8. Geheime Botschaften, sichere Passwörter und die Kryptologie

Brigitte Pemberger, Kristine Belewsky, Paula Bleckmann und Nino Mindiashvili

„Am Anfang verstehst du Bahnhof, aber easy. Wir haben echte Geheimschriften erfunden. Einige kann ich auch knacken!“

Tarek, 9 Jahre

	01000100	01110101	00100000
01100010	01110010	01100001	01110101
01100011	01101000	01110011	01110100
00100000	01101110	01101001	01100011
01101000	01110100	00100000	01000001
01101100	01100010	01100101	01110010
01110100	01101001	00100000	01111010
01110101	00100000	01101000	01100101
01101001	01110011	01110011	01100101
01101110	00100001	00100001	;-))

Geheimtext als binärer Blockcode[1]

Worum es geht

Der Schutz von Datenbanken und Datensammlungen stellt eine komplexe informatische Herausforderung dar, die im Informationszeitalter zwar brandaktuell, aber nicht ganz neu ist. Seit Jahrtausenden ist es ein menschliches Bedürfnis, selbst darüber zu bestimmen, mit wem man Botschaften teilt und mit wem nicht. Dies blieb mit jeder neuen Generation von Technologie gleich, ebenfalls die Suche nach immer ausgeklügelteren Methoden zur Ver- und Entschlüsselung von Daten.

Die Anfänge der Kryptologie (Wissenschaft des geheimen Schreibens, vom griechischen *kryptós* = verborgen) reichen weit in die Geschichte zurück. Bei dieser Kunstform geht es im Wesentlichen darum, Botschaften nach der Anwendung von genau definierten Regeln so zu verändern, dass sie nur noch für Eingeweihte verständlich sind. Dem Entschlüsseln von Geheimtexten widmet sich die Kryptoanalyse, ein Teilgebiet der Kryptologie. In diesem Kapitel stellen wir Ideen für die Praxis vor, die alle als Rätselaufgaben gestellt werden können und grundsätzlich lösbar sind. Da das Entwickeln von eigenen Geheimsprachen und Geheimschriften ein kreativer Prozess ist, der eine Vielfalt von Lösungsmöglichkeiten zulässt, sprechen Kinder auf dieses Thema erfahrungsgemäß sehr gut an.

Die Anschlussfähigkeit der zugrunde liegenden Konzepte an vertiefende oder weiterführende, anspruchsvollere Aufgabenstellungen der Kryptologie und ihren Teilbereich der Kryptoanalyse ist gewährleistet. Voraussetzungen für ein gutes Gelingen ist die Freude der Kinder am Rätseln und Knobeln und die Begeisterung, die Sie als Lehrkraft für das Thema mitbringen.

Im ersten Praxisbeispiel geht es um **regelhafte Geheim- und Spielsprachen**, im zweiten um **Geheimschriften** und im dritten um **sichere Passwörter**. Es ist gut möglich, dass Sie auf den folgenden Seiten auf Aktivitäten stoßen, die Sie mit den Kindern bereits umsetzen, nur vielleicht bislang noch ohne sich des Bezugs zur Informatik bewusst zu sein.

Für die Durchführung der vorgestellten Praxisideen ist keine informatische Vorbildung nötig. Ab S. 175 erfahren Sie mehr über die didaktischen, informatischen und historischen Hintergründe.

1 Verschlüsselt mit ASCII auf cryptotool.com. Siehe auch Kapitel 10 zu Binärcodes.

Ab Klasse 1
Ganze Klasse
Vorbereitung: 45 Min.
Durchführung: Ab 10 Min.
1 Lehrperson

Praxisbeispiel 1

8.1 „Pause widi Wause“ & Co. – Geheimsprachen: Vom Lautmalerischen zum Analytischen

Geheime Botschaften weitertragen im Deutschunterricht

„Hanafallonofo Kinifinonofo!“

„Geheimsprachen sind cool. Wenn ich Lust habe, erfinde ich eine neue – ich weiß, wie das geht!“
Lotta, 9 Jahre

Worum es geht

Die Kunst der geheimen Kommunikation kennt viele Spielarten und Schwierigkeitsgrade. Für den Einstieg haben sich Geheimsprachen besonders bewährt, weil deren Erlernen weder Lesen- noch Schreibenkönnen voraussetzt. Leichtere Varianten schnappen die Kinder sozusagen „übers Ohr auf“ und probieren sich nachahmend aus – meist mit Freude, Staunen und Gelächter.

