

Informatik auf der Sekundarstufe

Module für den Unterricht im 3. Zyklus, 3. Klasse



Inhalt

1	Einleitung.....	4
1.1	Übersicht	5
2	Daten 3: Modul «Fehlererkennende und -korrigierende Codes» (MI.2.1)	6
2.1	Darum geht es	6
2.2	Checkliste zur Vorbereitung	7
2.3	Bedeutung in der Informatik	8
2.4	Theorie	12
2.5	Lernziele, Kompetenzen	15
2.6	Unterrichtsidee	15
3	Daten 3: Modul Datenreplikation (MI.2.1k)	28
3.1	Darum geht es	28
3.2	Checkliste zur Vorbereitung	28
3.3	Bedeutung in der Informatik	28
3.4	Bedeutung für die Anwendung unter Berücksichtigung von Office 365.....	28
3.5	Lernziele, Kompetenzen	34
3.6	Unterrichtsidee	34
4	Programmieren 3: Modul «Verschiedene Algorithmen» (MI.2.2)	37
4.1	Darum geht es	37
4.2	Checkliste zur Vorbereitung	37
4.3	Bedeutung in der Informatik	37
4.4	Theorie	38
4.5	Lernziele, Kompetenzen	40
4.6	Unterrichtsidee	40
5	Systeme 3: Modul «Internet und Verschlüsselung» (MI.2.3)	43
5.1	Darum geht es	43
5.2	Checkliste zur Vorbereitung	43
5.3	Bedeutung in der Informatik	43
5.4	Theorie	44
5.5	Lernziele, Kompetenzen	52
5.6	Unterrichtsidee	53
6	Quellen	58
6.1	Daten 3	58
6.2	Programmieren 3	58
6.3	Systeme 3	59

Impressum

Amt für Volksschulen Basel-Landschaft, Liestal

Lehrplanteam:

Simone Meier, Urs Meyer und Lukas Dettwiler

Layout:

Priska Vögtli

Fotos Umschlag vorne und hinten:

Guido Schärli

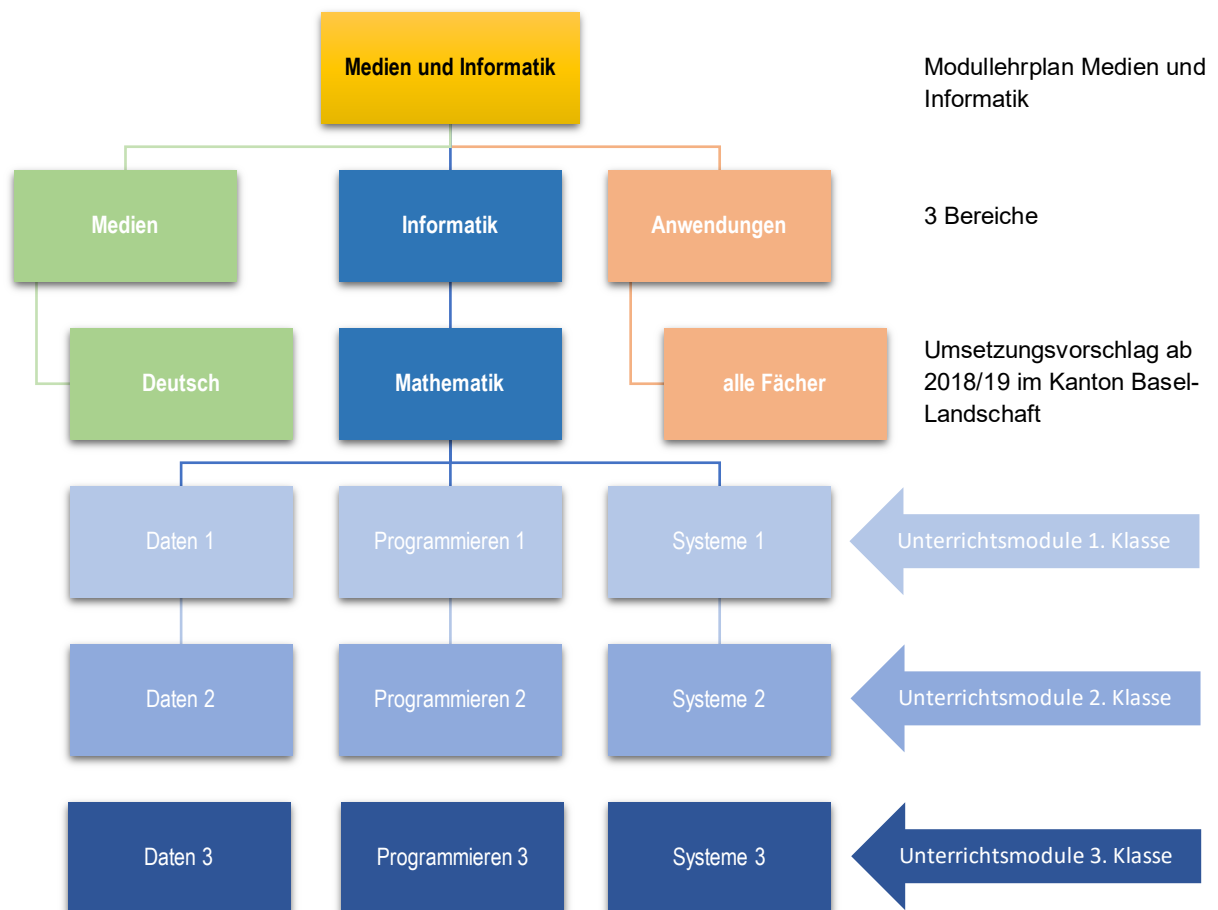
Liestal, 31.07.2020

1 Einleitung

Die im Jahr 2018 begonnene Reihe «Unterrichtsmodule Informatik» wird mit dieser Ausgabe abgeschlossen. Hiermit gibt es die Informatikmodule für alle drei Klassen der Sekundarstufe I.

Der Lehrplan «Medien und Informatik» umfasst die drei Bereiche: Medien, Informatik und Anwendungen. Im Kanton Basel-Landschaft geschieht die Umsetzung fächerübergreifend und fächerintegriert. Der Bereich Medien wird im Fach Deutsch unterrichtet, im Fach Mathematik ist eine halbe Jahreslektion Informatik enthalten und die Anwendungen resp. Anwendungskompetenzen werden in diversen Fächern behandelt, vgl. oberer Teil der Grafik 1.

Die vorliegende Broschüre enthält für jede der drei Informatik-Kompetenzen ein ausgearbeitetes Unterrichtsmodule. «Daten 3», «Programmieren 3» und «Systeme 3» decken den Unterricht in Informatik der 3. Klasse der Sekundarschule ab. Der Umfang entspricht einer halben Jahreslektion. Der Bezug zum Lehrplan ist in den Unterkapiteln «Lernziele, Kompetenzen» beschrieben und direkt über die Kompetenzkürzel (bspw. MI.2.1.k) verlinkt.



Diese Broschüre ist online über die Website des Kantons erreichbar²

¹ Vgl.: «Erläuterung Medien und Informatik (3. Zyklus)», vgl.: <https://www.baselland.ch/lehrplan-vs> | Lehrplan Volksschule Basel-Landschaft | Medien und Informatik 3. Zyklus: [Direkter Link zum PDF](#)

² Vgl.: <https://www.baselland.ch/lehrplan-vs> | Lehrplan Volksschule Basel-Landschaft | Medien und Informatik 3. Zyklus und auch: <https://www.baselland.ch/ict> | Downloads

1.1 Übersicht

Die Unterrichtsmodule der 3. Klasse sind folgendermassen aufgeteilt:

Unterrichtsmodul	Themen	Umfang
Daten 3	– Fehlererkennende und -korrigierende Codes MI.2.1.g	2 Lektionen
	– Datenreplikation MI.2.1.k	2 Lektionen
Programmieren 3	– Algorithmen anwenden MI.2.2.g , MI.2.2.h und MI.2.2.i	11 Lektionen
Systeme 3	– Das Internet mit seinen Diensten und als Infrastruktur MI.2.3.m	3 Lektionen
	– Risiken unverschlüsselter Datenübermittlung und -speicherung MI.2.3.n	

2 Daten 3: Modul «Fehlererkennende und -korrigierende Codes» (MI.2.1.g)

2.1 Darum geht es

Hast Du auch schon einmal «Stille Post» gespielt? Bei diesem Kinderspiel wird eine Botschaft weitergeflüstert. Das Spiel wird dadurch lustig, dass sich die Botschaft beim Weitersagen verändert. Probiert es doch einmal in der Klasse aus!

«Vielleicht hast Du Dich auch gefragt, warum die oft gespielten CDs so wenig kratzen und knacken, auch wenn die Oberfläche schon nicht mehr ganz unversehrt ist. Warum kommen die Texte und Bilder, die Du mit Freundinnen und Kollegen austauschst, genau so an, wie sie abgeschickt wurden, obwohl Du diese vielleicht um die halbe Welt gesendet hast? Passieren denn beim Übertragen gar keine Fehler?

Doch! Es passiert gar nicht selten, dass ein Bit falsch ankommt. Aber die Mathematikerinnen und Informatiker haben Codes entwickelt, bei denen etliche Fehler selbsttätig erkannt und sogar korrigiert werden können.

Das leuchtet zunächst gar nicht ein: Wie soll es denn noch richtig werden, wenn etwas beim Empfänger schon falsch ankommt?»³

³ Haftendorn, D. (2010), S. 51 f.

2.2 Checkliste zur Vorbereitung

- ☐ Computerraum, Laptops oder iPads
- ☐ Beamer
- ☐ «Daten 3 Code» mit folgendem Inhalt:

	1.1_Aufgaben_zu_fehlererkennenden_Codes.docx
	1.2_Aufgaben_zu_fehlererkennenden_Codes_Loesungen.docx
	1.3_Theorie_zu_fehlererkennenden_Codes.docx
	1.4_Arbeitsblatt_Redundanz_in_QR-Codes.docx
	2.1_Zaubertrick_Pruefbits.docx
	2.2_Aufgaben_Hamming_Code.docx
	2.3_Error_Correction_Hamming_Code.docx
	Check_EAN_Code.py
	Daten_3_MI_2_1_g.docx
	EAN_Pruefziffer_berechnen_Level_Easy.xlsx
	EAN_Pruefziffer_berechnen_Level_Medium.xlsx
	EAN_Pruefziffer_berechnen_Level_Tricky.xlsx
	einfachInformatik_Daten_Begleitband.pdf
	einfachInformatik_Daten_Schulbuch.pdf

- ☐ Hromkovič, J.: einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren, Schulbuch S. 52–69 und Begleitband S. 81–106.
- ☐ 36 Magnetkärtchen mit unterschiedlicher Vorder- und Rückseite («magnetische Wendeplättchen» googeln)
oder z.B. 36 blaue und 36 rote Magnete
- ☐ 1 Jasskartenspiel oder 36 Zündhölzer pro 2-er Gruppe



Alles mit zwei unterschiedlichen Seiten / Zuständen ist brauchbar. Dazu zählen Memorykarten, Münzen oder Karten, auf die 0 oder 1 aufgedruckt sind (als Brücke zum Binärsystem).

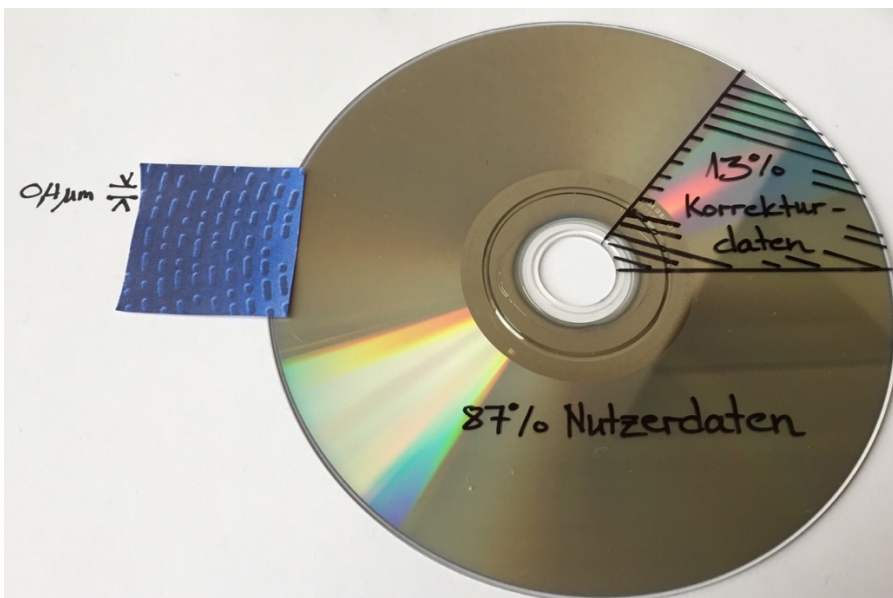
Bedeutung in der Informatik

In diesem Modul lernen wir, wie man Daten so kodieren kann, dass entstandene Fehler entdeckt und automatisch korrigiert werden können.

«Moderne Technologien ermöglichen es uns, immer grössere Datenmengen abzuspeichern, zu übertragen und zu verarbeiten. Je mehr Daten wir handhaben, desto grösser wird jedoch die Wahrscheinlichkeit, dass ab und zu ein Bit verloren geht oder «geflippt» wird (eine 1 wird zu einer 0 oder eine 0 zu einer 1). Wenn so etwas passiert, werden die Daten danach eventuell falsch interpretiert. Um das zu vermeiden, baut man spezielle Kodierungen der Daten. Diese erkennen, dass die Daten irgendwo einen Fehler enthalten. Manche Kodierungen können den Fehler sogar direkt ermitteln und ihn eigenständig korrigieren.

Die am weitesten verbreitete Anwendung ist die digitale Abspeicherung von Musik. Vor 50 Jahren verwendete man Schallplatten zur Abspeicherung und Wiedergabe von Musik. Ein kleiner Kratzer auf der Oberfläche der Platte reichte aus, und die korrekte Wiedergabe der Musik war nicht mehr möglich. Dies passierte, weil die beschädigten Daten im Bereich des Kratzers fehlten bzw. nicht mehr lesbar waren. Die darauffolgende Technologie der CD war bereits um einiges zuverlässiger. Selbst ca. zehn Kratzer konnten die korrekte Wiedergabe der CD nicht verhindern.»⁴

Auf einer DVD sind die Informationen in Milliarden von binären Zuständen gespeichert. Sie werden durch kleine Vertiefungen in einer optisch lesbaren Schicht dargestellt, die so dicht beisammen liegen, dass ein Staubkorn oder ein kleiner Kratzer gleich hunderte von Informationen unlesbar machen würde. Daher werden auch bei der DVD zusätzliche, sogenannte «redundante» Informationen hinzugefügt, die eigentlich nicht notwendig wären. Bei der DVD sind das 13% der Speicherkapazität, der Inhalt von vier ganzen CD-ROMs. Diese zusätzlichen Informationen sorgen jedoch dafür, dass Fehler korrigiert werden können und die DVD nicht sofort unbrauchbar machen.



⁴ Hromkovič, J. (2018) Schulbuch S. 52.

Eine kleine Anekdote zum Beethoven-Jahr 2020

Was hat der Durchmesser und die Speichergrösse von CDs mit dem vor 250 Jahren geborenen Beethoven zu tun?

Als Anfang der 80er-Jahre die Audio-CD entwickelt wurde, versuchten SONY und Philips sich auf einen gemeinsamen Standard bezüglich Durchmesser und Speicherkapazität dieser Scheibe zu einigen. Nach einigen Differenzen habe Sony vorgeschlagen, dass die neue CD zumindest Ludwig van Beethovens Neunte Sinfonie in voller Länge erfassen sollte. Dieser Vorschlag hing der Legende nach mit Sonys damaligem Vizepräsidenten zusammen, der ausgebildeter Opernsänger war und sich schon immer wünschte, Beethovens Neunte ohne störendes Wechseln des Tonträgers hören zu können. Die Techniker hielten sich an die damals längste zur Verfügung stehende Version mit einer Spieldauer von exakt 74 Minuten. Diese Länge bedeutete zwölf Zentimeter Durchmesser des optischen Datenträgers. Die Entwickler von Philips hätten mit Skepsis reagiert, da eine so grosse Scheibe nicht in die Anzugtasche wie eine Compact Cassette passen würde. Daraufhin hätten Sony-Entwickler Anzüge aus aller Welt ausgemessen, mit dem Ergebnis, dass für zwölf Zentimeter fast überall Platz sei.

QR-Codes

1.4_Arbeitsblatt_Redundanz_in_QR-Codes.docx

Auch in jeden QR-Code wird eine bestimmte Fehlertoleranz in Form von redundanten binären Daten integriert. Das bedeutet, diese Daten sind im fehlerfreien Fall (QR-Code ganz und lesbar) überflüssig oder redundant. Ist der QR-Code jedoch beschädigt, können diese zusätzlichen Daten bis zu einem bestimmten Grad helfen, die codierten Daten trotz Beschädigung wiederherzustellen. Die Menge dieser Redundanz und die daraus resultierende Fehlerkorrekturmöglichkeiten untergliedern sich in vier Toleranz-Level:

Level L (Low) - 7%

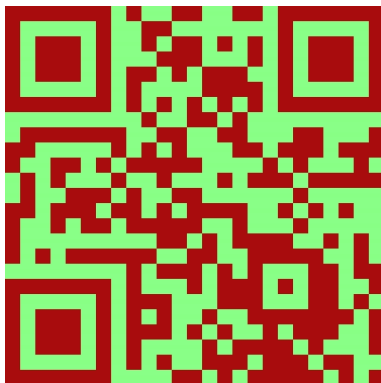
(das am meisten verwendete Level)



Level M (Medium) - 15%



Level Q (Quartile) - 25%



Level H (High) - 30%



Bildquelle: <https://www.xplore-dna.net/mod/page/view.php?id=1572>

Um die Fehlerredundanz zu veranschaulichen, verdecke beim Einscannen mit einem Finger einen Teil des Codes. Allerdings müssen die drei Positionsmarken in den Ecken erhalten bleiben. Man kann sehen, dass man bei dem QR-Code des Levels H einen grösseren Teil verdecken kann als beim QR-Code des Levels L. Das ist Redundanz, denn es sind alle Informationen so im QR-Code enthalten, dass trotz des Fehlens einiger Module die Information vollständig enthalten ist. Jedes Level gibt an, bis zu wie viel Prozent eines QR-Codes beschädigt bzw. unlesbar sein kann, ohne dass ein Datenverlust eintritt. Das Level kann beim Erstellen eines QR-Codes gewählt werden.

Die praktischen QR-Codes beinhalten aber auch Gefahren und Risiken. Viele QR-Code-Scanner führen den Scanvorgang und die anschliessende Weiterleitung «blind» aus. Das bedeutet, dass es für den Nutzer nicht möglich ist, zu erkennen, was sich eigentlich hinter dem QR-Code verbirgt.

