlüsselung. Der große Unterschied dabei ist, dass für die Ver- und Entschlüsselung nicht der gleiche Schlüssel genutzt wird.
- Recherchiere den Begriff der asymmetrischen Verschlüsselung und erkläre diesen. Erstelle zur Veranschaulichung ein entsprechendes Schaubild.
 - Asymmetrische Verschlüsselungen kommen insbesondere bei der Verschlüsselung im Browser per HTTPS zum Einsatz. Dieses Verfahren wird durch das folgende Beispiel dargestellt. Erkläre das in der Grafik dargestellte Verfahren des Schlüsseltausches. Gehe hierzu auf alle gezeigten Schritte ein und achte jeweils auf die Rollen der privaten und öffentlichen Schlüssel.



- 12 Der Geheimtext „MNHOREGENAX“ ist durch das Cäsar-Verfahren entstanden – Schlüssel unbekannt. Knacke die Verschlüsselung durch die Brute-Force-Methode.
- 13 Der folgende Binärcode konnte abgefangen werden: 00001010. Er wurde mit der folgenden Permutation verschlüsselt: (3, 7, 4, 8, 1, 5, 2, 6). Mache die Permutation rückgängig und finde den zugehörigen Klartextbuchstaben (ASCII).

Das große Info-Quiz!

Öffne die hinterlegte Datei und löse das Rätsel.



P38043-027
Info-Quiz

1. Mit welcher Methode wurden vor 2500 Jahren in Griechenland Botschaften verschlüsselt?
2. Vigenère ist eine ... Substitution.
3. In dieser Phase des Hackings dringen Angreifer in ein Informatiksystem ein.
4. Die ... entwickelt Methoden, um Verschlüsselungen zu brechen.
5. Passwörter für Informatiksysteme werden als ... gespeichert.
6. Erfinder des One-Time-Pad
7. Umwandlung von Klartext in Geheimtext
8. Mit einer ... werden einzelne Zeichen einer Nachricht ersetzt.
9. Mit dem Kasiski-Test ermittelt man die ... des Schlüsselwortes.
10. Einen verschlüsselten Text nennt man auch ...

- 1 a) Erläutere die Bedeutung einer Hashfunktion und des Hashwertes.
b) Erkläre, warum man keine zu einfachen Passwörter nutzen sollte.
- 2 a) Verschlüsse die Botschaft „Ich habe es geschafft“ mit einer Cäsar-Verschlüsselung um 7 Stellen.
b) Verschlüsse die gleiche Botschaft mit der Vigenère-Chiffre und dem Schlüsselwort „INFO“.
- 3 a) Erläutere, wie du mit dem Kasiski-Test eine mit Vigenère verschlüsselte Botschaft entschlüsseln kannst.
b) Erläutere, was ein One-Time-Pad ist und warum diese Chiffriermethode nicht geknackt werden kann.
- 4 Erläutere Blockchiffre, Permutation und XOR-Operation an einem Beispiel.

Ich kann ...	In Aufgabe	Hilfe
den Begriff Hashfunktion und die Bedeutung von sicheren Passwörtern erläutern.	1	2.1
Substitutionsverfahren als Möglichkeit der Verschlüsselung verwenden.	2	2.5
verschiedene Verschlüsselungsverfahren unter Berücksichtigung von ausgewählten Sicherheitsaspekten beurteilen.	3	2.6
computergestützte Verschlüsselungsverfahren an Beispielen erläutern.	4	2.8

Bedrohung für die Sicherheit durch Hacking

↳ 2.1

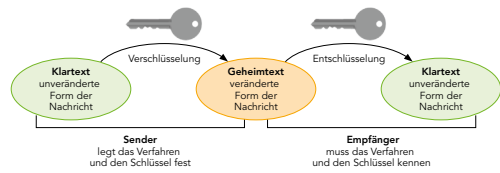
Das illegale Eindringen in Informatiksysteme wird als Hacking bezeichnet. Dieser Prozess kann in verschiedenen Phasen verlaufen. Häufig zielen Hacker auf Passwörter ab. Durch das Erbeuten von Hashwerten und eine Brute-Force-Angriffe können Passwörter ermittelt werden.