Material für dieses Projekt

- kein zusätzliches Material für die Kinder erforderlich, da Durchführung mündlich möglich

Anleitung Schritt-für-Schritt

0 Vorbereitung der Lehrkraft (45 Min.)

Üben Sie selbst eine Geheimsprache. Eine kleine Auswahl (von leicht zu anspruchsvoll) stellen wir weiter unten vor.

Als Minimalvorbereitung reicht es, wenn Sie die Namen der Kinder in der Klasse oder zehn Gegenstände im Klassenzimmer in Geheimsprache beherrschen und Sie „Guten Morgen“ in Geheimsprache fließend sprechen können.

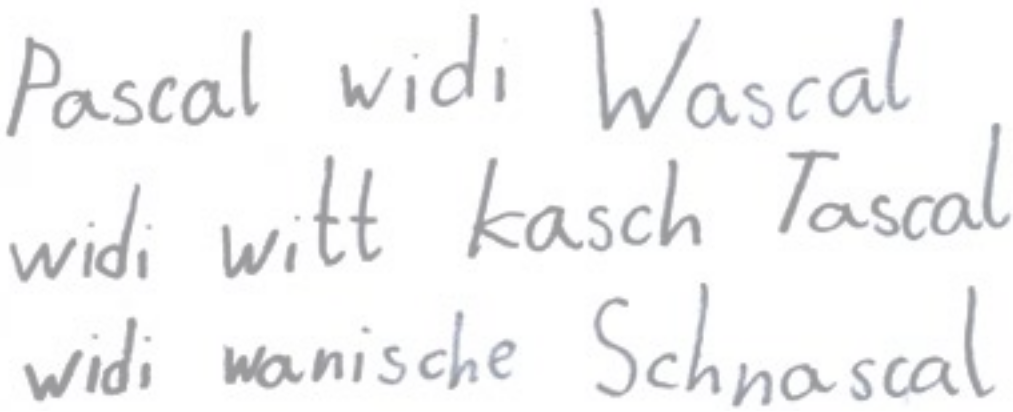
Überlegen Sie sich einen passenden Anlass, um die Geheimsprache in den pädagogischen Alltag mit einfließen zu lassen, oder seien Sie spontan und improvisieren Sie.

1 Lehrkraft spricht in der Klasse Geheimsprache, Kinder ahmen nach (mind. 10 Min.)

Der Moment der Überraschung, der Irritation und des Staunens, wenn Sie plötzlich in der Arbeit mit den Kindern etwas in Geheimsprache sagen, hat einen besonderen Reiz. Sprach- und spielfreudige Kinder wollen meist sofort auch können, was sie da hören.

Zum Beispiel kann die Begrüßung in Geheimsprache erfolgen. Auf jeden Fall sollten Sie so vorgehen, dass sich die Kinder aus der Nachahmung heraus über das Gehör erste Worte der geheimen Sprache aneignen können. Die Freude am lautmalerischen, kreativen Sprach- und Sprechspiel soll im Vordergrund stehen.

Tipp:
Die Kinder lernen Geheimsprachen ihrem Entwicklungsstand entsprechend. Wenn ein Kind Geheimsprache nicht aktiv sprechen kann, ist es trotzdem möglich, dass es die Sprache – oder Teile davon – versteht, weil es ein Gefühl für die Sprache entwickelt oder, wissenschaftlich gesprochen, „ein implizites Konzeptverständnis“ aufbaut.



Eine Auswahl an Geheimsprachen

1. Bekanntes Lied „Drei Chinesen mit dem Kontrabass …“

Die Lehrkraft singt vor, die Kinder ahmen nach. Alle Vokale des richtigen Liedtextes werden durch einen festgelegten anderen Vokal ersetzt. Nach ein paar Durchgängen probieren die Kinder selbst neue „Muster“ aus, die z. B. beginnen mit „DREE CHENESEN MET …“, „DROO CHONOSON MOT …“ usw.

Klartext[2]:	**Drei Chinesen mit dem Kontrabass usw.**
Geheimtext 1:	DRII CHINISIN MIT DIM KINTRIBISS usw.
Algorithmus zur Verschlüsselung 1:	Alle Vokale werden durch „I“ ersetzt
Geheimtext 2:	DRUU CHUNUSUN MUT DUM KUNTRUBUSS usw.
Algorithmus zur Verschlüsselung 2:	Alle Vokale werden durch „U“ ersetzt
Geheimtext 3:	DREE CHENESEN MET DEM KENTREBESS usw.
Algorithmus zur Verschlüsselung 3:	Alle Vokale werden durch „E“ ersetzt.