So gelangt man schnell auf schadhafte Webseiten oder erhält Malware, ohne es zu merken. Vor allem für Smartphones, die meist nicht so gut vor Schadprogrammen geschützt sind, stellt dies eine besonders grosse Gefahr dar.

Beachtet man die unten aufgeführten Punkte, kann das Risiko vor solchen Gefahren minimiert werden:

- Scanne keine überklebten QR-Codes.
- Benutze einen QR-Code Scanner, welcher nicht direkt «blind» weiterleitet, und prüfe vorab die komplette URL.
- Nutze Security-Lösungen, die Webseiten beim Öffnen auf schädliche Inhalte und Downloads auf Viren prüfen.⁵

⁵ Vgl.: <https://www.xplore-dna.net/mod/page/view.php?id=1566>

2.3 Theorie

EAN und ISBN Code

Die 13-stellige EAN (Europäische Artikel-Nummer) dient zur Identifizierung von Produkten und wird häufig auch durch einen Strichcode dargestellt, um die Nummer maschinenlesbar zu machen.

Beispiel: 4 0 0 1 5 0 5 0 0 7 3 7

- Die ersten 3 Ziffern beschreiben das Herkunftsland (400 = Deutschland).
(Hinweis: Bücher stammen immer aus «Bookland» 978 oder 979.)
- Die nächsten 3 Ziffern geben den Hersteller an (150 = Steiff).
- Die folgenden 5 Ziffern sind eine vom Hersteller gewählte Artikelnummer.
- Die letzte Ziffer ist die EAN-Prüfziffer.

Die EAN und die ISBN (Internationale Standardbuchnummer) werden normalerweise vom Laserscanner der Kasse oder der Ausleihe in der Bibliothek gelesen. Dann prüft der Kassenscomputer diese Nummer. Im Folgenden wird erklärt, wie diese Prüfung geschieht und welche Rolle dabei die sogenannte Prüfziffer spielt. Ist alles korrekt, piept die Kasse einen speziellen Ton. Wenn aber Fehler durch einen geknickten oder verschmutzten Barcode entstanden sind, piept die Kasse nicht wie sonst und die Nummer muss eventuell manuell eingetippt werden. Dann können noch Fehler beim Tippen entstehen.



Prüfung

1. Multipliziere die 13 Ziffern wechselweise mit 1 und mit 3.
2. Addiere alle diese Produkte. Es ergibt sich die Prüfsumme.
3. Ist die Prüfsumme ein voller Zehner, dann ist die EAN bzw. ISBN gültig.
4. Ist sie es nicht, dann ist die EAN bzw. ISBN ungültig.

9	1	2	3	4	5	6	7	8	9	0	1	3	// EAN CODE
x	x	x	x	x	x	x	x	x	x	x	x	↑	
1	3	1	3	1	3	1	3	1	3	1	3	10-7	// AUF 10 AUFRUNDEN
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↑	
$9 + 3 + 2 + 9 + 4 + 15 + 6 + 21 + 8 + 27 + 0 + 3 = 107$													// SUMME DES EAN

Lese- und Tippfehler führen in vielen Fällen zu einer falschen Prüfsumme. Bei einer gültigen EAN und ISBN ist die Prüfziffer so bestimmt, dass die Prüfsumme ein voller Zehner ist. Dadurch werden alle Einzelfehler und viele Zahlendreher entdeckt.

Selbstverifizierende Kodierungen

«Es gibt Situationen, in denen man gar nicht versuchen will, die entdeckten Fehler zu korrigieren, weil man die Verantwortung für die Korrekturen nicht übernehmen möchte. Im Online-Banking oder bei einer Online-Warenbestellung macht das System den Kunden oder die Kundin auf das Vorhandensein eines Fehlers aufmerksam und erwartet dann die Korrektur durch die Benutzerin oder den Benutzer. Wenn es um die Übertragung von Bild und Ton geht, wünscht man sich jedoch eine automatische und unverzügliche Korrektur der Daten, gleich nach der Entdeckung eines Fehlers.»⁶

In allen drei Leistungszügen A, E und P wird ein fehlerkorrigierender Code mit Hilfe eines «Zaubertricks» erarbeitet (vgl. Unterrichtsidee).

Im Leistungszug P kann auch als Erweiterung der Hamming Code mit folgender eingängigen Methode erfahren werden:

Hamming-Code

Der erste fehlerkorrigierende Code wurde von Richard Hamming gleich zu Beginn des Computerzeitalters 1948 entwickelt. Er zeigt das Grundprinzip so deutlich, dass wir ihn uns genauer ansehen.

Ein wesentlicher Begriff der Codierungstheorie ist der folgende:

Die Parität einer Bitfolge ist 0, wenn die Anzahl der Einsen in der Folge gerade ist.

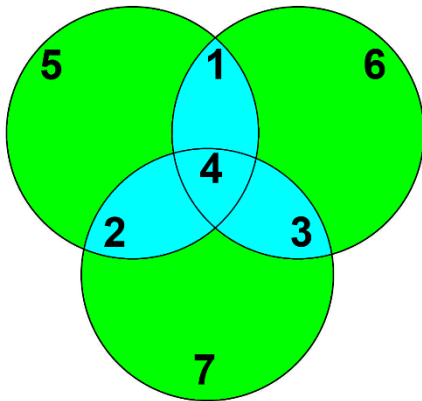
Die Parität einer Bitfolge ist 1, wenn die Anzahl der Einsen in der Folge ungerade ist.

Beispiel: Die Parität von 11101011 ist 0, die Parität von 11101010 ist 1.

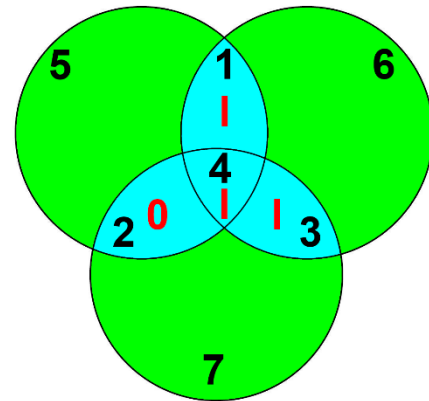
Übrigens schreibt man in der Handschrift gern die 1 in einer Bitfolge als einfachen Strich. Dann kann man gleich Bitfolgen von Dezimalzahlen unterscheiden.

⁶ Hromkovič, J. (2018) Begleitband S. 92.

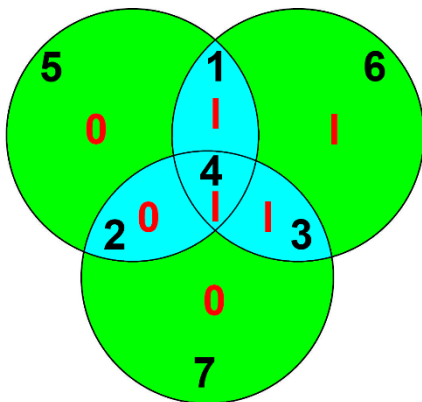
Zu je vier eigentlich zu sendenden Bits der Nachricht werden drei «Korrekturbits» berechnet und angehängt. Die folgenden Abbildungen verdeutlichen das Vorgehen:



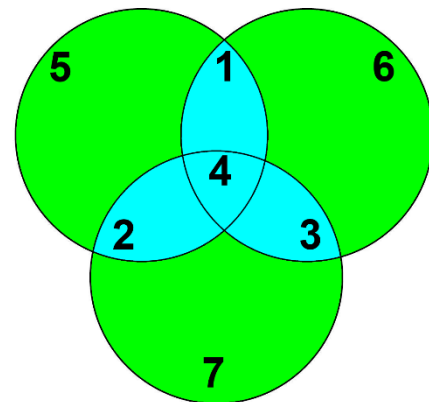
Gegeben ist dieses Venn-Diagramm.



Schreibe die Nachricht (**1 0 1 1**) in die blauen Felder 1, 2, 3, 4.



Schreibe in die grünen Felder 5, 6 und 7 die Parität der im zugehörigen Kreis stehenden Bits (**0 1 0**).



Hänge die Bits der Felder 5, 6, 7 an die Nachricht an.

Der Empfänger trägt die sieben Bits (**1 0 1 1 0 1 0**) in die Felder eines leeren Venn-Diagramms ein und prüft, ob die Paritäten übereinstimmen.

Im Beispiel der Abbildung ist dargestellt, dass statt der Nachricht **1011** die Bitfolge **1011 010** gesendet wird. Nur vier dieser sieben Bits tragen die eigentliche Information. Daher sagt man auch, der Hamming-Code habe einen Informationsgehalt von vier Siebenteln.⁷

⁷ Haftendorn, D. (2010)

2.4 Lernziele, Kompetenzen

- Die Schülerinnen und Schüler verstehen die Funktionsweise von fehlererkennenden und -korrigierenden Codes. (MI.2.1.g)
- Die Schülerinnen und Schüler verstehen, warum der Bedarf entstehen kann, Daten so robust darzustellen, dass kleine Beschädigungen erkannt und automatisch korrigiert werden können.
- Die Schülerinnen und Schüler kennen Beispiele von Datenkodierungen aus der Praxis, die einfache und häufig vorkommende Tippfehler oder Beschädigungen erkennbar machen.
- Die Schülerinnen und Schüler können Kodierungen selbstständig entwickeln oder anwenden, um einfache Arten von Fehlern zu erkennen und zu korrigieren.

2.5 Unterrichtsidee

a. Ablauf

Ein Fehler eines Textes (d.h. Buchstaben oder Zahlenfolge) besteht (für uns) darin, dass ein oder mehrere Zeichen verändert werden (d.h. zu anderen Zeichen werden).

Ziel: Der Empfänger soll erkennen können, ob ein (oder mehrere) Fehler passiert sind (Fehlererkennung) und wie die Originalzeichen aussehen (Fehlerkorrektur).

Grundidee: Man fügt der Nachricht etwas hinzu, eine «Kontrollinformation», die dazu dient, eventuelle Übertragungsfehler zu erkennen. Beispiele:

Namen buchstabieren («Emm o enn enn te a ge»)

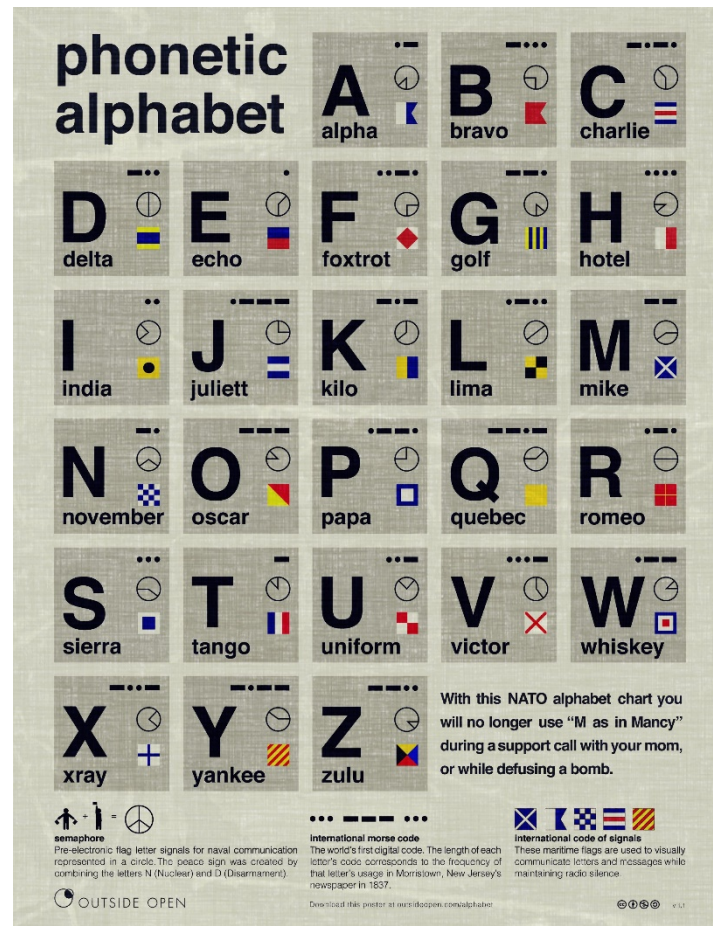
Buchstabieralphabet («A wie Anton, B wie Berta, ...»)

Buchstabieralphabet auf einem alten Schweizer Militärtelefon



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

Nato Alphabet



<https://www.pinterest.de/pin/515169644876118249/>

Natürliche Sprachen sind redundant (haben überflüssige Information):

man vrsteht alls, auc wnn eing Bchstbn fhln. Selpst wen groppe reckscreib Felr auftren, ged dr ssnn nich färlahn.

EAN und ISBN Code

(1 Lektion)

Unterrichtsverlauf und Übungen gemäss:

- Hromkovič, J. (2018) einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren, Schulbuch S. 52–56 und Begleitband S. 81–86
 - Übungen für Leistungszüge A, E und P Schulbuch S. 53, Beispiel 1.1 und 1.2
 - Weiterführende Betrachtungen für Leistungszug P: Schulbuch S. 54, Beispiel 1.3

t	Sozialform	Aktivitäten der Lehrperson	Aktivitäten der Schülerinnen und Schüler	Material
5'	LV, UG, GA	Einstieg «Habt ihr auch schon einmal «Stille Post» gespielt? Bei diesem Kinderspiel wird eine Botschaft weitergeflüstert. Das Spiel wird dadurch lustig, dass sich die Botschaft beim Weitersagen verändert. Probiert es doch einmal aus!»	Die SuS spielen «Stille Post» z.B. The White House 1600 Pennsylvania Avenue NW Washington, DC 20500 oder 001 202 456 1111 (Telefonnummer des Weissen Hauses)	
5'	LV, UG, SG, PA	«Vielleicht habt ihr euch schon einmal gefragt, warum die oft gespielten CDs so wenig kratzen und knacken, auch wenn die Oberfläche schon nicht mehr ganz unversehrt ist. Warum kommen die Texte und Bilder genau so an, wie sie abgeschickt wurden, obwohl diese vielleicht um die halbe Welt gesendet wurden? Passieren denn beim Übertragen gar keine Fehler?» «Wie soll der Empfänger Fehler erkennen und korrigieren können?» Aussagen und Begriffe sammeln und ergänzen	Die SuS nennen, erklären... evtl. Aufgabe 1 und 2 aus <i>1.1_Aufgaben_zu_fehlererkennen den_Codes</i> evtl. <i>1.4_Arbeitsblatt_Redundanz_in_QR-Codes.docx</i>	Visualisieren des Brainstormings WORD-Dateien: <i>1.1_Aufgaben_zu_fehlererkennenden_Codes</i> <i>1.2_Aufgaben_zu_fehlererkennenden_Codes_Loesungen</i> <i>1.3_Theorie_zu_fehlererkennenden_Codes</i> <i>1.4_Arbeitsblatt_Redundanz_in_QR-Codes.docx</i>

10'	LV, UG	«Zaubertrick» SuS diktieren der LP die ersten 12-Ziffern eines EAN- oder ISBN-Codes (Kaugummipackung, Schulbuch etc.). Danach berechnet die LP die 13. Ziffer.	Die SuS suchen und diktieren EAN-Codes von Produkten aus ihrem Schulsack.	Eigene Waren und Bücher, Wandtafel oder White Board
25'	PA, EA, UG	einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren Begleitband Seite 81–86 LP unterstützt die SuS bei den zu lösenden Aufgaben Alternativ oder ergänzend zu «einfach Informatik» kann für den Theorieteil auch die WORD-Datei <i>1.3_Theorie_zu_fehlererkennenden_Codes</i> verwendet werden.	einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren Schulbuch Seite 52–56 Die SuS bearbeiten und lösen die Beispiel 1.1 und 1.2 auf Seite 53 Weiterführende Betrachtungen für Leistungszug P: Schulbuch Seite 54, Beispiel 1.3 evtl. Aufgabe 3 bis 9 aus <i>1.1_Aufgaben_zu_fehlererkennenden_Codes</i> als Vertiefung und Festigung oder als Hausaufgaben.	Schulbuch und Begleitband einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren WORD-Dateien: <i>1.1_Aufgaben_zu_fehlererkennenden_Codes</i> <i>1.3_Theorie_zu_fehlererkennenden_Codes</i> Schreibzeug und Notizheft

LV – Lehrpersonenvortrag

SV – Schülerinnen- und Schülervortrag

UG – Unterrichtsgespräch

PA – Partnerinnen- und Partnerarbeit

EA – Einzelarbeit

GA – Gruppenarbeit

SG – Schülerinnen- und Schülergespräch

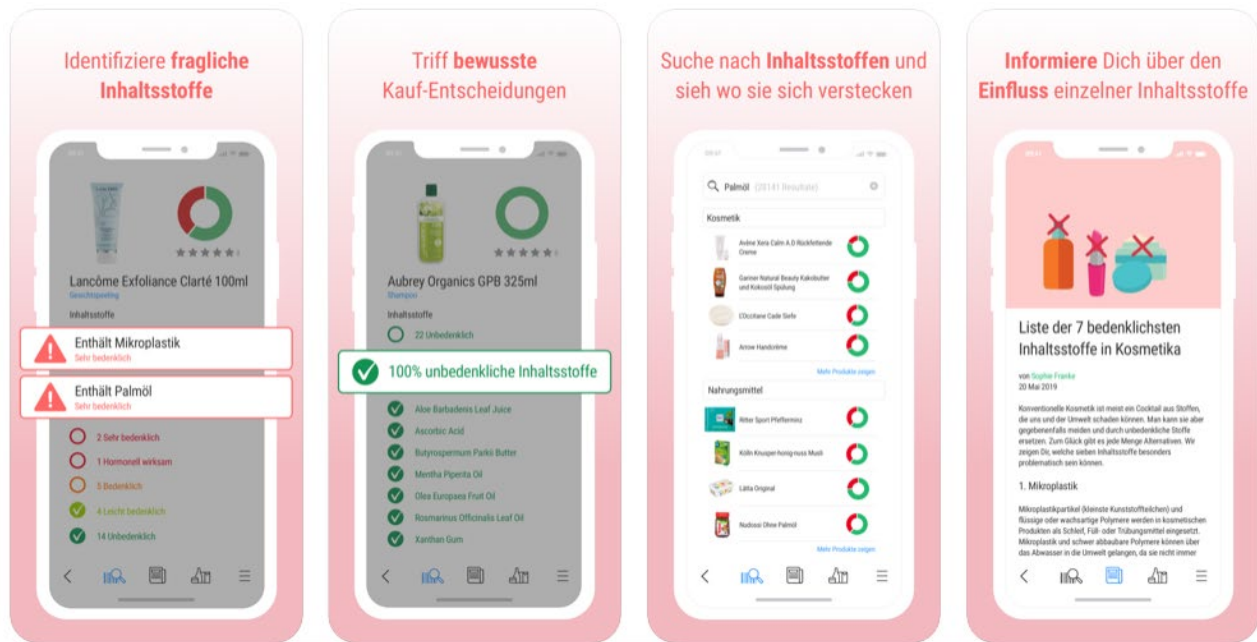
Erweiterung zum EAN: Gesellschaftlich-kulturelle Perspektive

Die Tatsache, dass alle käuflichen Objekte eine weltweit eindeutige Nummer besitzen, erlaubt nun, dass man Informationen über diese Objekte speichern und weltweit abrufen kann. So existieren heute zahlreiche Apps, die Zusatzinformationen bieten zu gesundheitlichen oder ökonomisch-gesellschaftlichen Aspekten von käuflichen Produkten.