Verschlüsselung von Daten

↳ 2.2

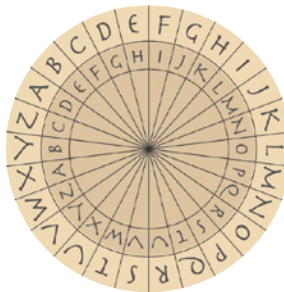
Der Sender verschlüsselt eine Nachricht mit dem Ziel, dass nur der Empfänger die Nachricht versteht. Dabei wird der Klartext einer Nachricht in einen Geheimtext verschlüsselt. Dadurch bleiben Daten geschützt.



Verschlüsselungsmethoden

↳ 2.5, 2.7, 2.8

Verschlüsselungsmethoden wie das Cäsar- oder Vigenère-Verfahren werden seit vielen Jahrhunderten verwendet. Im Laufe der Zeit entwickelten sich immer komplexere Verschlüsselungsmethoden, wie die Enigma oder Blockchiffren. Man unterscheidet zwischen mono- und polyalphabetischen Verschlüsselungsmethoden.

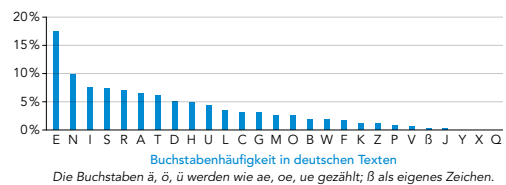


I	N	F	O	R	M	A	T	I	K
L	Q	I	R	U	P	D	W	L	N

Kryptoanalyse

↳ 2.6

Mit der Häufigkeitsanalyse und dem Kasiki-Test können mono- und polyalphabetische Verschlüsselungen geknackt werden.



FACHBEGRIFFE

Hier findest du die wichtigsten Begriffe aus diesem Kapitel:

Hacker
Pentester
Brute-Force
Kryptographie
Blockchiffre

Kryptogramm
monoalphabetisch
polyalphabetisch
Vigenère
Permutation

Kryptoanalyse
Kasiki-Test
One-Time-Pad
Enigma
XOR

AdobeStock / 7DesignUA – S. 14; - / jozeppe777 – S. 31; - / o_a – S. 15; - / VideoFlow – S. 35; - / ZKH studio – S. 40; akg-images – S. 27; Alamy Stock Photo / Bax Walker – S. 48; - / maximimages.com – S. 22; - / Peregrine – S. 8; - / Peter Probst – S. 18; - / Science History Images – S. 46, 49; - / Stephen Sweet – S. 49; - / True Images – S. 20; C.C.Buchner Verlag 2024 (mit KI generiert) – S. 21 (3), 42; Getty Images Plus / iStockphoto, AndreyPopov – S. 38; - / iStockphoto, Antony Robinson – S. 16; - / iStockphoto, bowie15 – S. 46; - / iStockphoto, Cindy_Giovagnoli – S. 16; - / iStockphoto, design56 – S. 27; - / iStockphoto, fizkes – S. 38; - / iStockphoto, GeorgiosArt – S. 42; - / iStockphoto, Givaga – S. 27; - / iStockphoto, Irina Nedikova – S. 7, 8, 23; - / iStockphoto, JoyImages – S. 28; - / iStockphoto, Katya_Havok – S. 27; - / iStockphoto, marchmeena29 – S. 28; - / iStockphoto, MriyaWildlife – S. 26; - / iStockphoto, MXW Photo – S. 11; - / iStockphoto, Mykyta Dolmatov – S. 56; - / iStockphoto, Nerthuz – S. 15, 34; - / iStockphoto, PeterHermesFurian – S. 41; - / iStockphoto, rootstocks – S. 50; iStockphoto / J J Osuna Caballero – S. 44; Shutterstock / SeventyFour – Cover; www.wikimedia.org – S. 36.

Mediencodes

S. 26

Getty Images Plus / iStockphoto, MriyaWildlife – P38043-014

Getty Images Plus / iStockphoto, martin-dm - P38043-014

Getty Images Plus / iStockphoto, Oleh Malshakov – P38043-014

Getty Images Plus / iStockphoto, Gabdulvachit Konurov – P38043-014