2. „Widiwittsprache“ aus dem Kindergarten

Die Lehrkraft macht vor, die Kinder ahmen nach. Der Name eines Kindes wird als rhythmische Sprachübung nach dem immer selben Muster variiert. Auch hier: mit den Kindern nicht analysieren, sondern nur sprechen.

Klartext 1:	**Paula**
Geheimtext 1:	**Paula**, WIDI Waula WIDI WITT KASCH Taula WIDI WANISCHE SCHNaula
Klartext 2:	**Aslan**
Geheimtext 2:	**Aslan**, WIDI Waslan WIDI WITT KASCH Taslan WIDI WANISCHE SCHNaslan
Klartext 3:	**Maya**
Geheimtext 3:	**Maya**, WIDI Waya WIDI WITT KASCH Taya WIDI WANISCHE SCHNaya
Algorithmus zur Verschlüsselung:	Der richtige Name wird immer am Anfang gesprochen. Danach werden alle Buchstaben vor dem betonten Stammvokal durch festgelegte (immer gleiche) Fantasiewort-Blöcke[3] in einer vorgegebenen (immer gleichen) Reihenfolge ersetzt.

2 Klartext = ursprünglicher Text, den jede:r lesen kann.
Geheimtext (häufig auch Chiffrierung genannt) = verschlüsselter Text, den nur lesen kann, wer den Schlüssel/Code dazu kennt.
Weitere Begriffe siehe S. 175.

3 Die fixen Fanatasie-Wortblöcke der „Widiwittsprache“ sind hier rot geschrieben. Man könnte auch andere Fantasie-Wortblöcke erfinden und damit eine Geheimsprache entwickeln.

3. Grüfnisch

Diese in der Deutschschweiz verbreitete Geheimsprache hat sich seit mehreren Generationen unter Kindern mündlich weiterverbreitet. Ursprünglich wurde sie von einer 5. Klasse im Deutschunterricht entwickelt. Bis heute scheint der Eifer der Kinder ungebrochen, diese Sprache zu erlernen, obwohl unterdessen viele Eltern damit vertraut sind und die Kinder längst nicht mehr so sehr „unter sich sind“, wie dies noch in der ersten Generation der Fall war. Im Grüfnischen wird der natürliche Sprachfluss möglichst beibehalten.

Klartext 1:	**Samuel**
Geheimtext 1:	**SANAFAMUNUFUENEFEL**
Klartext 2:	**Melissa**
Geheimtext 2:	**MENEFELINIFISSANAFA**
Klartext 3:	**Treffen wir uns um fünf!**
Geheimtext 3:	**TRENEFEFFENEFEN WINIFIR UNUFUNS UNUFUM FÜNÜFÜNF!**
Klartext 4:	**Achtung, sie kommen!**
Geheimtext 4:	**ANAFACHTUNUFUNG; SINIFII KONOFOMMENEFEN!**
Klartext 5:	**Der Ball ist auf dem Dach gelandet.**
Geheimtext 5:	**DENEFER BANAFALL INIFIST ANAFAUNUFUF DENEFEM DANAFACH GENEFELANAFANDENEFET.**

Algorithmus zur Verschlüsselung: Jeder Vokal wird durch seinen zweisilbigen Fantasie-Block ersetzt. Die Fantasie-Blöcke sind alle nach demselben Muster gestrickt.

A	=	ANAFA	IE	=	INIFII	Ä	=	ÄNÄFÄ
E	=	ENEFE	O	=	ONOFO	Ö	=	ÖNÖFÖ
I	=	INIFI	U	=	UNUFU	Ü	=	ÜNÜFÜ

Bei Diphthongen – also Doppellauten wie „ei“, „au“ usw. – haben sich im „Sprachgebrauch“ unterschiedliche Handhabungen etabliert. Das Wort „Eule“, das je nach Dialekt als *Oile* oder *Öile* ausgesprochen wird, kann sich durchaus verschieden anhören, zum Beispiel:

Vom Gehörten abgeleitet:

- Für „Öile“: **ÖNÖFÖINIFILENEFE** oder **ÖNÖFÖILENEFE** (Vereinfacht, zweiter Vokal bleibt unverändert)
- Für „Oile“: **ONOFOINIFILENEFE** oder **ONOFOILENEFE** (Vereinfacht, zweiter Vokal bleibt unverändert)