Ein Beispiel ist die App Codecheck, welche primär Gesundheitsinformationen zu Produkten liefert.⁸



⁸ Vgl.: <https://www.codecheck.info/so-gehts/mobil>



Bildquelle: App Codecheck

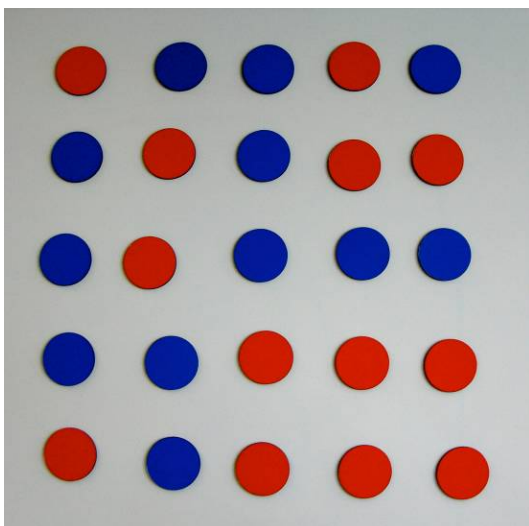
Selbstverifizierende Kodierungen

(1 Lektion)

Unterrichtsverlauf und Übungen gemäss:

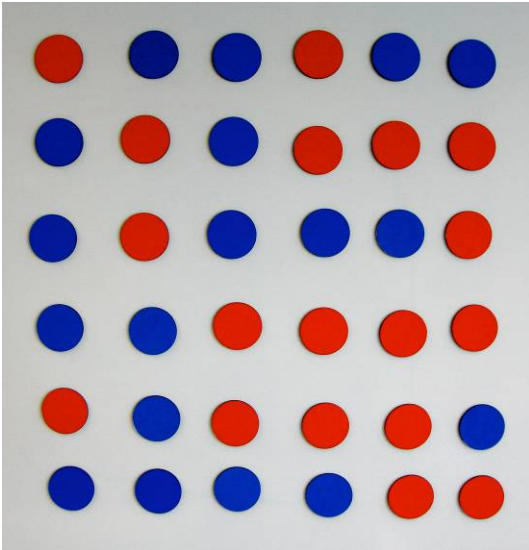
- Hromkovič, J. (2018) einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren, Schulbuch S. 64f und Begleitband S. 96.

Zu Beginn wird ein Kartentrick vorgestellt, der zunächst nichts mit Codes zu tun zu haben scheint. Dazu versammeln sich die Lernenden um einen Tisch, auf dem das Kartenspiel gezeigt wird. Wenn die Klasse gross ist, können statt Karten auch Magnete verwendet werden, die auf jeder Seite eine andere Farbe haben und die sich beidseitig an der Wandtafel befestigen lassen. Für den Kartentrick wird ein Helfer benötigt. Eine Schülerin heftet die Magnete in einem 5 x 5 Quadrat an die Wandtafel. Welche Seite sichtbar ist, sollte dem Zufall überlassen werden.

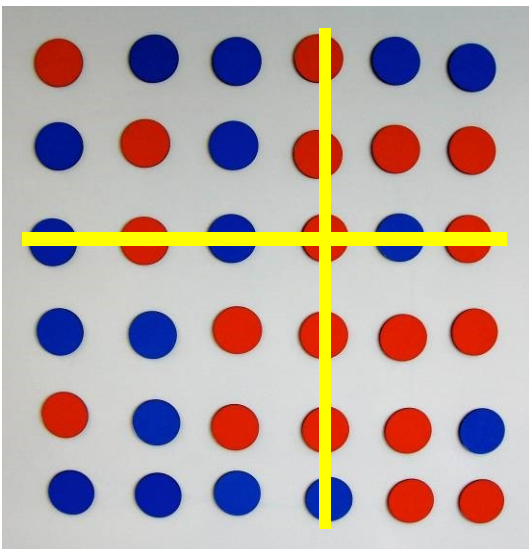


Jetzt ergänzt die Lehrkraft das Muster und fügt rechts und unten jeweils eine Reihe an, weil
 «Lehrer ja immer alles korrigieren müssen».

Diese Magnete müssen so gelegt werden, dass in jeder Reihe und in jeder Spalte immer eine
 gerade Anzahl gleicher Farbe sichtbar ist («Paritätsbit»).



Ein Schüler soll nun genau einen Magneten umdrehen, während die Lehrkraft sich die Augen
 zuhält. Die Reihe und die Spalte, in der ein Magnet umgedreht wurde, haben jetzt eine ungerade
 Zahl farbiger Karten. Dadurch lässt sich die veränderte Karte eindeutig identifizieren.



Wer durchschaut den «Trick»?

Nach Erarbeiten der Lösung wiederholen die Schüler/innen den Trick abwechselnd in Zweiergruppen mit einem Jasskartenspiel.



t	Sozialform	Aktivitäten der Lehrperson	Aktivitäten der Schülerinnen und Schüler	Material
5'	LV, UG, SG, PA	«Zaubertrick» LP demonstriert den Zaubertrick gemäss obiger Anleitung oder entsprechend einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren, Schulbuch Seite 64, Beispiel 7A, LP erklärt, wie der Trick funktioniert. Entweder gemäss obiger Beschreibung oder mit Hilfe der Erklärung aus einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren, Schulbuch Seite 64, «Wie funktioniert der Trick?»	Die SuS assistieren gemäss Anleitung und versuchen den Zaubertrick «zu erraten».	Magnetplättchen, Jasskarten, Kärtchen aus farbigem Papier o.ä. einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren, Schulbuch und Begleitband WORD Datei <i>2.1_Zaubertrick_Pru efbits</i>
10'	PA		Die SuS führen sich den Kartentrick mit den Prüfbits in PA mit rechteckigen Anordnungen von Jasskarten, Münzen, farbigem Papier etc. gegenseitig vor.	Magnetplättchen, Jasskarten, Kärtchen aus farbigem Papier o.ä.
30'	LV, EA, PA, SG	Leistungszug A (auch E und P möglich) Erweiterung zum EAN: Gesellschaftlich-kulturelle Perspektiven LP stellt die App «Codecheck» vor Schülerinnen und Schüler, welche bereits entsprechende Anwendungskompetenzen in EXCEL erworben haben, können mit Hilfe einer Tabellenkalkulation eine eingegebene EAN testen. Die vorliegende Aufgabe liegt in drei unterschiedlichen Schwierigkeitsgraden vor (vgl. Abschnitt c. dieser Broschüre «Differenzierung und Erweiterung»).	Die SuS sammeln mit einer App (z.B. mit «Codecheck») Zusatzinformationen zu gesundheitlichen oder ökonomisch-gesellschaftlichen Aspekten von käuflichen Produkten.	App «Codecheck», eigene Produkte und Lebensmittel EXCEL Files: <i>EAN_Pruefziffer_ber echnen_Level_Easy</i> <i>EAN_Pruefziffer_ber echnen_Level_Medi um</i> <i>EAN_Pruefziffer_ber echnen_Level_Trick y</i>

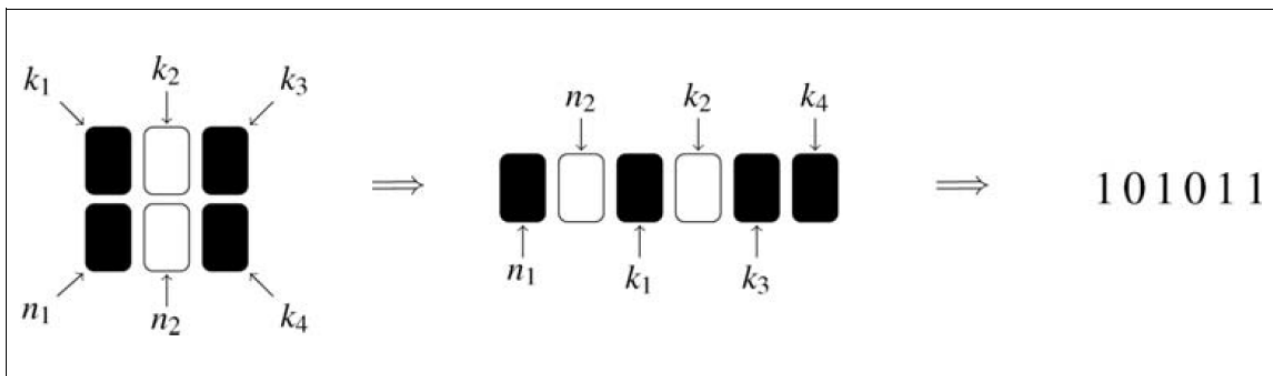
30'	LV, EA, PA	Leistungszug E und P (als Vertiefung) Falls eine vertiefte Betrachtung fehlerkorrigierender Codes erwünscht ist, kann die Kartendarstellung verlassen und die Information als Bitfolge betrachtet werden. Eine ausführliche Erklärung dieser Abstraktion, welche den Kartentrick zu binären Code-Wörtern transformiert, wird in «einfach Informatik, Daten darstellen, verschlüsseln, komprimieren» auf den Seiten 64 ff. im Schulbuch, auf den Seiten 96 ff. des Begleitbandes oder im unten stehenden Abschnitt beschrieben. Ein in der Informatik konkret angewandtes fehlerkorrigierendes Verfahren ist der Hamming-Code. Er wird in der WORD-Datei <i>1.3_Theorie_zu_fehlererkennenden_Codes</i> beschrieben und den SuS vorgestellt.	SuS lösen mit Hilfe des Hamming Codes die Aufgabe 11 des folgenden Arbeitsblattes: <i>1.1_Aufgaben_zu_fehlererkennenden_Codes</i> oder folgende Aufgabe: <i>2.2_Aufgaben_Hamming_Code</i>	einfach Informatik, Daten darstellen, verschlüsseln, komprimieren, Schulbuch und Begleitband WORD Dateien: <i>1.1_Aufgaben_zu_fehlererkennenden_Codes</i> <i>1.2_Aufgaben_zu_fehlererkennenden_Codes_Loesungen</i> <i>1.3_Theorie_zu_fehlererkennenden_Codes</i> <i>2.2_Aufgaben_Hamming_Code</i> <i>2.3_Error_Correction_Hamming_Code</i>
-----	------------	--	---	---

Erweiterung für Leistungszug P: Darstellung als Bitfolge

«Nun wird der Kartentrick anders dargestellt. Anstatt die Karten so aufzuzeichnen, wie wir es bis jetzt gemacht haben, schreiben wir für jede verdeckte Karte eine 1 und für alle anderen Karten eine 0. Wir interpretieren also die Karten als Bits. (Jede beliebige Nachricht kann bekanntlich als Bitfolge dargestellt werden.)

Die Karten, die ursprünglich auf den Tisch gelegt wurden, seien nun eine Nachricht, die wir an jemanden verschicken möchten. Auf dem Weg zum Empfänger kann es vorkommen, dass die Nachricht beschädigt wird. Wir nennen solche Beschädigungen Übertragungsfehler. In unserem Spiel war das Umdrehen einer Karte ein Übertragungsfehler. In der Darstellung mit den Nullen und Einsen entspricht das dem Invertieren eines Bits. Das heisst, wenn das Bit eine 1 ist, dann wird es zu einer 0 und umgekehrt. Es gibt natürlich noch andere Übertragungsfehler, wie zum Beispiel das Verschwinden oder das Dazukommen eines Bits. Wir beschränken uns hier aber auf das Invertieren eines oder mehrerer Bits. Die Lehrperson hatte zur Nachricht noch zusätzliche Karten auf den Tisch gelegt. Diese Karten haben es uns ermöglicht, dass wir den Fehler (also das Umdrehen einer Karte) finden konnten. Diese zusätzlichen Bits nennen wir Prüfbits. Um die Brücke zu dem vorangegangenen Kartentrick zu schlagen, wenden wir als Erstes diese Methode an, um die Nachrichten zu codieren. Für die Nachricht 10 sieht dies dann beispielsweise aus wie im untenstehenden Bild dargestellt. Die beiden Bits n_1 und n_2 sind unsere Nachrichtenbits, um die vier verschiedenen Nachrichten darzustellen. Die vier Prüfbits k_1 bis k_4 entsprechen den Karten, die jeweils angehängt werden, um Fehler korrigieren zu können.

Wir wollen nun die Karten-Darstellung verlassen und schreiben daher alle Bits hintereinander als ein Wort, indem wir zum Beispiel die Bits in der folgenden Reihenfolge angeben: $n_1, n_2, k_1, k_2, k_3, k_4$.»⁹



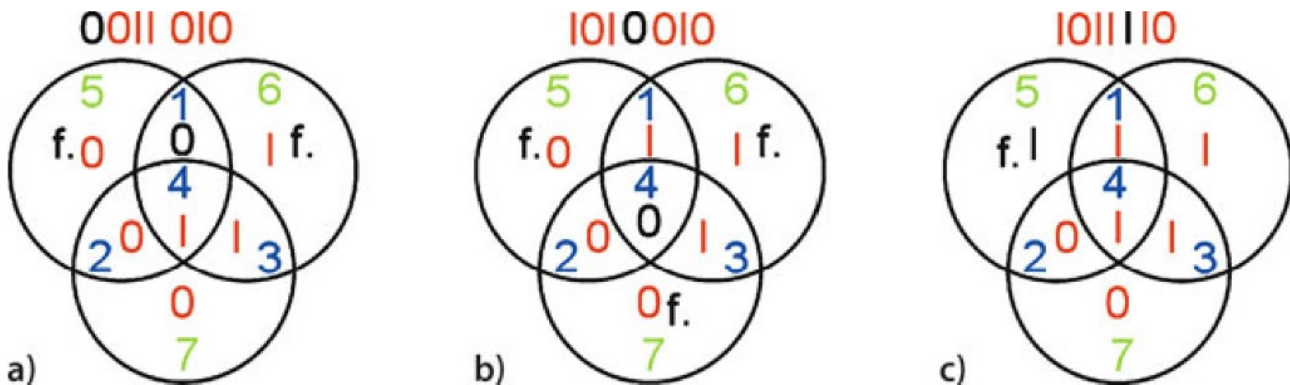
Darstellung der Codierung der Nachricht «10». Die Karten werden der Darstellung entsprechend hintereinandergelegt. Anstelle der Karten verwenden wir schliesslich eine Bitfolge (Codewort).

Eine ausführliche Erklärung dieser Abstraktion, welche den Kartentrick zu binären Code-Wörtern transformiert, wird in «einfach Informatik, Daten darstellen, verschlüsseln, komprimieren» auf den Seiten 64 ff. im Schulbuch und auf den Seiten 96 ff. des Begleitbandes beschrieben.

⁹ Hromkovič, J. et al. (2011)

Hamming-Code

Die Schülerinnen übermitteln einander:



Fehler in der Sendung

«Wir betrachten die Fälle, bei denen beim Senden der Nachricht nur ein einziger Fehler auftritt. Dann gibt es drei Fehlertypen.

Typ 1

In Abb. a) ist eins der ersten drei Bits falsch übermittelt, hier schwarz in Feld 1 dargestellt. 0011010 wurde empfangen. Dann zeigt aber Bit 5 etwas Falsches an, denn die Felder 1, 2 und 4 haben nun nur eine 1, darum müsste in Feld 5 eine 1 stehen. Ebenso passt der Eintrag in Feld 6 nicht mehr. Aber in Feld 7 steht weiterhin das Richtige. Wenn der Empfänger also die Bitfolge prüft, merkt er, dass genau zwei Fehler aufgetreten sind, nämlich in Feld 5 und 6, darum muss – es durfte ja nur ein Fehler beim Senden auftreten – Feld 1 falsch sein. Da dort das Bit 0 angekommen ist, hätte es eine 1 sein müssen. Also korrigiert der Empfänger den Fehler und nimmt als Nachricht nun 1011010 an. Ebenso können Einzelfehler in Feld 2 oder 3 korrigiert werden.

Typ 2

In Abb. b) ist das vierte Bit falsch übermittelt, hier schwarz in Feld 4 dargestellt. 1010010 wurde empfangen. Nun sind ebenfalls die Felder 5 und 6 falsch, aber auch Feld 7. Hieraus schliesst der Empfänger, dass das Bit in Feld 4 falsch angekommen ist. Er berichtigt es und nimmt als Nachricht nun 1011010 an.

Typ 3

In Abb. c) ist eins der Korrekturbits falsch übermittelt, hier schwarz in Feld 5 dargestellt. 1011110 wurde empfangen. Von diesem Fehler sind die Felder 6 und 7 nicht berührt, ausschliesslich Feld 5 zeigt etwas Falsches an. Daraus schliesst der Empfänger, dass nur das Bit in Feld 5 selbst falsch angekommen ist. Er berichtigt es und nimmt als Nachricht nun 1011010 an. Ebenso geht es bei Einzelfehlern in Feld 6 oder 7. Wir haben gesehen: Der Hamming-Code kann Einzelfehler immer korrigieren. Wenn also in einer sehr langen Bitfolge in keinem Siebenerblock mehr als ein Übertragungsfehler auftritt, ist am Ende dennoch die ganze Folge vollständig richtig.»¹⁰

¹⁰ Haftendorn, D. (2010) S. 52 f.

b. Material

- Siehe Planung

c. Leistungsüberprüfung/Bewertung

- Aufgaben zu EAN- und Hamming-Codes analog zu den Beispielen der Unterrichtseinheit «Selbstkorrigierende Kodierungen» aus «einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren», Seite 52 ff. bzw. der Theorie-, Arbeits- und Aufgabenblätter.

d. Differenzierung, Erweiterung

- Alternativ oder ergänzend zur Unterrichtseinheit «Selbstkorrigierende Kodierungen» aus «einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren», Seite 52 ff. können auch die Theorie-, Arbeits- und Aufgabenblätter verwendet werden.
- Schülerinnen und Schüler, welche bereits entsprechende Anwendungskompetenzen in EXCEL erworben haben, können mit Hilfe einer Tabellenkalkulation eine eingegebene EAN testen.

Die Aufgabe liegt in drei unterschiedlichen Schwierigkeitsgraden vor:

EAN_Pruefziffer_berechnen_Level_Easy.xlsx

Es muss nur noch der EAN-Code eingegeben werden. Alle Formeln sind bereits in der Tabelle vorhanden. Das Arbeitsblatt ist geschützt und kann nicht bearbeitet werden. Es können nur die Ziffern in die 12 grünen Felder eingetragen werden. Der Blattschutz kann ohne Passwort aufgehoben werden.

EAN_Pruefziffer_berechnen_Level_Medium.xlsx

Die angegebenen Formeln müssen in die entsprechenden Zellen der Tabelle eingegeben werden.

EAN_Pruefziffer_berechnen_Level_Tricky.xlsx

Die EXCEL-Tabelle wird gemäss den Anweisungen auf dem Arbeitsblatt von Grund auf erstellt.

- Falls die Schülerinnen und Schülern bereits mit TigerJython Erfahrungen haben, kann mit dem Python-Programm Check_EAN_Code.py die Korrektheit eines EAN-Codes überprüft werden.

e. Fächerübergreifend

- Mit Hilfe einer App und Online-Recherchen lassen sich mit dem EAN-Code Zusatzinformationen zu gesundheitlichen oder ökonomisch-gesellschaftlichen Aspekten von käuflichen Produkten beschaffen.
 Diese gesellschaftlichen, ökologischen und wirtschaftlichen Perspektiven lassen sich darum auch in den Fächern Biologie, Chemie, Wirtschaft, Geographie, Geschichte, Hauswirtschaft, Ethik, BNE oder in einer Projektarbeit untersuchen.

3 Daten 3: Modul Datenreplikation (MI.2.1.k)

3.1 Darum geht es

Wir alle waren wahrscheinlich schon einmal in der Situation, dass ein Dokument, an dem wir gearbeitet hatten, plötzlich nicht mehr vorhanden war. Entweder funktionierte der Datenträger nicht mehr oder ein Absturz des Computers im dümmsten Moment löschte die Arbeit der letzten Stunden. Um dies verhindern zu können, setzen wir uns in diesem Modul mit verschiedenen Möglichkeiten der Datenreplikation auseinander. Das Thema betrifft uns sowohl als Privatperson wie auch im Beruf; für IT-Systeme in Firmen ist es von grosser Bedeutung.

3.2 Checkliste zur Vorbereitung

- ☐ Computerraum, Notebooks
- ☐ Beamer
- ☐ «Daten 3 Datenreplikation» mit folgendem Inhalt:
 - 1_Einstieg_Backup.docx
 - 2_Backup_Regel.docx
 - 3_Bedeutungsquadrat.docx
 - 4_Synchronisierung.docx
 - 5_Versionierung.docx

3.3 Bedeutung in der Informatik¹¹

Datenreplikation ist im Grunde ein Datenkopiervorgang und dient in erster Linie der Datensicherung.

Die verschiedenen Verfahren resp. Methoden haben in der Informatik eine grosse Bedeutung, da sie in der Anwendung den zuverlässigen, sicheren Betrieb von Informationssystemen ermöglichen. Bei komplexen Datenbanken erhöht Datenreplikation die Verfügbarkeit der Informationen und erlaubt einen zuverlässigen Betrieb, auch wenn viele Personen gleichzeitig auf das System resp. die Datenbank zugreifen und Änderungen vornehmen.

3.4 Bedeutung für die Anwendung unter Berücksichtigung von Office 365

Wie wichtig die Datensicherung ist, wird uns immer dann bewusst, wenn ein Datenverlust eingetreten ist.

Im Folgenden werden die drei Methoden der Datenreplikation, die im Lehrplan explizit erwähnt werden, kurz besprochen. Zudem wird auf den Funktionsumfang der Datenreplikation von Office 365 eingegangen.

Backup

Ein Backup ist eine Sicherheitskopie. Bei einem Datenverlust kann auf diese Kopie zurückgegriffen werden und das Original kann damit wiederhergestellt werden, vgl. (engl.) Restore. Damit im Schadenfall auch wirklich eine Kopie vorhanden ist, werden heute zunehmend automatisierte Abläufe zur Datensicherung eingesetzt, die zum Teil auf den klassischen Sicherungsarten und Backupstrategien beruhen.

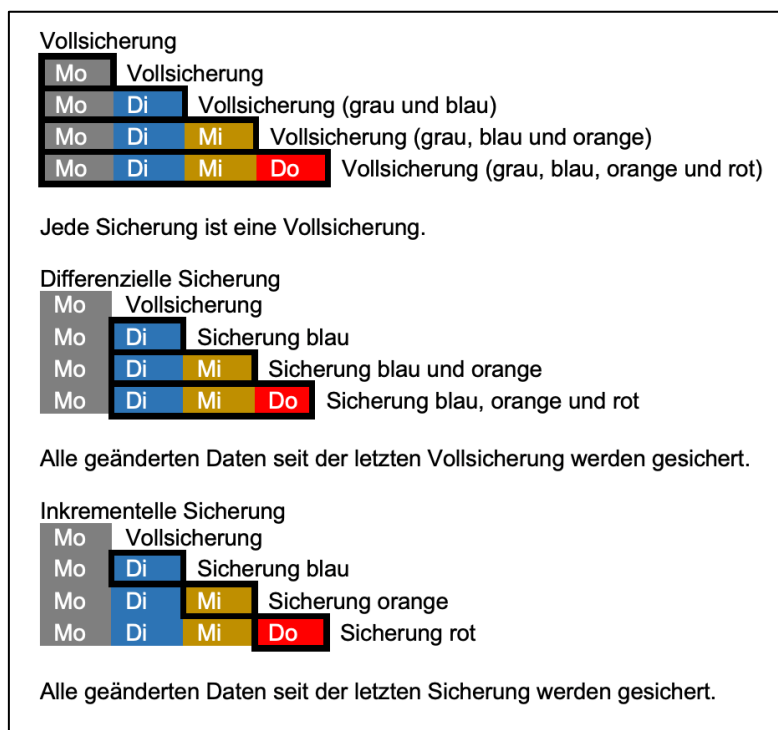
¹¹ Vgl.: [https://de.wikipedia.org/wiki/Replikation_\(Datenverarbeitung\)](https://de.wikipedia.org/wiki/Replikation_(Datenverarbeitung))

Grundlage für die Wahl der Datensicherungslösung bildet die entsprechende Risiko-Abklärung. Je nach Bedeutung der Daten und gesetzlichen Vorschriften werden verschiedene Sicherungsarten und Backupstrategien angewendet. Dabei gilt zu berücksichtigen, dass auch das Speichermedium, auf dem das Backup liegt, ausfallen kann. Bei einem Brand oder Diebstahl beispielsweise könnten Computer und Backup abhandenkommen. Auch gilt es, Malware und Cybercrime miteinzubeziehen. Daher geht es darum, alle Risiken zu beachten und gegebenenfalls auch Sicherheitskopien von Backups zu erstellen und diese an geschützten Orten unterzubringen.

Sicherungsarten

Das Anlegen von Backups braucht Zeit und Speicherplatz, daher kommen je nach Schutzbedarf unterschiedliche Arten der Sicherung zur Anwendung¹²:

Am meisten Zeit und Speicherplatz benötigt die Vollsicherung. Damit ist das vollständige Kopieren aller Daten eines Laufwerkes auf ein Sicherheitsmedium gemeint. Die beiden folgenden Methoden ergänzen die Vollsicherung, indem jeweils nur Änderungen gespeichert werden. Dadurch wird der Backup-Prozess deutlich weniger zeitaufwändig. Differenzielle Sicherung bedeutet, dass nur die geänderten Daten seit der letzten Vollsicherung gespeichert werden. Bei der inkrementellen Sicherung schliesslich werden nur die geänderten Daten seit der letzten Sicherung gespeichert. Diese Sicherungsart benötigt am wenigsten Zeit und Speicherplatz; der Restore ist aufgrund der zahlreichen Backups jedoch aufwändiger. Heute kommen inkrementelle Backups als automatisierte Lösungen in Netzwerken und in der Cloud zur Anwendung.



Sicherungsarten, nach <https://www.logical-concepts.de/site/assets/files/3344/backup.png>

¹² Vgl.: <https://de.wikipedia.org/wiki/Datensicherung>

Backupstrategien

«First in, first out (FIFO)¹³ ist die einfachste Strategie. Sobald die Speichermedien – oder der Speicherplatz eines Mediums – zur Neige [gehen], wird die älteste Vollsicherung gelöscht, beziehungsweise auch alle inkrementellen oder differenziellen Backups, die auf der ältesten Vollsicherung beruhen.»¹⁴

Grossvater-Vater-Sohn

Auch als Generationenprinzip bekannt, ist «Grossvater-Vater-Sohn» eine der häufigsten Strategien für die Erstellung von Backups.¹⁵

Das «Sohn»-Backup als häufigstes wird jeden Werktag erstellt, das Backup des «Vaters» am Ende der Woche und jenes des «Grossvaters» am Ende des Monats. «Verwendet man Vollsicherungen – und pro Vollsicherung ein Speichermedium – benötigt man vier Medien für die Wochentage (am letzten Werktag wird nämlich die wöchentliche Sicherung durchgeführt) und für die Wochen insgesamt fünf Speichermedien. Hinzu kommen beliebig viele Speichermedien, um die vergangenen Monate abzudecken, vgl. Abb. Generationenprinzip.

Auf macOS verwendet Time Machine¹⁶ eine ähnliche Strategie auf einem einzelnen Speichermedium: Für die letzten 24 Stunden werden stündliche Backups vorgehalten, für den letzten Monat tägliche Backups, und schliesslich wird das jeweils älteste monatliche Backup erst gelöscht, wenn der Speicherplatz ausgeht. Da jeweils das älteste Backup eine Vollsicherung darstellt, müssen vor dem Löschvorgang die Daten in das zweitälteste Backup transferiert werden.»¹⁷

Woche 1		Woche 2		Woche 3		Woche 4		Woche 5		Woche 6	
Mo	Sohn 1	Mo	Sohn 1	Mo	Sohn 1	Mo	Sohn 1	Mo	Sohn 1 Grossvater 1	Mo	Sohn 1
Di	Sohn 2	Di	Sohn 2	Di	Sohn 2	Di	Sohn 2	Di	Sohn 2	Di	Sohn 2
Mi	Sohn 3	Mi	Sohn 3	Mi	Sohn 3	Mi	Sohn 3	Mi	Sohn 3	Mi	Sohn 3
Do	Sohn 4	Do	Sohn 4	Do	Sohn 4	Do	Sohn 4	Do	Sohn 4	Do	Sohn 4
Fr	Vater 1	Fr	Vater 2	Fr	Vater 3	Fr	Vater 4	Fr	Vater 5	Fr	Vater 1

Generationenprinzip

Die Abbildung illustriert die Anwendung des Rotationsprinzips «Grossvater-Vater-Sohn» am Beispiel von Vollsicherungen auf einzelne Speichermedien am Ende der jeweiligen Tage. 4 Speichermedien für die Tage: Sohn 1–4, 5 Speichermedien für die Wochen, Vater 1–5 und 11 Speichermedien für die Monate. Die Farben zeigen, dass die Speichermedien jeweils immer

¹³ In der Informatik bezeichnet man diese Datenstruktur als Warteschlange oder Queue. Sie kann bei Videoüberwachungssystem oder Flugschreibern auch als sogenannter Ringpuffer realisiert werden.

¹⁴ Vgl.: <https://de.wikipedia.org/wiki/Datensicherung>

¹⁵ Vgl. als Erklärung des ganzen Vorgangs das Video von Ralph Friederichs:

<https://www.youtube.com/watch?v=aH815nTIW28>

¹⁶ Vgl.: «Mit Time Machine ein Backup eines Mac erstellen»: <https://support.apple.com/de-ch/HT201250>

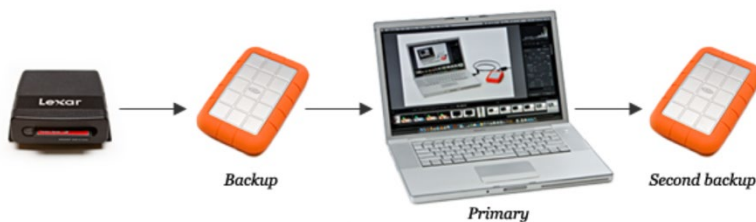
¹⁷ Vgl.: <https://de.wikipedia.org/wiki/Datensicherung>

wieder überschrieben werden, die einzelnen Tage bereits in der nächsten Woche usw. Mit 20 Speichermedien lässt sich ein ganzes Jahr abdecken ($4 + 5 + 11 = 20$).

- Die Tage 1–4 werden jeweils durch die Backups Sohn 1, Sohn 2 bis Sohn 4 gesichert. In der folgenden Woche werden diese jeweils überschrieben.
- Die Wochen 1–5 werden durch die jeweils am Freitag einer jeden Woche gespeicherten Vater-Backups gesichert. Auch diese werden im nächsten Monat überschrieben.
- Die jeweiligen Monate schliesslich werden durch die Grossvater-Backups 1–11 gesichert.

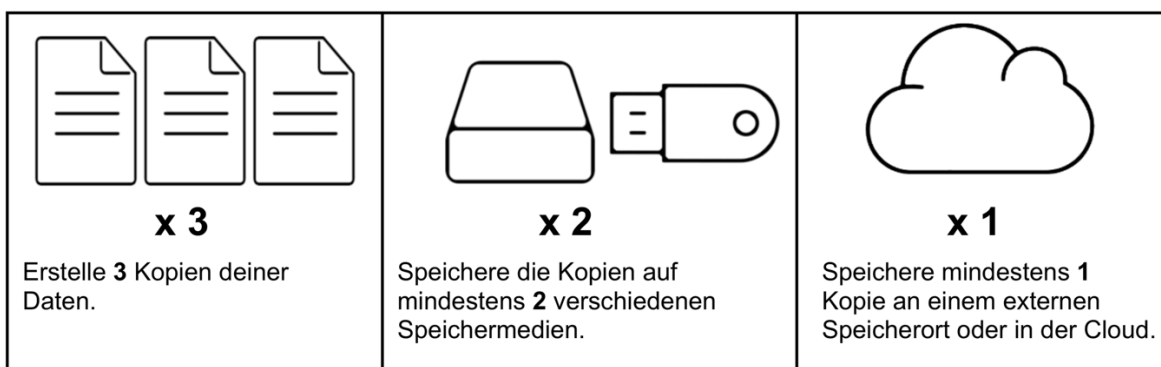
Die 3-2-1 Backup Regel

Mit dem Aufkommen der Digitalkameras wurde die Sicherung der Bilddateien für Fotografen immer wichtiger. Die nachfolgende Abbildung zeigt, wie die Bilddateien der Kamera zuerst auf eine Backup-Festplatte kopiert werden und anschliessend auf den Computer. Von dort werden sie noch auf eine zweite Festplatte kopiert. Die weitere Bearbeitung der Bilddateien findet auf dem Computer statt.



Einfaches Backup-System für Fotografen, vgl. <https://dpbestflow.org/backup/backup-overview>

Die bekannte Backup-Regel «3 Datenkopien, 2 Medien, 1 externes Backup» geht auf den Fotografen Peter Krogh zurück und ist heute elementarer Baustein jeder Datensicherungs- und Datenschutzstrategie¹⁸. Mit dieser einfachen Backup-Regel kann eine Backup-Strategie eines Unternehmens überprüft werden, aber auch für den privaten Gebrauch ist sie geeignet. Wie viele Backups sollen angelegt und wo sollen sie gespeichert werden?



3-2-1 Backup Regel, nach www.serverbase.ch

Drei Kopien bedeutet, dass neben den Originaldaten noch mindestens zwei Kopien vorhanden sein müssen. Die beiden Backups müssen auf zwei verschiedenen Speichermedien liegen. Die Abbildung zeigt dies mit den Symbolbildern einer Festplatte und eines USB-Speichersticks.

¹⁸ Vgl.: <https://www.storage-insider.de/was-ist-die-3-2-1-backup-regel-a-782641/>

Im privaten Umfeld könnten dafür eben diese Speichermedien genutzt werden, in Unternehmen werden es Backup-Server sein. Eines dieser beiden Speichermedien muss an einem externen Ort gelagert werden, dies kann auch ein Cloud-Speicher sein. Bei Verlust der Originaldaten kann bei Anwendung dieser Regel immer auf zwei voneinander unabhängige Kopien zurückgegriffen werden. Damit ist beim Ausfall eines Backups immer noch ein zweites vorhanden.

Backups, SBL-Umgebung (IT.SBL – Informatik Schulen Baselland)

Allen Lehrpersonen wie auch allen Schülerinnen und Schülern steht eine Datei-Ablage zur Verfügung, die Datenspeicher in kantonalen Rechenzentren umfasst. Diese Ablage ist von allen schulinternen Computern nach Anmeldung mit SBL-Account zugänglich. Von ausserhalb und von persönlichen Geräten aus erfolgt der Zugriff mit dem Netzwerkprotokoll WebDAV. Die Datensicherung auf dieser Ablage ist Sache des Betriebs, d.h. des Kantons. IT.SBL verwendet Backup-Server und ermöglicht die Wiederherstellung aller Tage (immer 20 Uhr) des letzten Monats sowie immer den letzten Tag aller Monate des letzten Jahres und immer den letzten Tag der letzten zwei Jahre.

In Office 365 (OneDrive und SharePoint Online) werden Dokumente automatisch gesichert. Gelöschte Dateien bleiben 90 Tage lang im Papierkorb¹⁹ und können während dieser Zeit von den Anwenderinnen und Anwendern selber wiederhergestellt werden. Ein eigentliches Backup gibt es jedoch nicht.

Backups im privaten Umfeld

Private Anwenderinnen und Anwender müssen sich selber um Backups kümmern. Wie im professionellen Umfeld ist eine Abklärung von Bedeutung und Umfang der Daten notwendig. Häufig ist auch hier die automatische Lösung die zuverlässigste. Die Computer-Betriebssysteme von Apple²⁰ und Microsoft²¹ haben eine Backup-Funktionalität bereits eingebaut, zudem gibt es eine grosse Fülle von entsprechenden Software-Lösungen²². Gemäss der 3-2-1-Backup-Regel ist es damit jedoch nicht getan. Externe Speichermedien sind für zusätzliche Sicherungen praktisch, weil sie sich, abgetrennt vom Computer, als Alternative oder Ergänzung zu einem Cloud-Speicher auch extern aufbewahren lassen. Festplatten mit USB-Anschluss lassen sich an jeden Computer anschliessen, selbst iPads können via Adapter auf diese Weise gesichert werden.