Vom Geschriebenen abgeleitet:

Für „Eule“: **ENEFEUNUFULENEFE** oder **ENEFEULENEFE** (Vereinfacht, zweiter Vokal bleibt unverändert)

4. Die Räubersprache von Astrid Lindgren

Diese Sprache ist schon schwieriger zu sprechen, da man sich bei der Verschlüsselung auf die Konsonanten konzentrieren muss und dadurch der Sprachfluss eher unterbrochen wird, als dies etwa bei Grüfnisch der Fall ist, wo nur Vokale verschlüsselt werden.

Klartext:	**Danke**
Geheimtext:	**DODANONKOKE**
Algorithmus zur Verschlüsselung:	1. Verdopple alle Konsonanten Bsp. „**danke**“ wird zu „**DD A NN KK E**“ 2. Füge zwischen alle Konsonanten ein „O“ ein. Bsp. „**DD A NN KK E**“ wird zu „**DODANONKOKE**“

Das Alphabet lässt sich einfach ableiten. Konsonanten werden umgebildet, Vokale, Umlaute und Diphthonge nicht. Unterschiede gibt es bei „ch“ und bei „sch“. Einige Sprecher:innen trennen bzw. verschlüsseln in „COC-HOC“ und „SOS-COC-HOH“, andere machen „CH-O-CH“ oder „SCH-O-SCH“ daraus.

Klar-text		Geheim-text	Klar-text		Geheim-text	Klar-text		Geheim-text
A	=	A	J	=	JOJ	S	=	SOS
B	=	BOB	K	=	KOK	T	=	TOT
C	=	COC	L	=	LOL	U	=	U
D	=	DOD	M	=	MOM	V	=	VOV
E	=	E	N	=	NON	W	=	WOW
F	=	FOF	O	=	O	X	=	XOX
G	=	GOG	P	=	POP	Y	=	YOY
H	=	HOH	Q	=	QOQ	Z	=	ZOZ
I	=	I	R	=	ROR			

Ab Klasse 2
Ganze Klasse
Vorbereitung: 45 Min.
Durchführung: Ab 5 Min.
1 Lehrperson

Praxisbeispiel 2

8.2 „Siehst du diesen Muab?“ – Geheimschriften: Vom Einfachen zum Komplexen[4]

„Es gefällt mir, dass ich selber Geheimschriften machen kann. Nicht alle können sie lesen.“
Britta, 10 Jahre

Streng geheim!

Worum es geht

Die Entwicklung der heutigen verschlüsselten Kommunikation nahm vor ca. 3500 Jahren ihren Anfang, also rund 2000 Jahre nach der Entwicklung der ersten Schriftsysteme in Keilschrift. Seither beschäftigt sich die Kryptografie und die Informatik (im Mittelalter die Mathematik) mit der Frage: „Wie können Texte[5] so umgestaltet werden, dass sie nur für Ausgewählte und Eingeweihte lesbar sind?“

Interessanterweise war es lange Zeit nicht nötig, Geschriebenes zu verschlüsseln. Das mag daran liegen, dass nur sehr wenige Menschen lesen und schreiben konnten. Das Lesen- und Schreibenkönnen an sich war während dieses Zeitalters so etwas wie eine Geheimwissenschaft, da die Mehrheit der Bevölkerung mit Geschriebenem nichts anzufangen wusste.

Die arabischen Gelehrten vermochten Geheimschriften nicht nur anzuwenden, sie gelten darüber hinaus als Erfinder:innen der Kryptoanalyse. Wer diese beherrscht, kennt Methoden, um Geheimtexte zu knacken, selbst wenn er nicht weiß, wie sie verschlüsselt wurden.

4 Inspiriert und angelehnt an das umfassende Lehrwerk von Prof. Dr. Juraj Hromkovič und Team der ETH Zürich/Schweiz, hier ganz besonders Bezug zum Kapitel Datensicherheit im Begleitband *Einfach Informatik. Lösungen finden 5/6*, erschienen im Verlag Klett und Balmer.
5 In der Informatik sind es Datenstränge aus Folgen von Symbolen, die aus Sicherheitsgründen verschlüsselt werden.

Material für dieses Projekt

- Stift und Papier

Anleitung Schritt-für-Schritt

0 Vorbereitung der Lehrkraft (45 Min.)

Üben Sie selbst eine Geheimschrift. Eine kleine Auswahl (von leicht zu anspruchsvoll) stellen wir weiter unten vor. Als Minimalanforderung reicht es, wenn Sie die Namen der Kinder in der Klasse oder zehn Gegenstände im Klassenzimmer in Geheimschrift beherrschen und Sie „Guten Morgen" in Geheimschrift fließend schreiben können. Wichtiger noch ist allerdings, dass Sie **das Rezept kennen**, wie die Geheimschrift gebildet wird.

Überlegen Sie sich einen passenden Anlass, um die Geheimschrift in den pädagogischen Alltag mit einfließen zu lassen, oder seien Sie spontan und improvisieren Sie.

1 Lehrkraft führt Geheimschrift ein, Kinder knobeln (mind. 5 Min.)

Mit der Einführung von einfachen Geheimschriften beginnen.
Die Geheimschrift möglichst so einführen, dass die Kinder

1. das Konzept Geheimschrift verstehen, indem sie
2. den Verschlüsselungsalgorithmus möglichst selbst herausfinden können.
   Das heißt: Hilfestellungen als Hilfe zur Selbsthilfe geben.

Beispiel:
Die Lehrkraft schreibt an die Wandtafel

XPXAXUXSXE

und sagt: „Wer das versteht, darf es machen!"

Nach der Pause kann mit einem neuen Satz fortgesetzt werden:

XNXEXHXMXT XDXAXS XLXEXSXEXBXUXCXH XHXEXRXVXOXR.

Bei der späteren Einführung von komplexen Geheimschriften ist diese Vorgehensweise nicht immer zielführend. Da eignen sich ggf. Anleitungen, die erklären, wie der Geheimtext konstruiert wird.

Tipp zum Lernen von Geheimsprachen und Geheimschriften
Die Kinder lernen und entwickeln Geheimschriften ihrem Entwicklungsstand entsprechend. Das Entschlüsseln und Entwickeln von Geheimschriften stellt beispielsweise höhere Anforderungen an Fähigkeiten zum logischen Denken, als dies bei einfachen Geheimsprachen (Bsp. 1 und 2 auf S. 159) der Fall ist, bei denen stärker rhythmisch-nachahmende Fähigkeiten über das Gehör angesprochen werden.

Eine Auswahl an Geheimschriften

1. Rückwärts schreiben = „Rückwärtsisch“ (ab Klasse 2)

Eine einfache Art des „geheimen Schreibens“ ist bereits,

- das Lösungswort in ein Rätsel zu verpacken und/oder
- die gesuchten Wörter jeweils rückwärts zu schreiben.

Rätsel 1

Was ist es?
Es hat drei Beine und eins noch dazu,
bin ich müde, so lädt es mich zur Ruh.

RED LHUTS / SAD TTEB

Rätsel 2[6]

Was ist es?
Bin ich davor, dann bin ich darin;
bin ich darin, dann bin ich davor.

RED LEGEIPS

Rätsel 3

Er hat ein rotes Kleidchen an
mit schwarzen Punkten dran.
Bringt Glück und Segen
auf all deinen Wegen.

RED REFÄKNEIRAM

Rätsel 4

Ich sehe sie nicht,
wenn ich sehe.
Wenn ich nichts sehe,
so sehe ich sie!

EID SINRETSNIF

Rätsel 5

Ich bin ganz leicht und kugelrund,
hab ne dünne Haut, die schimmert bunt.
Fasst du mich mit den Händen an,
platz ich, so schnell ich kann.

EID ESALBNEFIES

Rätsel 6

An der Schnur hält's das Kind,
in die Höhe trägt's der Wind.
Schön ist's und aus Papier,
weißt du es, dann sag es mir.

RED EHCARD

Rätsel 7

Es wärmen die Flammen
in diesem Winterkalt,
den Hirten, der zum Rechten schaut.
Siebenhundert an der Zahl,
steh'n dicht beisammen,
haben's warm.

EID EDREHFAHCS

Rätsel 8

Willst du mit der Feder etwas schreiben,
kann er nicht mehr ruhig bleiben.
Hast du's eilig, gibst nicht acht,
hüpft er auf das Blatt, grinst und lacht –
blau und plitschplatsch nass!
Wer sitzt da drin im großen Tintenfass?