Aufgrund von Unachtsamkeit und Fehlmanipulation können Datenverluste nie ganz ausgeschlossen werden. Daher ist Datensicherung via Backup grundlegende Pflicht aller IT-Anwenderinnen und -Anwender. Der im IT-Support beliebte Spruch «Kein Backup? – kein Mitleid!» illustriert, dass das Thema Backup selbst bei automatischer Datensicherung aktuell ist.

¹⁹ Office 365 verwendet einen «ersten» und einen «zweiten» Papierkorb. Dateien, die im Papierkorb gelöscht werden, bleiben bis zum Ablauf der 90 Tage im zweiten Papierkorb («endgültiger Papierkorb»).

²⁰ Vgl.: «Mit Time Machine ein Backup eines Mac erstellen»: <https://support.apple.com/de-ch/HT201250>

²¹ Vgl. «Sichern und Wiederherstellen in Windows 10»: <https://support.microsoft.com/de-ch/help/4027408/windows-10-backup-and-restore>

²² Vgl. Chip, «Backup-Software»: https://www.chip.de/download/39018_Backup-Software/

Synchronisation

Synchronisation von Daten wird in komplexen Datenbanken eingesetzt, um die Verfügbarkeit der Daten zu erhöhen. Im Cloud-Computing, beispielsweise in Office 365, ermöglicht die Synchronisation den Zugriff auf Dokumente von unterschiedlichen Endgeräten aus, wie Smartphones, Tablets und Computern. Die Synchronisation ist auch Voraussetzung für die gemeinsame gleichzeitige Bearbeitung von Dokumenten.



Synchronisieren von Dateien mit OneDrive²³

Die Abbildung symbolisiert die Synchronisierung von Dateien auf verschiedenen Endgeräten (Desktop, Smartphone und Notebook) über den Cloud-Dienst. Dadurch wird sichergestellt, dass auf allen Geräten und in der Cloud die Dateien immer aktuell sind. Eine Änderung beispielsweise auf dem Smartphone bewirkt, dass das entsprechende Dokument auch auf dem Desktop-Computer, dem Notebook und auf der Online-Plattform automatisch aktualisiert wird.

Synchronisierung: Komfort statt Datensicherheit

Das Synchronisieren der verschiedenen Geräte resp. Speicherorte dient vor allem dem Komfort und weniger der Datensicherheit. Obwohl identische Dateien sowohl in der Cloud wie auch lokal auf dem Computer vorhanden sind, wird die Datensicherheit durch die Synchronisierung nicht erhöht. Vielmehr besteht ein grösseres Risiko, dass versehentlich auf allen Geräten und in der Cloud Dateien gelöscht werden. Die Synchronisierung verbindet die verschiedenen Speicherorte und vollzieht alle Änderungen und damit auch das Löschen an allen Speicherorten.

Versionierung

Versionierung oder Versionsverwaltung bedeutet, dass ein System alle Änderungen an Dateien registriert. Bei der Entwicklung von Software ist die Versionsverwaltung ein wichtiges Tool, das die sichere und arbeitsteilige Erarbeitung ermöglicht und alle Entwicklungsstände (Versionen) in einem Archiv mit Zeitstempel und Benutzerkennung ablegt. In professionellen «Dokumenten Management Systemen» für Firmen funktioniert die Versionierung automatisch, dies bedeutet, dass Änderungen an Dateien lückenlos protokolliert werden und die Historie jederzeit, entsprechend der Anforderungen des jeweiligen Betriebes, nachvollzogen werden kann.

In Office 365 der SBL-Umgebung ist die Versionsverwaltung für Office-Dateien aktiviert, dadurch werden automatisch alle Änderungen an den Dokumenten als Versionen gespeichert.²⁴

²³ Vgl. «Synchronisieren von OneDrive-Dateien und -Ordern»:

<https://support.office.com/de-de/article/synchronisieren-von-onedrive-dateien-und-ordnern-3b8246e0-cc3c-4ae7-b4e1-4b4b37d27f68>

²⁴ Vgl. «Funktionsweise der Versionsverwaltung in einer SharePoint-Liste oder -Bibliothek»:

<https://support.office.com/de-de/article/funktionsweise-der-versionsverwaltung-in-einer-sharepoint-liste-oder-bibliothek-0f6cd105-974f-44a4-aadb-43ac5bdfd247>

3.5 Lernziele, Kompetenzen

- [MI.2.1.k](#): Die Schülerinnen und Schüler können Methoden zur Datenreplikation unterscheiden und anwenden (Backup, Synchronisation, Versionierung).
- Teilziele
 - Die Schülerinnen und Schüler kennen die verschiedenen Methoden der Datenreplikation.
 - Die Schülerinnen und Schüler können Methoden der Datenreplikation zur Erhöhung der Datensicherheit anwenden.

3.6 Unterrichtsidee

a. Ablauf

- Lektion 1: Thema «Backup»

Was ist ein Backup? Wie kann Datenverlust vermieden werden? Was muss ich wissen, um ein Backup meiner Daten zu erstellen? Wie kann ich die 3-2-1-Backup-Regel anwenden?

t	Sozialform	Aktivitäten der Lehrperson	Aktivitäten der Schülerinnen und Schüler	Material
10'	EA/Plenum	Einstieg Was bedeutet «Backup»? Wozu dient es? Weshalb ist es notwendig? Wie wird ein Backup erstellt? «Hat jemand von euch ein Backup?» «Ich zeige euch nun ein Foto eines Backups. Was erfahren wir vom Foto über Backups?»	Diskussion zum Thema SuS bearbeiten Arbeitsauftrag Abschliessende Diskussion zu Foto «Backup-Festplatte».	1_Einstieg_Backup.docx
30'	EA/Plenum	Arbeitsauftrag gemäss Arbeitsblatt Die Grundlagen der Backup-Regel können von der Lehrperson erklärt werden oder die SuS erhalten einen entsprechenden Recherchier-Auftrag. Auftrag «Entwirf eine persönliche Backupstrategie nach der 3-2-1-Backup-Regel, die du für deine Projektarbeit anwenden willst.»	SuS erarbeiten sich eine Backupstrategie nach der 3-2-1 Backupregel SuS erstellen einen eigenen Backup-Plan für ihre Daten und wenden die Backup-Regel an.	2_Backup_Regel.docx
5'	Plenum	Kurzpräsentation der Ergebnisse und Fazit	Beteiligen sich am Gespräch und bringen ihre Sicht ein.	

c. Leistungsüberprüfung/Bewertung

d. Differenzierung, Erweiterung

- Brainstorming oder Mindmap zum Thema «Backup» als Einstieg
- Bedeutungsquadrat «digitale Daten», vgl. Arbeitsblatt 3_Bedeutungsquadrat.docx
- «Kultur im Unterricht vorleben»:

«Die Datenreplikationsmechanismen Backup, Synchronisation und Versionierung können im Unterricht durchaus auch vermittelt werden, indem eine entsprechende Kultur vorgelebt wird. Gelegentliche Backups können mit den Schülerinnen und Schülern zusammen angelegt werden. Beim Verfassen von Textdokumenten und Präsentationen werden bewusst verschiedene Versionen angelegt. Und falls unterschiedliche digitale Geräte zur Verfügung stehen, kann auch die Synchronisation von Dateien erprobt werden. Deutlicher sichtbar wird die Synchronisation, wenn z.B. Fotos mit einem Smartphone aufgenommen werden und gleich automatisch in einer entsprechenden Cloud erscheinen. Im Schulumfeld werden Clouds immer wichtiger. Es gehört zu einem zeitgemässen Informatik-Unterricht, die aktuellen Entwicklungen zu verfolgen und deren Möglichkeiten und Risiken zu thematisieren – auch wenn diese im Lehrplan noch nicht explizit erwähnt sind.»²⁷

e. Fächerübergreifend

- Anwendungskompetenzen:
 Bei der Arbeit mit Office-Dateien auf Datensicherheit hinweisen und Methoden anwenden.

²⁷ Vgl.: Waldvogel, B.: Die Datenflut bändigen, Datenstrukturen Zyklus 3, Schaffhausen 2019, S. 33f.
https://mia21.ch/pluginfile.php/271/mod_resource/content/2/MIA21_2019_Datenstrukturen_Z3.pdf

4 Programmieren 3: Modul «Algorithmen anwenden» (MI.2.2)

4.1 Darum geht es

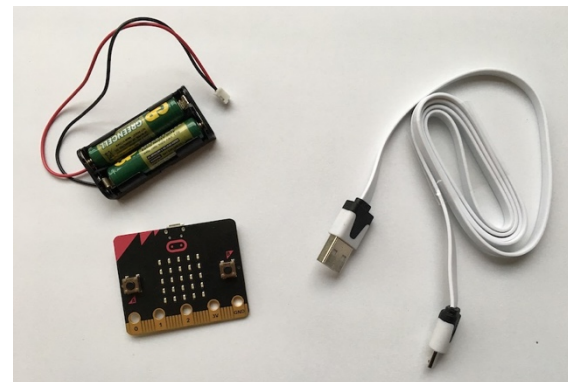
Den Einplatinencomputer «micro:bit», den die Schülerinnen und Schüler im zweiten Schuljahr kennen und programmieren gelernt haben, wollen wir nun fürs Physical Computing einsetzen, um eine Verbindung zwischen der physischen und der virtuellen Welt herzustellen. Die Schülerinnen und Schüler sollen so die Grundlagen der Informatik noch vertiefter begreifen.

Zuerst repetieren wir Schleifen, bedingte Anweisungen, Parameter, Variablen und Unterprogramme. Dazu nutzen wir wiederum die scratch-ähnliche Programmierungsumgebung [MakeCode](#). Anschliessend sollen sich die Jugendlichen mit einem eigenen Projekt vertieft auseinandersetzen und verschiedene Algorithmen zur Lösung des gleichen/ähnlichen Problems miteinander vergleichen.

Wir arbeiten in diesem Modul nicht nur mit dem 5x5-LED-Bildschirm, sondern auch mit den diversen Sensoren des micro:bits.

4.2 Checkliste zur Vorbereitung

- ☐ Computerraum bzw. Laptopwagen reservieren;
1 Gerät pro 2 Schüler/-innen
- ☐ Beamer
- ☐ 1 micro:bit pro 2 Schüler/-innen mit USB-Kabel und evtl. Batteriepack
- ☐ Bastelmaterial (z. B. Nägel, Schrauben, Gefässe, Erde, Stoff, Garn, Krokodilklemmen, LED...)
- ☐ «Programmieren 3» mit folgendem Inhalt:
 - 1.0_Programmier-Konzepte.pptx
 - 1.1_Einstieg_A.docx
 - 1.1_Einstieg_B_Loesungsvorschlaege.docx
 - 1.1_Einstieg_B.docx
 - 2.1_Leitfaehigkeit_Loesungsvorschlag.docx
 - 2.1_Pflanzenwaechter_Loesungsvorschlag.docx
 - 2.1_Pflanzenwaechter.docx
 - 2.2_Schrittzaehler_Loesungsvorschlag.docx
 - 2.2_Schrittzaehler.docx
 - 2.3_Data_Logging.docx



micro:bit mit USB-Kabel und Akkupack

4.3 Bedeutung in der Informatik

Physical Computing soll interaktive Systeme erschaffen, welche die Welt um uns herum über Sensoren wahrnehmen und darauf reagieren können. Physical Computing erfordert rechnerisches und fächerübergreifendes Denken, das Entwickeln von Strategien zur Lösung eines Problems und die Gestaltung von Systemen, wobei auf für die Informatik wesentliche Konzepte zurückgegriffen wird.

In der Informatik geht es nicht nur um das Erlernen von Technologie, sondern Logik, Problemlösung und Kreativität sind wesentliche Konzepte dieser Wissenschaft. Die Verknüpfung dieser Konzepte mit der wirklichen Welt führt zum «Physical Computing» und ermöglicht es den Schülerinnen und Schülern, dass sich ihnen die reale Welt und der Computer auf eine neue Weise erschliessen.

4.4 Theorie

Computational Thinking

«Wenn man an Computer und digitale Geräte denkt, kommen einem wahrscheinlich in erster Linie Laptops, Desktops, Smartphones und Tablets in den Sinn. Dies ist natürlich korrekt, diese Geräte machen aber nur einen kleinen Teil der digital vernetzten Welt aus. So benutzen wir tagtäglich bewusst und unbewusst eine Vielzahl von Computern, sei es im Self-Checkout im Supermarkt, beim Betreten eines Gebäudes, im Auto, im Kino, im Fitnesscenter usw.

Wenn wir die Informatik verstehen und die Möglichkeiten von Computern erkunden möchten, müssen wir das gängige Bild eines Computers ablegen und eher von «Computing» sprechen. Mit Computing ist dabei die automatisierte Informationsverarbeitung gemeint, also alle Tätigkeiten, die mithilfe von Algorithmen auf Computersystemen ausgeführt werden. Dabei können diese Computersysteme jede technisch mögliche physische Form annehmen, die für die Tätigkeit notwendig ist: z.B. ein Fitnessarmband, ein Babyphone, elektronische Anzeigen an Haltestellen, Zugangssysteme in Gebäuden, Gamekonsolen, Smart-TVs, Staubsaugerroboter, Analysegeräte in Arztpraxen, Alarmanlagen, moderne Prothesen und Implantate. Computing umfasst den Entwurf und die Entwicklung von Hardware und Software sowie die Strukturierung und Verarbeitung verschiedener Arten von Informationen.

Mit «Computational Thinking» ist die Problemlösekompetenz gemeint, die es im Computing braucht: ein Ziel zu definieren, das Problem in Teilprobleme aufzubrechen und eine Lösung zu implementieren, welche anschliessend getestet und verbessert wird. Die Lösung soll dabei von einem Computer ausführbar sein.

«Physical Computing» ist ein Bereich des Computing, welcher die physische Welt mit der virtuellen Welt von Computern verbindet. Es geht also nicht nur um die Computer selber, sondern auch um die Interaktion mit der physischen Aussenwelt. Als zentrales Konzept gilt der Informationsfluss, der von der physischen Welt in die virtuelle Welt gelangt, dort verarbeitet wird und wiederum in die physische Welt ausgegeben wird.

Natürlich funktioniert fast jeder Computer nach dem «EVA-Prinzip», Eingabe – Verarbeitung – Ausgabe: ein Laptop hat beispielsweise Maus und Tastatur für die Eingabe, einen Prozessor für die Verarbeitung und einen Bildschirm und Lautsprecher für die Ausgabe. Physical Computing geht aber darüber hinaus und befasst sich noch tiefer mit den Eingabe- und Ausgabemöglichkeiten und der Interaktion mit der physischen Welt über Sensoren und Aktoren. Es geht dabei auch hauptsächlich darum, solche interaktiven Computersysteme mit kleinen Computern selber zu entwerfen, zu entwickeln und zu programmieren.

Roboter sind sehr beliebt als didaktisches Mittel im Informatik- und Technikunterricht in der Volksschule. Bezüglich Computerhardware, Sensoren, Aktoren sowie Programmierkonzepten gibt es beim Thema Physical Computing keinen Unterschied zur Robotik – in beiden Gebieten verbindet man die physische mit der virtuellen Welt. Ob ein Projekt ein Robotikprojekt ist, hängt eher von der Anwendung des Endprodukts ab. Roboterprojekte befassen sich eher mit Systemen, die sich autonom in der Umwelt orientieren und/oder physische Arbeit für den Menschen verrichten. Oftmals sind die Produkte Roboterarme, kleine autonome Fahrzeuge und Drohnen sowie humanoide Roboter. In der Roboterprogrammierung liegt der Schwerpunkt häufig bei der Lösung von Problemen der autonomen Navigation des Roboters und der künstlichen Intelligenz.

Produkte im Bereich des Physical Computings können alles Mögliche sein: eine automatische Bewässerungsanlage für die Zimmerpflanze, ein Fitnessarmband, eine interaktive

Kunstinstallation, eine automatische Zugangskontrolle für die Katzentür, E-Textilien, ein interaktiver Geburtstagskuchen usw. Die benötigten Kompetenzen in Programmierung sowie Hardware- und Software-Fachwissen sind im Bereich des Physical Computings und in der Robotik identisch. Wer sich also mit Physical Computing auseinandersetzt, kann problemlos in das Thema Robotik einsteigen und umgekehrt.»²⁸

Problemlöseprozesse

Dort, wo etwas Neues geschaffen wird, werden Problemlöseprozesse durchlaufen. Sei dies nun im textilen, bildnerischen oder technischen Gestalten, in der Musik oder eben im Informatikunterricht – überall führt ein Entwicklungs- und Gestaltungsprozess (meist ein iterativer Prozess) von der Idee zum Endprodukt. Auch wenn sich Methoden und Modell je nach Fachgebiet unterscheiden, sind folgende drei Hauptphasen allgemein anwendbar: Think, Make, Improve

«In diesen drei Phasen können folgende Tätigkeiten stattfinden [...]:

- **Think**
Brainstorming, Diskussion, Prognostizieren, Sammeln von Material, Expertise identifizieren, Gruppen bilden (oder alleine arbeiten), Zielsetzung, Skizzieren, Abgrenzen, Diagramme zeichnen, Recherchieren, Planen.
- **Make**
Spielen/Ausprobieren, Bauen, Basteln, Kreieren, Programmieren, Experimentieren, Konstruieren, Auseinandernehmen, Vorgehensweisen und Materialien testen, andere beobachten, Code kopieren, Code teilen, Prozess dokumentieren, Probleme suchen und finden, Fragen stellen, Fehler beheben.
- **Improve**
 - Wenn es nicht funktioniert oder das Team steckenbleibt: Recherchieren, Ausdiskutieren im Team, Diskutieren mit Kollegen, das Problem von einem anderen Blickwinkel betrachten, andere Materialien verwenden, einzelne Komponenten des Projektes verändern, diskutieren, ob und wie ein ähnliches Problem zu einem früheren Zeitpunkt gelöst wurde, herumspielen, ein ähnliches Projekt finden zum Analysieren oder Auseinandernehmen, eine Expertin oder einen Experten fragen, cool bleiben, frische Luft schnappen, darüber schlafen.
 - Wenn das Team «fertig» ist: Möglichkeiten finden, um das Produkt zu verbessern oder weiterzuentwickeln. Fragestellungen: Wie kann das Produkt so gestaltet werden, dass es schneller, langsamer, besser, genauer, schöner, ökologischer, cooler, stärker, smarter, flexibler, grösser, kleiner, effizienter, kostengünstiger, verlässlicher, leichter, eleganter, einfacher zu benutzen ist?

Schliesslich soll das Produkt kommuniziert und die Expertise geteilt werden. Gemäss Papert und der konstruktivistischen Lerntheorie fördert der Kreislauf «Making» und «Making things better» das Verständnis.»²⁹

Weiteres theoretisches Hintergrundwissen zu **Informatiksystemen**, zum **micro:bit** und **Programmieren mit MakeCode** sowie ein Input zu **Variablen und Unterprogrammen** finden sich in der Broschüre zum Modul «Programmieren 2».

²⁸ https://mia.phsz.ch/pub/Informatikdidaktik/PhysicalComputing/PhysicalComputing_PHSZ_DA_V2.0.pdf, S. 5

²⁹ https://mia.phsz.ch/pub/Informatikdidaktik/PhysicalComputing/PhysicalComputing_PHSZ_DA_V2.0.pdf, S. 45

4.5 Lernziele, Kompetenzen

- Die Schülerinnen und Schüler können verschiedene Algorithmen zur Lösung desselben Problems vergleichen und beurteilen (z.B. lineare und binäre Suche, Sortierverfahren). ([MI.2.2.i](#))
- Die Kompetenzen MI.2.2.c-f des 2. Zyklus und die Kompetenzen MI.2.2.g, MI.2.2.h und MI.2.3.i des 1. und 2. Schuljahres des 3. Zyklus sind als Repetition oder Vertiefung ebenfalls in diesem Modul enthalten:
 - [MI.2.2.c](#): Die Schülerinnen und Schüler können Abläufe mit Schleifen und Verzweigungen aus ihrer Umwelt erkennen, beschreiben und strukturiert darstellen (z.B. mittels Flussdiagramme).
 - [MI.2.2.d](#): Die Schülerinnen und Schüler können einfache Abläufe mit Schleifen, bedingten Anweisungen und Parametern lesen und manuell ausführen.
 - [MI.2.2.e](#): Die Schülerinnen und Schüler verstehen, dass ein Computer nur vordefinierte Anweisungen ausführen kann und dass ein Programm eine Abfolge von solchen Anweisungen ist.
 - [MI.2.2.f](#): Die Schülerinnen und Schüler können Programme mit Schleifen, bedingten Anweisungen und Parametern schreiben und testen.
 - [MI.2.2.g](#): Die Schülerinnen und Schüler können selbstentdeckte Lösungswege für einfache Probleme in Form von lauffähigen und korrekten Computerprogrammen mit Schleifen, bedingten Anweisungen und Parametern formulieren.
 - [MI.2.2.h](#): Die Schülerinnen und Schüler können selbstentwickelte Algorithmen in Form von lauffähigen und korrekten Computerprogrammen mit Variablen und Unterprogrammen formulieren.
 - [MI.2.3.i](#): Die Schülerinnen und Schüler kennen die wesentlichen Eingabe-, Verarbeitungs- und Ausgabeelemente von Informatiksystemen und können diese mit den entsprechenden Funktionen von Lebewesen vergleichen (Sensor, Prozessor, Aktor und Speicher).

4.6 Unterrichtsidee

Die Unterrichtsideen stammen vorwiegend aus dem Heft [«Computational Thinking mit BBC Micro:bit. Digitale Bildung in der Sekundarstufe»](#), das unter Mitwirkung verschiedener Pädagogischer Hochschulen in Österreich herausgegeben wurde. Sämtliche Projekte sind auch in einem [Wiki](#) erklärt, das diverse Hilfestellungen anbietet. Das Werk ist lizenziert unter einer [Creative Commons Namensnennung 4.0 International Lizenz](#).

a. Ablauf

- Repetitionsübung in zwei Schwierigkeitsgraden:
 - «Smile!» (einfacher): Die SuS programmieren ein Smiley (und Frowney) und repetieren die Arbeit mit der Programmierungsumgebung MakeCode.
 - «Kopf oder Zahl» (anspruchsvoller): Einstieg über Experiment «Münzwurf» (Bezug möglich zu mathbuch 2, LU31: Gesetze des Zufalls; mathbuch 3, LU18: Roulette und Zahlenlotto); Repetition Programmierungsumgebung MakeCode, Schleifen, bedingten Anweisungen, Operatoren und Variablen; Kennenlernen des Zufallsgenerators.
- Projekt mit dem micro:bit, Vergleichen von Algorithmen – Auswahl:
 - Pflanzenwächter bzw. (die einfachere Alternative) Leitfähigkeitsprüfer
 - Data-Logging
 - Schrittzähler

t	Sozialform	Aktivitäten der Lehrperson	Aktivitäten der Schülerinnen und Schüler	Material
45'		Einstieg: Repetition Schwierigkeitsgrad der Aufgabe auswählen, Coaching Diskussionsleitung: Programmier-Konzepte, Hilfestellung: Folien Ausblick auf Unterrichtseinheit und Input zu Computational Thinking	Die SuS schreiben Code. Die SuS nennen die Programmier-Konzepte, die sie im letzten SJ kennen gelernt haben.	1.1_Einstieg_A.docx oder 1.1_Einstieg_B.docx und 1.1_Einstieg_B_Loesungsvorschlaege.docx 1.0_Programmier-Konzepte.pptx
		Projekt «Pflanzenwächter» bzw. die einfachere Variante «Leitfähigkeit» Erweiterung: Projekt Data Logging: Tageswerte Temperatur oder Lichtstärke mit dem micro:bit abrufen, sammeln bzw. speichern und mit EXCEL auswerten.	SuS arbeiten nach Auftrag.	2.1_Pflanzenwaechter.docx und 2.1_Pflanzenwaechter_Loesungsvorschlag.docx bzw. 2.1_Leitfaehigkeit_Loesungsvorschlag.docx Div. Bastelmaterial Erweiterung: 2.3_Data_Logging.docx
		Projekt «Schrittzähler» Bemerkung: Wenn mit der Eingabe «geschüttelt» gearbeitet wird, müssen die Schritte sehr deutlich ausgeführt werden, damit der Schrittzähler richtig zählt. Fächerübergreifend: Sport, Biologie, Textiles Gestalten Erweiterung: Warnton nach einer gewissen Anzahl Schritte (externer Summer/Lautsprecher muss angeschlossen und programmiert werden)	SuS arbeiten nach Auftrag.	2.2_Schrittzaeher.docx und 2.2_Schrittzaeher_Loesungsvorschlag.docx Evtl. Bastelmaterial

b. Material

- micro:bit-Sets (Bezugsquelle: z. B. educatec.ch)
- Bastelmaterial siehe Aufträge
- Kopien/Arbeitsaufträge siehe Planung

c. Leistungsüberprüfung/Bewertung

- Ein Beispiel für ein Bewertungsraster findet sich im Modul «Programmieren 1».

d. Differenzierung, Erweiterung

- Im Heft [Computational Thinking mit dem BBC micro:bit](#) eignen sich zum Beispiel auch folgende Projekte:
 - Reaktionszeit-Messgerät (S. 89)
 - Elektronische Sonnenuhr (S. 97)
 - Animiertes Micro-Buch (S. 33)
 - Audioalarm (S. 37) und Nachrichten senden und empfangen (S. 49): allenfalls ohne Lautsprecher
 - Clever raten (S. 77): Binär-Suche
 - Schere, Stein, Papier (S. 93), falls das Schere-Stein-Papier-Spiel aus dem Modul «Programmieren 2» in der 2. Klasse noch nicht programmiert wurde (Programmieren 2: 3.1_Bedingungen_Aufg.1)
- Die Pädagogische Hochschule St. Gallen hat Challenge-Cards für den micro:bit herausgegeben.
- Ideensammlung für weitere Projekte:
 - Würfel: <https://www.101computing.net/bbc-microbit-roll-the-dice/>
 - Tetris: <https://www.101computing.net/bbc-microbit-tetris-game/>
 - Gold Rush: <https://www.101computing.net/gold-rush/>
 - Blitz und Donner: <https://www.101computing.net/bbc-microbit-lightning-distance-calculator/>
 - Whack-a-Mole: <https://www.101computing.net/bbc-microbit-whack-a-mole/>
 - Alarmanlage: <https://make.techwillsaveus.com/microbit/activities/combo-lock/>
 - MicroBike (Game Controller): <https://musab.netlify.com/projects/microbike/>
 - Reaktionszeit: <https://makecode.microbit.org/projects/reaction-time>
 - Wasserpumpe: <https://www.youtube.com/watch?v=jANCdtkJAKY>
 - Weitere Projektideen von microbit.org: <https://microbit.org/de/ideas/>
 - Weitere Projekte von 101 Computing: <https://www.101computing.net/category/bbc-microbit/>
 - 100 Projekte von der Uni Potsdam: <https://www.cs.uni-potsdam.de/~mprz/Projekte.html>

e. Fächerübergreifend

- Mikrocontroller und Physical Computing-Projekte: bildnerisches, textiles und technisches Gestalten, Naturwissenschaften, MINT, Sport (Schrittzähler), vgl.: Assaf, D. (2018), Physical Computing – Verbindung der physischen mit der virtuellen Welt
- Physical Computing auch als Projekt in Projektwoche umsetzbar, (elektronisches) Lerntagebuch führen (z. B. in OneNote-Kursnotizbuch)

f. Hinweise

- Wird mit dem Lehrmittel einfach Informatik, Band Programmieren gearbeitet, werden die Kapitel 2, 5 und 6 empfohlen. Dort werden die Algorithmen-Kompetenzen des LP21 abgedeckt, jedoch ohne Bezug bzw. Anwendungen zu Physical Computing.

5 Systeme 3: Modul «Internet und Verschlüsselung» (MI.2.3)

5.1 Darum geht es

Unsere Schülerinnen und Schüler unterscheiden im Alltag oft nicht zwischen dem Internet als Infrastruktur und seinen Diensten. Deswegen gehen wir in diesem Modul den Fragen nach, wie das Internet funktioniert und was genau geschieht, wenn zum Beispiel Nachrichten übermittelt werden. Dabei betrachten wir technische Aspekte, werfen einen Blick auf eine Seekabelkarte und überlegen uns, wie Musik oder Filme scheinbar über die Luft direkt auf unser Handy oder Tablet gelangen.

Bei der Nutzung des Internets stellt sich immer wieder die Frage nach der Sicherheit: Wie können geheime Daten auch wirklich geheim bleiben? Die Schülerinnen und Schüler haben sich bereits im Modul «Systeme 1» mit der unverschlüsselten Datenspeicherung befasst. Nun sollen sie die Risiken unverschlüsselter Datenübermittlung und -speicherung noch besser abschätzen lernen.

5.2 Checkliste zur Vorbereitung

- ☐ «Systeme 3» mit folgendem Inhalt:
 - 1.1_Wie_funktioniert_das_Internet.pptx
 - 2.1_Verschlüsselung.pptx
 - 3.1_Spielanleitung_Coprotrac_Papp.pdf
 - 3.2 Corona Proximity Tracing Paper App (Ordner)
 - 4.1_Auftrag_Internet_A.docx
 - 4.1_Auftrag_Internet_B.docx
- ☐ Computerraum/Laptopwagen reservieren

5.3 Bedeutung in der Informatik

Das Internet und seine Dienste

«Die Begriffe Internet und World Wide Web werden im Sprachgebrauch häufig gleichgesetzt. Doch technisch besteht ein erheblicher Unterschied zwischen beiden. Das Internet ist ein weltumspannendes Netz von vielen einzelnen Computernetzwerken. Zahlreiche Dienste erwecken diese Infrastruktur erst zum Leben – zum Beispiel E-Mail, Chats, Dateiübertragung, [... Filme-Streamen oder auch Videokonferenzen]. Einer der bekanntesten Dienste ist das World Wide Web (WWW), das die Übertragung von Webseiten ermöglicht. Zur Anzeige brauchen Nutzer einen Browser wie den Internet Explorer, Safari [...oder Chrome]. Für alle Dienste sind straffe Standards notwendig. Denn die im Internet verbundenen Rechner sind höchst unterschiedlich: Einige könnten schon im Technikmuseum stehen, andere haben die neueste Ausrüstung an Bord. Auch bei Software und Betriebssystemen ergeben sich riesige Unterschiede.»³⁰

³⁰ https://www.focus.de/digital/internet/internetgeschichte/tid-13637/vor-20-jahren-internet-versus-world-wide-web_aid_379722.html

Verschlüsselungsverfahren

«In der Computerwelt handelt es sich bei Verschlüsselung um die Konvertierung von Daten von einem lesbaren Format in ein verschlüsseltes Format, das erst nach einer Entschlüsselung wieder gelesen oder verarbeitet werden kann.

Verschlüsselung ist der grundlegende Baustein der Datensicherheit und die einfachste und wichtigste Art und Weise, um zu gewährleisten, dass die Informationen eines Computersystems nicht zu betrügerischen Zwecken gestohlen und gelesen werden. [...] Diese Informationen können von Zahlungsdaten bis hin zu persönlichen Informationen reichen. [...]

Neben den offensichtlichen Vorteilen, die der Schutz persönlicher Daten vor Diebstahl oder Offenlegung mit sich bringt, bietet die Verschlüsselung auch die Möglichkeit, die Authentizität von Informationen sowie ihren Ursprung nachzuweisen. Mithilfe von Verschlüsselung lässt sich die Herkunft einer Nachricht überprüfen und nachweisen, dass die Nachricht während der Übertragung nicht verändert wurde.

Die Grundlagen der Verschlüsselung beruhen auf dem Konzept von Verschlüsselungsalgorithmen und Schlüsseln. Gesendete Daten werden mithilfe eines Algorithmus verschlüsselt und können nur mit dem passenden Schlüssel entschlüsselt werden. Ein solcher Schlüssel kann etwa auf dem empfangenden System gespeichert oder zusammen mit den verschlüsselten Daten übertragen werden.»³¹

5.4 Theorie

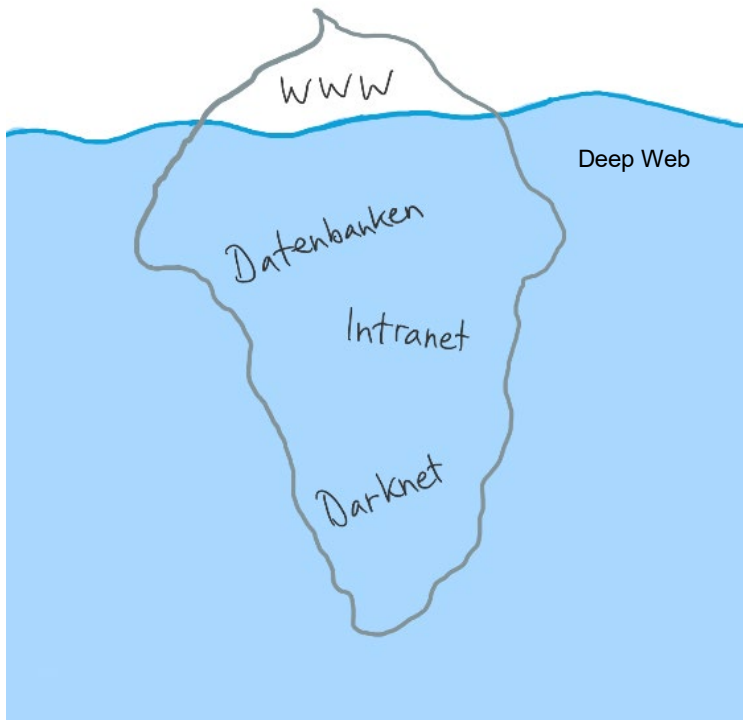
Das Internet ist ein weltweites Netzwerk von Computern. Sofern zwei oder mehr Computer über einen Internetanschluss verfügen, können sie über das Internet miteinander verbunden werden – unabhängig davon, wo auf der Welt sie stehen. «Dieses grosse Netzwerk besteht aus vielen einzelnen Netzwerken. Zuhause nutzt man das Netzwerk des **Providers**, also einer Dienstleistungsfirma, die dem User einen Zugang zum Internet bereitstellt.»³² In der Schweiz gehören die Telefonanbieter Swisscom, Salt., upc oder Sunrise zu den grossen Providern.

Der grösste Teil des Internets befindet sich im **Deep Web**, einem Teil, der sich über normale Suchmaschinen nicht finden lässt. Dazu gehören zum Beispiel Netzwerke, «die nur bestimmten Usern vorbehalten sind. Im firmeneigenen **Intranet** werden den Mitarbeitern Informationen zur Verfügung gestellt, die nicht für die Öffentlichkeit bestimmt sind. Vor allem für grössere Unternehmen, Institutionen und Behörden ist das oft der einfachste Weg, interne Entwicklungen und Neuigkeiten schnell für jeden Mitarbeiter zugänglich zu machen.»³³ Auch Datenbanken von Universitäten, Forschungseinrichtungen oder Museen (vgl. Modul «Daten 2») oder das **Darknet** (Zugriff über spezielle Browser, Ort für illegale Onlineshops, Drogenhandel, Waffenhandel, Falschgeld, anonyme Chat-Rooms...) sind Teil des Deep Webs.

³¹ <https://www.kaspersky.de/resource-center/definitions/encryption>

³² https://www.planet-wissen.de/technik/computer_und_roboter/das_internet/pwieinternetfuereinsteiger100.html

³³ https://www.planet-wissen.de/technik/computer_und_roboter/das_internet/pwieinternetfuereinsteiger100.html



Das Internet: Stellt man sich das Internet als Eisberg vor, ist das WWW nur ein kleiner Teil des Internets, der bedeutend grössere Teil befindet sich unter der Oberfläche, im sogenannten Deep Web.³⁴

Im Alltag werden die Wörter Internet und World Wide Web meist synonym verwendet. Dies ist jedoch nicht korrekt. Während das Internet das Grundgerüst darstellt, gehört das WWW zu den **Internetdiensten**, wie zum Beispiel auch E-Mail, Dateiverwaltung, Cloud, Diskussionsforen, Chat, Telefonie, Fernsehen, Radio oder Spiele.³⁵

Mit einem **Browser**, wie zum Beispiel Safari, Google Chrome, Firefox oder Internetexplorer, «können Webseiten dargestellt werden. Diese Webseiten liegen auf Servern und sind von dort jederzeit abrufbar.»³⁶ In der Adresszeile des Browsers wird der Name der Webseite eingetippt. Das Kürzel **http** (Hypertext Transfer Protocol) steht für den Übertragungsstandard des WWW; wird mit **https** (Hypertext Transfer Protocol Secure) gearbeitet, bedeutet dies, dass die Kommunikation verschlüsselt wird.

http und https funktionieren mit dem «Frage-Antwort-Prinzip. Der Computer des Nutzers stellt eine Anfrage nach einer Seite an den Server des Providers. Der Provider schickt die Anfrage weiter über Knotenpunkte im Netz, die den genauen Weg zu dem Standort der Webseite vermitteln. Irgendwann trifft die Anfrage auf den Zielsever, auf dem die angeforderten Daten liegen»³⁷ und von dort aus werden sie wiederum zurückgeschickt, sodass auf dem Computer der Nutzerin bzw. des Nutzers die angewählte Webseite erscheint.