RED KCELFNETNIT

6 https://www.janko.at/Raetselgedichte/00/851.htm

2. Die X-Verschlüsselung (ab Klasse 2)

Vor oder nach jedem einzelnen Buchstaben eines Wortes wird ein zusätzliches „X“ gesetzt.

Klartext 1:	ELIA
Geheimtext 1:	exlxixax
Klartext 2:	MADITA
Geheimtext 2:	mxaxdxixtxax

3. Atbasch-Codierung (auch AZBY-Code genannt)

Der Name Atbasch leitet sich ab von den beiden ersten und letzten Buchstaben des hebräischen Schriftsystems (A-T-B-Sch) und illustriert zugleich das Vorgehen, bei dem der erste Buchstabe „Aleph“ vertauscht wird mit dem letzten Buchstaben „Taw“, der zweite Buchstabe Beth mit dem vorletzten Buchstaben Schin usw.

Klartext																									
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
z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a
Geheimtext																									

Die Atbasch-Codierung ist ein Beispiel für Verschlüsselungstechniken, wie es sie bereits vor 2500 Jahren in Indien, China, Ägypten, Palästina und Griechenland gab. Eine Besonderheit ist, dass die Atbasch-Codierung ein sog. involutorisches Verfahren ist. Das bedeutet, dass die Verschlüsselungs- und die Entschlüsselungsmethode identisch sind.

Das Problem: Wenn die Zuordnung zu einfach ist, kann der Geheimtext sehr schnell entschlüsselt werden. Wenn aber die Zuordnung richtig schwierig (beliebig) ist, kann man sie sich nicht merken und muss sie aufschreiben.

↓

Nächstes Problem:
Ist die komplizierte Zuordnung zur Entschlüsselung (= Dechiffrierung) des Geheimtextes aufgeschrieben, so ist dies zu riskant – sie könnte in falsche Hände geraten!

↓

Die Lösung:
Die Menschen wählten bereits früher Chiffrierungen, die man sich merken konnte und nicht aufzuschreiben brauchte.
Ein bekanntes Beispiel aus der Geschichte ist die Caesar-Chiffrierung.

4. Verschiebe-Verschlüsselung: Caesar-Chiffrierung[7]

Die Grundvoraussetzung für die Anwendung der Caesar-Chiffrierung ist, dass man die richtige Reihenfolge der Buchstaben im Alphabet auswendig kennt. Dann ersetzt (= „chiffriert“) man jeden Buchstaben mit einem Buchstaben, der um eine gewisse Anzahl Positionen rechts von ihm im Alphabet steht.
Überliefert ist, dass der römische Staatsmann Julius Caesar im 1. Jahrhundert v. Chr. mit dieser Methode seine geheime militärische Korrespondenz führte. Ein Beispiel für eine Chiffrierung mit „Verschiebung um 2“:

A wird zu „c“
B wird zu „d“
C wird zu „e“
usw.

Klartext																									
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
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
Geheimtext bei „Verschiebung um 2“																									

Klartext 1:	**Melissa**
Geheimtext 1:	**ognkuuc**
Klartext 2:	**Samuel**
Geheimtext 2:	**ucowgn**
Klartext 3:	**UmzwanzigUhr!**
Geheimtext 3:	**wobycpbkiwjt!**

Aufgepasst: Verschiebung um 2

„Es entstehen lustige neue Wörter“[8]

7 Substitutionsverfahren, da jeder Buchstabe durch einen anderen ersetzt wird.
8 Name des Fußballers (Vincenzo) Grifo, chiffriert mit Caesar. Dabei in der Grundschule beim Chiffrieren in Sache Rechtschreibung auch mal ein Auge zudrücken …

Rätselaufgaben zur Caesar-Chiffrierung (ab Klasse 3)

Rätsel 1

Verwandle mit Caesar folgende Texte in Geheimbotschaften:

A) Verschiebung um 2	Klartext:	BeiSonnenaufgang
	Geheimtext:	
B) Verschiebung um 4	Klartext:	ImKoffer
	Geheimtext:	
C) Verschiebung um 16	Klartext:	UnterDerSchuhsohle
	Geheimtext:	

Rätsel 2

Versuche, die Geheimbotschaften zu entschlüsseln!

A) Verschiebung um 2	Geheimtext:	**dgko dtwppgp**
	Klartext:	
B) Verschiebung um 4	Geheimtext:	**yrxiv hiv pmrhi**
	Klartext:	
C) Verschiebung um 16	Geheimtext:	**mudd tyu ieddu qc xösxijud ijuxj**
	Klartext:	

Rätsel 3

Du erhältst den folgenden Geheimtext:

oc scd uosxo rohobs, rkcd ne nso nborcmroslo nklos!