«Ein **Server** ist ein Speicher, auf dem Inhalte von Webseiten, E-Mails oder Dateien abgelegt sind. Zusätzlich ist dort ein Programm installiert, das es erlaubt, auf die Daten des Servers zuzugreifen.

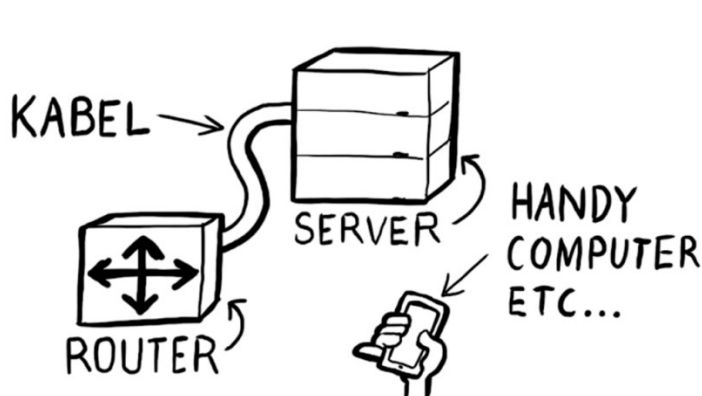
³⁴ Vgl. auch <https://www.giga.de/extra/internet/specials/deep-web-so-kommt-ihr-in-den-geheimen-teil-des-internets/>

³⁵ Vgl. auch <https://de.wikipedia.org/wiki/Internetdienst>

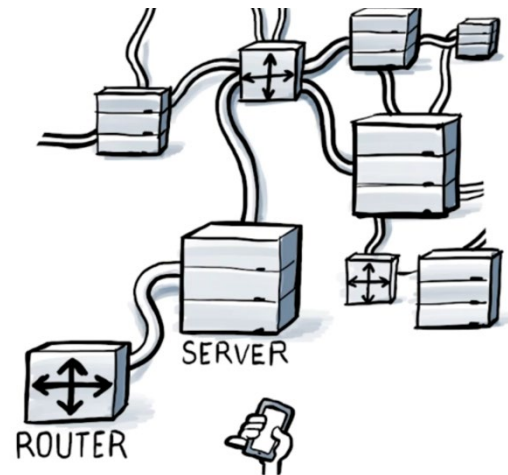
³⁶ https://www.planet-wissen.de/technik/computer_und_roboter/das_internet/pwieinternetfuereinsteiger100.html

³⁷ https://www.planet-wissen.de/technik/computer_und_roboter/das_internet/pwieinternetfuereinsteiger100.html

Suchmaschinen [...] können so die Inhalte von Webseiten durchforsten und die gewünschten Informationen, die der User in die Suchmaske eingegeben hat, herausfiltern.»³⁸



Datenpakete im Internet: Datenpakete werden mittels Router vom Handy zum Server transportiert.³⁹



Datenpakete im Internet: Die Router leiten die Datenpakete so lange weiter, bis sie bei der angegebenen IP-Adresse ankommen.⁴⁰

Damit eine Abfrage den richtigen Weg durchs Internet findet, werden **Router** eingesetzt. Dabei besteht das grundlegende (und «revolutionäre») Prinzip darin, dass die Nachrichten in einzelne Datenpakete aufgeteilt werden. Ein solches Paket enthält «die Quelle des Paketes, das Ziel des Paketes, die Länge des Datenteils, die Paketlaufnummer, die Klassifizierung des Paketes und den Datenteil»⁴¹. Die einzelnen Datenpakete werden auf unterschiedlichen und unabhängigen Wegen im Netz von Router zu Router weitergesendet, bis sie beim Server bzw. wieder beim Computer des Nutzers ankommen und dort erneut zusammengesetzt werden. Als unabhängige Einheiten können sie unterwegs zwischengespeichert werden. Die Kommunikationssprache wird **TCP/IP** (Transmission Control Protocol/Internet Protocol) genannt. Jedes Gerät (Computer, Tablet, Handy, Server, Router, Smart-TV etc.) hat eine eigene **IP-Adresse**, an welche die Datenpakete adressiert werden.⁴²

Mittels WLAN und Router wird auch die Verbindung zwischen Computer, Tablet oder Handy mit dem Internet hergestellt. Ist kein WLAN vorhanden, verbinden sich mobile Geräte über die SIM-Karte mit dem nächsten Mobilfunkmasten, um ins Internet zu gelangen.

Weil Daten von jedermann veröffentlicht und somit für andere zugänglich gemacht werden können, ist das Internet auch die grösste Informationsquelle, die ununterbrochen und sehr intensiv genutzt

³⁸ https://www.planet-wissen.de/technik/computer_und_roboter/das_internet/pwieinternetfuereinsteiger100.html, vgl. auch Modul «Systeme 1, Suchmaschinen»

³⁹ <https://www.srf.ch/sendungen/myschool/wie-funktioniert-das-internet>

⁴⁰ <https://www.srf.ch/sendungen/myschool/wie-funktioniert-das-internet>

⁴¹ <https://de.wikipedia.org/wiki/Paketvermittlung>

⁴² Vgl. auch <https://www.youtube.com/watch?v=4VxPazIA0Zc>

wird. Die Internetsuche ist dabei «die häufigste Aktivität, die am Computer oder an anderen vernetzten Geräten durchgeführt wird.»⁴³

Sobald man sich entscheidet, Webseiten im World Wide Web zu veröffentlichen, stehen sie auch anderen Personen zur Verfügung. Dies funktioniert, «weil für die Erzeugung der Dokumente die gleiche Sprache (Kodierung) verwendet wird. Diese in den Jahren 1989 bis 1991 entwickelte Sprache heisst **HTML** (Hypertext Markup Language) und legt die Strukturierung der digitalen Dokumente fest. In dieser Sprache verfasste Dokumente heissen auch HTML-Seiten oder Webseiten. Mittlerweile gibt es Milliarden von Webseiten.»⁴⁴

Die Datenpakete reisen also von Router zu Router, ohne dass wir bestimmen können, welchen Weg sie nehmen, und ohne dass wir Einfluss darauf haben, dass sie nur über sichere Knoten geschickt werden. «Mit sogenannten «packet analyzer» oder «packet sniffer» (Software zur Analyse von Netzwerken auf Auffälligkeiten im Datenverkehr) können die Datenpakete ausspioniert werden. Und mit etwas technischem Know-how können die Datenpakete auch «von Hand» wieder zu den Originaldaten zusammengesetzt werden.»⁴⁵ Jede Kommunikation kann also theoretisch abgehört werden, sprich wenn eine Textmitteilung per SMS oder eine E-Mail (oder auch ein Brief) verschickt wird, kann der Inhalt durch Unbefugte gelesen werden. Der einfachste Weg, die Daten zu schützen, ist, diese zu verschlüsseln. Solange nur der/die Empfänger/-in den Schlüssel kennt, kann niemand Unbefugtes die Nachricht lesen.

Bei klassischen **Verschlüsselungsverfahren** besitzen Sender/-in und Empfänger/-in einen gemeinsamen geheimen Schlüssel. Beim Senden wird der Klartext mit diesem Schlüssel codiert, beim Empfangen wird der Geheimtext mit dem gleichen Schlüssel decodiert. Man spricht von zwei Verschlüsselungsklassen: Bei der **Substitution** werden Symbole durch andere Symbole ersetzt: Jedes Symbol wird jedes Mal mit dem genau gleichen Symbol ersetzt, z. B. wird das C (Klartext-Zeichen) immer mit dem f (Geheimtext-Zeichen) chiffriert. Bei der **Transposition** wird die Reihenfolge der Symbole vertauscht. Diese Verfahren sind symmetrisch. Der gemeinsame Schlüssel – und das ist das Problem dieser Verfahren – muss ausgetauscht werden und dies ist nur mit sogenannt asymmetrischen⁴⁶ Verfahren sicher.⁴⁷

Auch «Daten, die wir lokal auf unserem Computer speichern, können entweder gestohlen werden, wenn jemand vorbeikommt und den Computer mitnimmt oder wenn Schadsoftware (z.B. Viren, Trojaner) über ein Netzwerk (Internet, lokales Netzwerk) oder über einen «verseuchten» USB-Stick auf unseren Computer gelangen. Daten, die auf Servern oder im Cloud-Speicher abgelegt sind, sind selbst dann noch den Gefahren von Schad-Software und Diebstahl ausgesetzt, wenn unser lokaler Computer ausgeschaltet ist. Umso wichtiger ist es, dass die Daten verschlüsselt abgelegt werden.»⁴⁸ Um die Übertragungssicherheit zu erhöhen, können wir einerseits beim Menschen, andererseits bei der Technik ansetzen. Dazu gehören zum Beispiel starke Passwörter, die wir auch niemandem verraten, die Zwei-Faktor-Authentifizierung, die (meist sechsstellige) TAN (Transaktionsnummer), die zum Beispiel im Onlinebanking verwendet wird, die Ende-zu-Ende-

⁴³ Hromkovič, J. (2018) S. 75.

⁴⁴ ebd.

⁴⁵ MIA21: Reiseführer durch den digitalen Dschungel, Zyklus 3, S. 36

⁴⁶ Bei der asymmetrischen Verschlüsselung (Public-Key-Verfahren) besitzt sowohl der/die Absender/-in als auch der/die Empfänger/-in zwei Schlüssel: einen öffentlichen und einen privaten. Der öffentliche Schlüssel wird für das Chiffrieren gebraucht und bleibt nicht geheim. Zum Dechiffrieren wird der geheime, private Schlüssel benötigt. Dieser wird berechnet. Asymmetrische Verfahren funktionieren nur, wenn Sender/-in und Empfänger/-in das gleiche Tool verwenden.

⁴⁷ https://swisseduc.ch/informatik/theoretische_informatik/paper_computer_science/docs/13_kryptographie.pdf

⁴⁸ MIA21: Reiseführer durch den digitalen Dschungel, Zyklus 3, S. 36

Verschlüsselung zum Beispiel bei Nachrichtendiensten oder das «Schlösschen» im Browser (vgl. [https](https://www.basel-landschaft.ch) weiter oben).

Verschlüsselungsverfahren unterscheiden sich darin, wie technisch aufwändig das Chiffrieren und das Knacken sind. Folgende Verfahren können von den Schülerinnen und Schülern angewandt werden.

Das Verfahren von Caesar (monoalphabetische Substitution): Man fand Briefe an Julius Caesar, in denen eine Geheimschrift eingesetzt wurde: Das Klartextalphabet wurde dabei in ein Geheimtextalphabet umgeschrieben, indem man es um drei Stellen nach links versetzte:

Cäsar

A	B	C	D	E	F	G	H	I	J
d	e	f	g	h	i	j	k	l	m

K	L	M	N	O	P	Q	R	S	T
n	o	p	q	r	s	t	u	v	w

U	V	W	X	Y	Z				
x	y	z	a	b	c				

Die Caesar-Verschlüsselung⁴⁹: Verschiebung um drei Buchstaben nach links

⁴⁹ <https://mgje.github.io/Crypto/exp1/index.html>

Das ROT13-Verfahren funktioniert ähnlich wie die Caesar-Geheimschrift. Die Verschiebung erfolgt hier um 13 Buchstaben (nach links oder rechts):

ROT-13

A	B	C	D	E	F	G	H	I	J
n	o	p	q	r	s	t	u	v	w

K	L	M	N	O	P	Q	R	S	T
x	y	z	a	b	c	d	e	f	g

U	V	W	X	Y	Z				
h	i	j	k	l	m				

Die ROT-13-Verschlüsselung⁵⁰: Verschiebung um 13 Buchstaben

«ROT13 ist nicht zur sicheren Verschlüsselung gedacht, es wird im Gegensatz dazu sogar oft als Beispiel für eine schwache, unsichere Verschlüsselung genannt. Vielmehr dient ROT13 dazu, einen Text unlesbar zu machen, also zu verschleiern, so dass eine Handlung des Lesers erforderlich ist, um den ursprünglichen Text lesen zu können. ROT13 lässt sich daher mit Lösungen von Rätseln in Zeitschriften vergleichen, die kopfüber gedruckt werden, damit sie nicht sofort versehentlich gelesen werden können.»⁵¹

Vigenère-Verschlüsselung (polyalphabetische Substitution): «Die Stärke der Vigenère-Verschlüsselung beruht darauf, dass nicht nur zwei, sondern sogar 26 verschiedene Geheimtextalphabete zur Verschlüsselung verwendet werden. Die Auflistung dieser Alphabete nennt man Vigenère-Quadrat (vgl. Abbildung). Jede Zeile des Quadrats ist um eine Stelle gegenüber der darüber liegenden Zeile nach links verschoben. Dadurch befindet sich jeder Buchstabe des Alphabets einmal zu Beginn einer Zeile. Wie üblich wird das Klartextalphabet mit Kleinbuchstaben angegeben und die Geheimtextalphabete mit Grossbuchstaben. Für die Verschlüsselung einer Meldung muss nun aber irgendwie festgelegt werden, bei welchem (Klartext)Buchstaben welches (Geheim)Alphabet verwendet werden soll. Diese Festlegung erfolgt über ein Schlüsselwort.

⁵⁰ <https://mgje.github.io/Crypto/exp2/index.html>

⁵¹ <https://de.wikipedia.org/wiki/R%C3%A4tsel>

Klartext- alphabet	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère-
Quadrat

Das Vigenère-Quadrat

Zum besseren Verständnis der Verschlüsselung schauen wir uns ein konkretes Beispiel an. Es soll die Mitteilung

informatik ist heute sehr wichtig

mit der Vigenère-Verschlüsselung verschlüsselt werden. Als Lösungswort wählen wir SARNEN. Als erstes ist nun das Schlüsselwort über die zu verschlüsselnde Nachricht zu schreiben. Das Schlüsselwort wird dabei so oft wiederholt, bis es über die ganze Nachricht reicht.

Schlüsselwort: SARNENSARNENSARNENSARNENSARNE

Klartext: informatikistheutesehrwichtig

Sinnvollerweise werden zum Verschlüsseln die Leerschläge weggelassen, damit nicht durch die Wortlängen auf den Klartext geschlossen werden kann. Der Buchstabe aus der Schlüsselwortzeile gibt nun an, welches Geheimalphabet für die Verschlüsselung des darunterstehenden Klartextbuchstabens gebraucht wird. So steht über dem ersten Klartextbuchstaben i der Schlüsselwortbuchstabe s. Es wird also im Vigenère-Quadrat die Zeile 18 (mit dem s zuvorderst) verwendet. Das Klartext-i entspricht somit auf der Zeile 18 dem Geheimtextbuchstaben A. Über dem zweiten Klartextbuchstaben n steht das A aus dem Schlüsselwort. Mit der Zeile 0 ergibt sich daraus für das Klartext n der Geheimtextbuchstabe N. Die vollständig verschlüsselte Mitteilung heisst somit wie folgt:

Schlüsselwort: SARNENSARNENSARNENSARNENSARNE

Klartext: informatikistheutesehrwichtig

Geheimtext: ANWBVZSTZXMFHLVHXRKEYEAVUHKVK

Vergleicht man nun gleiche Buchstaben im Klartext, so sieht man, dass diesen im Geheimtext durchaus verschiedene Buchstaben zugeordnet sind. Nur ausnahmsweise, z.B. bei den letzten beiden vorkommenden i, resultiert auch der gleiche Geheimtextbuchstabe.

Mit der Einführung der polyalphabetischen Verschlüsselung konnte der Nachteil der identischen Buchstaben behoben werden. Solche Verschlüsselungen galten lange Zeit als nicht zu knacken»⁵², bis dies dem Mathematiker Charles Babbage gelang (um 1854). Die polyalphabetische Verschlüsselung ist zwar sicherer als die monoalphabetische. Jedoch konnte damit das Problem des Schlüsseltausches nicht behoben werden.

Auch bei modernen Verfahren wie zum Beispiel der AES-Verschlüsselung (Advanced Encryption Standard), die zum Beispiel fürs WLAN oder die Datenübertragung zwischen elektronischen Identitätsdokumenten (z. B. Pass) und Inspektionsgeräten⁵³ verwendet wird, handelt es sich um symmetrische Verschlüsselungsverfahren. Die grosse Sicherheit ergibt sich aufgrund ihrer komplexen Berechnungen.⁵⁴

Unsere Schülerinnen und Schüler sind in der Lage, monoalphabetische Verschlüsselungen zu knacken (Kryptoanalyse). Dabei können sie folgendermassen vorgehen: systematisches Durchprobieren (z. B. Verdacht auf Verschiebechiffre → alle 25 Möglichkeiten durchprobieren), statistische Analyse (Häufigkeiten von Buchstaben untersuchen):

Entschlüsseln

Relativ Absolut 367

a	b	c	d	e	f	g	h	i	j
7.6%	2.7%	7.9%	2.7%	0.5%	0.0%	5.4%	9.5%	4.6%	2.5%
k	l	m	n	o	p	q	r	s	t
1.1%	0.3%	0.0%	0.5%	2.5%	5.4%	2.5%	1.9%	4.4%	19.1%
									E
u	v	w	x	y	z				
1.1%	3.5%	4.1%	9.0%	0.0%	1.1%				

Häufigste Buchstaben (deutsch)

E	N	I	S	R	A	T	D	H	U
17,40%	9,78%	7,55%	7,27%	7,00%	6,51%	6,15%	5,08%	4,76%	4,35%

sxt opwa tau vxai paavbtxc pah cäggxhrtw opwa jcs hextai xb apjut sth zpgetkpah txc
vgdhht gdaat. ojb jghegicv sxthtg opwatchnbqdxz vxqi th ktghrwtstct pchxrwitc. th vxqi
txct gtxwt kdc opwatc, stctc kdc htxitch stg glaxvxc txc qthdcstgt hnbqdxhrtw qtstijcv
qtxvbtthtc lxgs. sxt tau vxai spqtx pah opwa stg bphhadxvxtxi, stg hüest, hdpvg pah
itjuaxhrtw opwa. xb bxiiitapaitg ztccobxrwitit hxt btchrtw pjhhtgwpag stg hxiitcvthtiot.

Entschlüsseln

sxE opwa Eau vxai paavEExc pah cÄggxhrtwE opwa jcs hexEai xb apjuE sEh zp
gcEkpah ExcE vgdhE gdaat. ojb jghegicv sxEhEg opwaEhnbqdxz vxqi Eh hEg
hrwEExE pchxrwE. Eh vxqi ExE gEwE kdc opwE, sEExE kdc hEhEhEg
gEaxvxc ExcE gEndcEhE hnbqdxhrtwE gEhEijcv gEwEExE lxgs. sxE Eau
vxai spqEx pah opwa hEg bphhadxvxE, sEg hüE, hdpvg pah iEjuaxhrtwE op
wa. xb bxiiEapaitg zEccEExrwEExE hxE hEhrtwE pjhEgwpag hEg hxiEcvthtiot
E.