Du weißt, dass der Text mit Caesar verschlüsselt ist und A nach k verschlüsselt wurde.
Wie lautet der Klartext?

Lösung:

5. Die „Alberti-Maschine“ oder Caesar-Scheibe (ab Klasse 3)

Um das Jahr 1470 hatte Leon Battista Alberti die geniale Idee, eine „Maschine“ zu bauen, die den Menschen das Ver- und Entschlüsseln von Nachrichten mit Caesar erleichtern sollte. Albertis „Maschine“ besteht aus zwei Scheiben, wobei die eine etwas größer ist als die andere. Am Rand der beiden Scheiben sind die Buchstaben des Alphabets jeweils in der richtigen Reihenfolge angegeben.

Die kleinere Scheibe wird auf die größere gelegt und im Mittelpunkt eine Befestigung (z. B. eine Flachkopfklammer) so angebracht, dass die Scheiben gegeneinander verdreht werden können. Der gewünschte Verschiebeschlüssel kann direkt eingestellt und die Chiffrierungen für jeden einzelnen Buchstaben leicht abgelesen werden.

Alberti-Maschine eingestellt auf Verschlüsselung mit Verschiebung „plus 4“

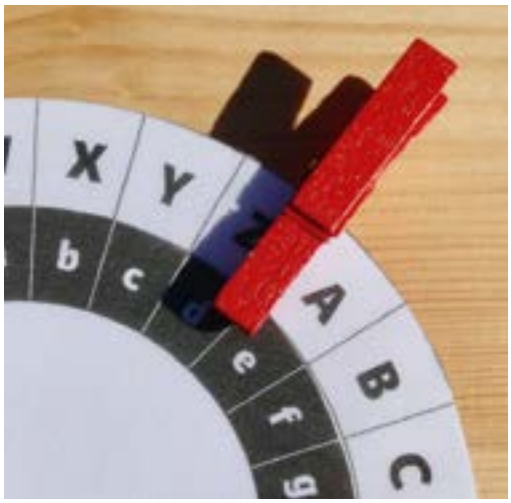
Pädagogisch-didaktische Anmerkung

Für die Arbeit mit den Schüler:innen ist die Herstellung einer eigenen Alberti-Maschine ungefähr ab der zweiten Hälfte der 3. Klasse möglich, die Anwendung aber noch sehr anspruchsvoll, da leicht ein Durcheinander von Klartext und Geheimtext entstehen kann oder sich die Scheiben unbeabsichtigt verdrehen. Der Schritt, die Alberti-Maschine einzuführen bzw. mit ihr zu arbeiten, sollte sinnvollerweise erst erfolgen, wenn die Schüler:innen einfache Verschiebungen um eine, zwei oder drei Positionen mit Hilfe einer Handskizze oder gar in Gedanken beherrschen und sie somit das Prinzip der Verschlüsselung durch Verschiebung begriffen haben.[9]

Der medienpädagogische Grundsatz **„analog vor digital“** lässt sich anhand dieses Beispiels gut weiter verfeinern in **„analog vor maschinell vor digital“**.

Sogenannte „Krypto Tools“ im Internet, die eine Vielfalt von Verschlüsselungsmethoden bieten, sollten erst angewendet werden, wenn die Schüler:innen die zugrunde liegenden Konzepte verstanden haben.

Alberti-Maschine zum Selbermachen, zwei Scheiben und eine Klammer



Kleine Wäscheklammer zum Fixieren des Verschiebe-Schlüssels (hier A -> e, B -> f, C-> g, D -> h, E -> i, usw.)