Tool zum Entschlüsseln von geheimen Botschaften: Der Buchstabe E kommt im Deutschen am häufigsten vor.⁵⁵

⁵² https://www.swisseduc.ch/informatik/daten/kryptologie_geschichte/docs/vigenere_verschlueselung_theorie.pdf

⁵³ https://de.wikipedia.org/wiki/Advanced_Encryption_Standard

⁵⁴ Das Verfahren ist eine Blockchiffre, bei der jeder Block in eine Tabelle mit vier Zeilen notiert wird. Die Anzahl der Spalten hängt von der Blockgrösse ab (vier bis acht Spalten). Mit jedem Block werden nacheinander verschiedene Transformationen durchgeführt: Nach einer Substitution werden Zeilen verschoben, Spalten mit einer Matrix multipliziert und die Blöcke mit einem Rundenschlüssel XOR verknüpft; weitere Informationen: <https://studyflix.de/informatik/aes-verschlüsselung-1611>

⁵⁵ <https://mgje.github.io/Crypto/exp5/index.html>

Weiterführende Theorie: Wer sich vertiefter mit der [Internetgeschichte](#) auseinandersetzen möchte, findet auf SRF MySchool einen guten Überblick. MrWissen2go hat zur Frage «[Wem das Internet wirklich gehört](#)» ein Erklärvideo erstellt. [CrypTool-Online](#) bietet vertieften Einblick in die Kryptologie und verschiedene Verfahren können ausprobiert werden. In der Tagespresse sind immer wieder Artikel zu Datenschutz und Kryptologie zu finden. Anfang 2020 berichteten unter anderem die [Rundschau](#), die [bz – Zeitung für die Region Basel](#) und die [Republik](#) über den Cryptoleaks-Skandal. SRF befasst sich unter anderem in den beiden DOK-Filmen «[Die Schweiz in geheimer Mission](#)» und «[Cryptoleaks – Wie CIA und BND mit Schweizer Hilfe weltweit spionierten](#)» mit dem Thema. In Zusammenhang mit COVID-19 wurden Tracing-Apps entwickelt. Wie dank Kryptografie die Privatsphäre bewahrt werden kann, hat die Republik im Artikel «[So funktioniert eine Corona-Tracing-App, die Ihre Privatsphäre schützt](#)» so einfach wie möglich erklärt.

5.5 Lernziele, Kompetenzen

- Die Schülerinnen und Schüler können das Internet als Infrastruktur von seinen Diensten unterscheiden (z.B. WWW, E-Mail, Internettelefonie, Soziale Netzwerke). ([MI.2.3.m](#))
- Teilziele (nach <https://unterricht-digital.ch/2017/09/04/mi-2-3-m/>):
 - Die Schülerinnen und Schüler verstehen, dass das Internet selbst lediglich die Infrastruktur zur Verfügung stellt.
 - Die Schülerinnen und Schüler verstehen, wie das Internet aufgebaut ist.
 - Die Schülerinnen und Schüler verstehen, dass ein Internetdienst eine Anwendung ist, und sie kennen verschiedene Internetdienste: World Wide Web, E-Mail, Dateiverwaltung, Cloud, Diskussionsforen, Chat, Telefonie, Fernsehen, Radio, Soziale Netzwerke, Spiele
 - Begriffe: Server, Router, Provider, Browser
- Die Schülerinnen und Schüler können die Risiken unverschlüsselter Datenübermittlung und -speicherung abschätzen. ([MI.2.3.n](#))
 - Bezug zu Systeme 1, Kompetenz MI.2.3.j: Die Schülerinnen und Schüler können lokale Geräte, lokales Netzwerk und das Internet als Speicherorte für private und öffentliche Daten unterscheiden.
 - Die Schülerinnen und Schüler erforschen und argumentieren; sie suchen nach Gesetzmässigkeiten, beschreiben, überprüfen und hinterfragen sie.
 - Die Schülerinnen und Schüler untersuchen technische Erfindungen und denken über die Folgen nach.
 - Begriffe: chiffrieren, dechiffrieren

5.6 Unterrichtsidee

a. Ablauf

- Lektion 1: Das Internet als Infrastruktur vs. Dienste des Internets
 - Technische Aspekte: Auswahl aus verschiedenen anspruchsvollen Vorschlägen wählen
 - Das Internet als Infrastruktur: Der Learning Snack bezieht sich auf den ersten Film: Wie funktioniert das Internet? (5:41), Learning Snacks lassen sich gut selbst herstellen.

t	Sozialform	Aktivitäten der Lehrperson	Aktivitäten der Schülerinnen und Schüler	Material
10'	EA, PA oder direkt PL	Einstieg «Heute beschäftigen wir uns mit einer (zumindest auf den ersten Blick) einfachen Frage: Was ist das Internet?» «Was ist im Internet?» Aussagen und Begriffe sammeln und aufräumen, ergänzen	Die SuS nennen, erklären...	Visualisieren des Brainstormings Unterstützung: 1.1_Das_Internet.pp tx, Folie 2
10'	EA/Plenum	Technische Aspekte Auftragserteilung Film Wie funktioniert das Internet? (5:41) z. B. Unterbruch bei 2:54; Diskussionsleitung z. B. Unterbruch bei 3:39; Diskussionsleitung z. B. Unterbruch bei 4:49; WhatsApp erst ab 16 Jahren; Diskussionsleitung Hinweis: Die Nachricht wird in <i>Datenpaketen</i> verschickt und vor Ort wieder zusammengesetzt. Anspruchsvoller: Wie funktioniert das Internet? (9:06) Einfacher (weniger Fachbegriffe, weniger Details): Das Netz – eine kurze Geschichte des Internets (3:18) plus Das Netz – Wie gelangt eine Nachricht durchs Netz? (2:28) Mögliche Vertiefung (anspruchsvoll): Warrios of the net (12:59, Konzept der Pakete, deutsch)	Die SuS sehen den Film und notieren sich (Fach)Begriffe SuS beantworten Frage: Geht die Nachricht «durchs Meer»? SuS nennen Provider in der Schweiz. SuS nennen Konsequenzen, wenn sie den Nutzungsbedingungen zustimmen.	Beamer, Ton

15'	Plenum und EA	Das Internet als Infrastruktur Variante A: Diskussionsleitung, Coaching Vergleich der Zeichnungen und Korrektur Idee: Seekarte mit Kabeln zeigen Variante B: Learning Snack Coaching, evtl. Diskussion zu Datenschutz/WhatsApp ab 16 J.	SuS nennen wichtige technische Begriffe (Server, Router, Provider, Browser), sie erstellen eine Übersicht zum Weg, den eine Nachricht von Gerät A zu Gerät B nimmt. SuS lösen Learning Snack für sich.	1.1_Das_Internet.pptx, Folien 3 (-11) Handy/Computer für LearningSnack
5'	EA, PA oder direkt PL	Die Dienste des Internets Unterscheidung Infrastruktur (technisch, SuS-Übersichten) und Dienste des Internets Diskussionsleitung und Visualisierung ergänzen Überleitung/Ausblick: Verschlüsselung	SuS nennen Dienste des Internets (World Wide Web, E-Mail, Dateiverwaltung, Cloud, Diskussionsforen, Chat, Telefonie, Fernsehen, Radio, Spiele)	1.1_Das_Internet.pptx, Folien 12-13 Folie 14

- Lektionen 2 und 3: Risiken unverschlüsselter Datenübermittlung und -speicherung
 Aufträge zum Verschlüsseln: Die Lehrperson soll eine Auswahl treffen.
 - [Informatik-Biber](#): M3_Kopiervorlagen → BiberFit_M3_Kopiervorlagen_v02.pdf:
 - AB1 (Botschaften mit Caesar verschlüsseln) und AB2 (Geheime Botschaften knacken, ROT-13): einfach, sehr gut machbar
 - AB3 (Botschaften sicher verschlüsseln, AES): sehr anspruchsvoll, weniger empfohlen (neuer Link zum [Tool](#))
 - [Informatik-Biber](#): M3_Biber_Aufgabe → schwierig → Vigenere_Verschlueselung.pdf: anspruchsvoll
 - Corona Proximity Tracing Paper App: Ein Spiel, das auf Papier eine Proximity-Tracing-App simuliert und Schritt für Schritt zeigt, wie technisch mit solchen Smartphone-Anwendungen Corona-Infektionen zurückverfolgt werden können; sehr gut machbar.
 - SwissEduc.ch: [Public Key Kryptographie](#) mit Schatzkiste und Vorhängeschloss, Paper Computer Science Experiment zur asymmetrische Verschlüsselung: anspruchsvoll

t	Sozialform	Aktivitäten der Lehrperson	Aktivitäten der Schülerinnen und Schüler	Material
10'	Plenum	Einstieg Auftragserteilung Gesprächsführung	SuS lesen Geheimbotschaft, sollen diese entschlüsseln SuS erklären ihr Vorgehen.	2.1_Verschlueselung.pptx, Folien 2–3 Statt Folie 3: Homepage
10'	EA/Plenum	Film Informatik-Biber Warum ist es wichtig, Daten zu verschlüsseln? Weitere Impulse für Diskussion Film (5:41) schauen als Beispiel, was eben passieren kann...	SuS beschreiben, in welchem Zusammenhang man Texte verschlüsseln muss/soll. Wann tun sie dies konkret?	Beamer, Ton

15'	EA/PA/PL	Zuverlässigkeit von Verschlüsselungen (kann auch nach dem nächsten Schritt angegangen werden) Auftragserteilung, Coaching Sicherheit von Verschlüsselungsmethoden thematisieren; evtl. symmetrische und asymmetrische Verschlüsselung thematisieren	Die SuS berechnen Kombinationsmöglichkeiten und beurteilen die Sicherheit.	2.1_Verschlüsselung.pptx, Folie 4
30'	EA/PA	Verschlüsseln Auftrag auswählen, Auftragserteilung, Coaching AB 1: Botschaften verschlüsseln (Cäsar, sehr einfach) AB2: Geheime Botschaften knacken (ROT-13, etwas zum Knacken) Corona Proximity Tracing Paper App: Aktualität zu Tracking und Corona Informatik-Biber Aufgaben, z. B. zur Vigenère-Verschlüsselung (schwierig) Public Key Kryptographie (asymmetrische Verschlüsselung)	Die SuS bearbeiten die ausgewählten Aufträge. Tipp: Für die Arbeiten mit AB1 und AB 2 empfiehlt sich das Krypto-Tool (statt Scheibe). Knacknüsse; die SuS und/oder LP können ihre eigenen Knacknüsse herstellen und gegenseitig austauschen	Material Informatik-Biber: LP-Kommentar (.pdf) und Kopiervorlagen (.zip, mit .pdf) Computer/Tablet 3.1_Spielanleitung_Coprotrac_Papp.pdf 3.2 Corona Proximity Tracing Paper App (Ordner) Material Informatik-Biber: Informatik-Biber Aufgaben (.zip mit .pdf) Public Key Kryptographie
25'	EA	Ergebnissicherung Auftragserteilung, Coaching (Auftrag A ist einfacher und besteht aus Teilaufgaben, B ist umfassender und anspruchsvoller)	SuS schreiben eine E-Mail.	4.1_Auftrag_Internet_A.docx und 4.1_Auftrag_Internet_B.docx

b. Material

- Siehe Planungen

c. Leistungsüberprüfung/Bewertung

- E-Mail mit Zusammenfassung, z. B. als geheime Botschaft
- Learning Snack
- Rätsel herstellen

d. Differenzierung, Erweiterung

- Wem das Internet gehört: <https://www.nanoo.tv/link/v/nURnKGjp> (MrWissen2go)
- Internetgeschichte: <https://www.nanoo.tv/link/v/ydEZJXBf> oder <https://www.srf.ch/sendungen/myschool/internetgeschichte> (SRF MySchool)
- Auf der Seekarte können Wege gesucht werden, die z. B. eine E-Mail nimmt, um von der Schweiz nach Grönland zu kommen: <https://www.submarinecablemap.com/>
- Vertiefung zum Thema Routing: <http://informatik-biber.ch/de/internet-routing/> (bis 4 Lektionen) Konzept der Datenpakete: <https://www.nanoo.tv/link/v/YjRiiZzv>
- einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren: Das Kapitel 2 beinhaltet viele Übungen zum Chiffrieren und Dechiffrieren.
- Chiffrieren und Dechiffrieren mit Caesar und anderen Methoden mittels Onlinetool: <https://mgje.github.io/Crypto/exp1/index.html>
- CryptoTool online: Einblick in die Welt der Kryptologie mit einer Vielzahl von Chiffrierverfahren, Kodierungen und Analysetools: <https://www.cryptool.org/de/cto-ueber-cryptoolonline>
- Unterrichtsidee zur asymmetrischen Verschlüsselung (mit Primzahlen und Semiprimzahlen): https://bscw.schule.de/pub/bscw.cgi/d938724/RSA_fast_ohne_Mathematik.pdf
- Unterlagen EDÖB (Eidg. Datenschutz- und Öffentlichkeitsbeauftragter): Informationsdossier (Basismodul) und Unterrichtsvorschläge für 7 Lektionen zum Thema Datenschutz https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/jugend-und-internet/lehrmittel-datenschutz/datenschutz-lehrmittel-fuer-13-15-jaehrige.html
- Die Plattform Jugend und Medien (Bundesamts für Sozialversicherungen) hat zur Förderung von Medienkompetenzen verschiedene Broschüren herausgegeben. Darin werden unter anderem Tipps zum Veröffentlichen von (privaten) Daten und die rechtliche Lage thematisiert. Sie können gratis bestellt werden: <https://www.jugendundmedien.ch/de/angebote-beratung/bestellung-publikationen.html>
- Wie viel muss man über einen einzelnen Kreditkartennutzer wissen, um ihn aus einem riesigen Datensatz (mit anonymisierten Daten) eindeutig identifizieren zu können? SRF hat dazu eine Sendung ausgestrahlt: https://www.srf.ch/wissen/mensch/anonymisierte-daten-von-wegen?ns_source=app
- Risiko Internet? Sicherheitsaspekte bei der Internet-Benutzung (PDF des 2000 im Orell Füssli Verlag Zürich unter demselben Titel erschienenen Buches) https://www.swisseduc.ch/informatik/internet/internet_sicherheit/docs/sicherheit.pdf

e. Fächerübergreifend

- Mathematik: Kombinatorik (Passwörter ausrechnen), mathbuch 2, LU 21; mathbuch 3+, LU18
- Geschichte: Verschlüsselungstechniken im 2. Weltkrieg (Enigma, zum Beispiel auch: <https://www.cryptool.org/de/cto-chiffren/enigma>)
- Anwendungskompetenzen:
 - Ampelsystem: <http://kibs.ch/datenschutz/ampelsystem/>
 - Dateien verschlüsselt aufbewahren
 - Schreiben und Versenden von E-Mails
 - Arbeit mit dem Medienkompass 2: z. B. Kapitel «Hier steckt der Wurm drin» (S. 66ff) und Kapitel «Spuren im Netz» (S. 70ff)

6 Quellen

6.1 Daten 3

Haftendorn, D.: Mathematik sehen und verstehen, Springer Spektrum, Heidelberg 2010.

Hromkovič, J.: einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren, Schulbuch, Klett und Balmer AG, Baar 2018.

Hromkovič, J.: einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren, Begleitband, Klett und Balmer AG, Baar 2018.

Hromkovič, J., Kohn, T., Keller, L., Komm, D., Serafini, G. und Steffen, B.: Fehlerkorrigierende Codes, Ein Unterrichtsbeispiel zum gelenkten entdeckenden Lernen, in LOG IN, NR. 168, Berlin 2011: http://www.log-in-verlag.de/PDF-Dateien/LOG_IN_168pub.pdf

Meyer, U.: Experimente ohne Computer zu 13 Informatikthemen, Verein SwissEduc, Wettingen, 2017: https://www.swisseduc.ch/informatik/theoretische_informatik/paper_computer_science/

6.2 Programmieren 3

Assaf, D.: Physical Computing – Verbindung der physischen mit der virtuellen Welt, PH Schwyz, Schwyz 2018:

https://mia.phsz.ch/pub/Informatikdidaktik/PhysicalComputing/PhysicalComputing_PHSZ_DA_V2.0.pdf

Bachinger, A., Teufel, M. (Hrsg.): Computational Thinking mit Micro:bit. Digitale Bildung in der Sekundarstufe, Austro.Tec, Grieskirchen 2018, vgl.: <https://microbit.eeducation.at/wiki/Hauptseite>

Hromkovič, J., Kohn, T.: einfach Informatik 7–9, Programmieren, Schulbuch, Klett und Balmer AG, Baar 2018.

Hromkovič, J., Kohn, T.: einfach Informatik 7–9, Programmieren, Begleitband, Klett und Balmer AG, Baar 2018.

Kiang, D., Kiang, M.: Basiscurriculum für den Einsatz des micro:bit, dt. Fassung: Deumer, S. et al., Microsoft Schweiz 2018:

<https://education.microsoft.com/courses-and-resources/courses/basiscurriculum-fr-den-einsatz-des-microbit>, freigegeben als [OneNote-Datei](#)

6.3 Systeme 3

Affolter, W. et al.: mathbuch 2, Bern und Baar 2014.

Affolter, W. et al.: mathbuch 3+, Bern und Baar 2015.

Birrer, Alex: Streifzug durch die Geschichte der Kryptologie: Vigenère, Verein SwissEduc, Wettingen 2017:

https://www.swisseduc.ch/informatik/daten/kryptologie_geschichte/docs/vigenere_verschluesselung_theorie.pdf

Hromkovič, J., Kohn, T.: einfach Informatik 7–9, Daten darstellen, verschlüsseln, komprimieren, Schulbuch, Klett und Balmer AG, Baar 2018.

Informatik-Biber Schweiz: Geheime Botschaften: Verschlüsseln, Luzern: <http://informatik-biber.ch/de/geheimebotschaften/>

Ingold, Urs et al.: Medienkompass 2, Lehrmittelverlag Zürich, Zürich 2008.

Kooperationspartner MIA21 (Verantwortung: Gumpert Andrea und Zaugg Pascal, PH Zürich): Reiseführer durch den digitalen Dschungel, Zyklus 3. Version August 2019.

Meyer, Urs: Experimente ohne Computer zu 13 Informatikthemen: For your eyes only (Public Key Kryptographie), Verein SwissEduc, Wettingen 2017:

https://swisseduc.ch/informatik/theoretische_informatik/paper_computer_science/docs/13_kryptographie.pdf

Planet Wissen (Ziegler, Wiebke und Delvaux de Fenffe, Gregor): Internet für Einsteiger, Köln 2020:

https://www.planet-wissen.de/technik/computer_und_roboter/das_internet/pwieinternetfuereinsteiger100.html