9 Kopiervorlage für Alberti-Maschine im Anhang dieses Kapitels auf S. 186 /187.

6. Skytale, ein Verschlüsselungsverfahren aus Sparta[10] (ab Klasse 3)

Ausschnitt aus geheimer „Wickel-Botschaft“, erkennbar von links *LOTTA*

„Das Verschlüsselungsverfahren der Skytale funktioniert so, dass man einen langen Papierstreifen **von links nach rechts** und **von oben nach unten** auf einen zylinderförmigen Gegenstand – die Skytale – aufwickelt und die Nachricht dann anhand der Buchstaben nebeneinander **zeilenweise** lesen kann.“[11]

Die Skytale (vom altgriechischen *skytálē* = „Stock“, „Stab“) zählt mit zu den ältesten Verschlüsselungsverfahren. Vor ungefähr 2500 Jahren kam es in Sparta zum Einsatz. In der pädagogischen Grundschulpraxis ist die Skytale sehr beliebt, weil sich der Schlüssel wortwörtlich in die Hand nehmen und das zugrunde liegende Prinzip „be-greifen“ lässt: Eine geheime Nachricht kann mit einem Stock oder Stab eines bestimmten Durchmessers leicht entschlüsselt und verschlüsselt werden.

Material für dieses Projekt

- Zylinderförmige Gegenstände wie leere Toilettenpapierrolle, Nudelholz, Klebstift, Holzstab, Ast o. Ä.
- Papier, Schere und Stift

Anleitung Schritt-für-Schritt

1 **Papier in Streifen schneiden**

Streifendicke ca. 1 – 2 cm

2 **Papierstreifen um Zylinderform wickeln**

Regel: von oben nach unten, von links nach rechts wickeln

3 **Klartext aufschreiben**

Regel: Zeilenweise von links nach rechts

4 **Nachricht senden**

Papierstreifen abwickeln, falten und Geheimtext versenden

10 Transpositionsverfahren, da die Positionen der Buchstaben des Ursprungstextes verschoben bzw. systematisch umsortiert werden.
11 https://www.inf-schule.de/kids/datennetze/verschluesselung/skytale

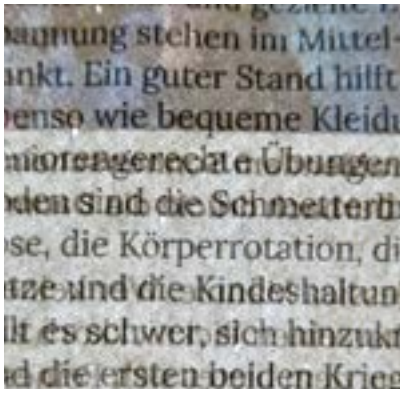
Weiterführende Ideen für den Unterricht

- **Kryptologie-Kurs**
  Z. B. 32 Stationen mit vielen verschiedenen Verschlüsselungstechniken und Selbstkontrolle für Schüler:innen ab Klasse 3:
  Schmidt, Hans-J. (2021). Stationenlernen Geheimschriften. Top Secret – Verschlüsseln und knacken wie der Geheimdienst. 7. Auflage. Kohl Verlag.

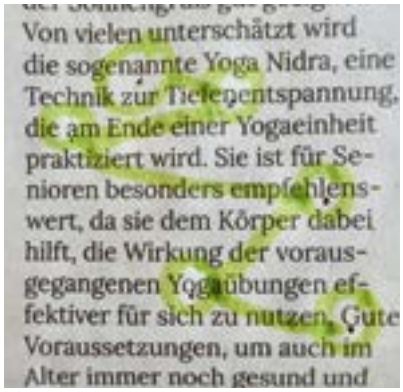
- **Ausflug in die Steganografie**
  - **Schreiben mit Geheimtinte** z. B. aus Zitronensaft, Milch oder Zuckerwasser. Die Geheimtinte verschwindet beim Trocknen auf dem Papier. Sichtbar wird das Geschriebene erst wieder beim Erwärmen z. B. mit Glühbirne, Bügeleisen, Herdplatte oder Haartrockner.
  - **Stechmuster-Codes** mit einer Nadel auf einer Zeitungsseite anbringen: unter jeden Buchstaben, der gelesen werden soll, fein einstechen.

Einstechen der Löcher

Der versteckte Geheimtext ist auf den ersten Blick nicht ersichtlich



Der Geheimtext zeigt sich, wenn die Zeitungsseite gegen das Licht gehalten wird



Alle Buchstaben mit Einstichstelle aneinandergereiht ergeben die geheime Nachricht

- **Schnitzeljagd mit Rätsel- und Kryptologie-Aufgaben**
  Verschiedene Posten mit Aufgaben zum Ver- und Entschlüsseln von Geheimbotschaften auf dem Schulareal verteilen. Die einzelnen Posten ggf. sogar im Unterricht (Gruppenarbeit) mit den Kindern herstellen.

- **Thema „Sichere Passwörter“** (Kapitel 8.3)

- **Binäre Murmelmuster** (Kapitel 10)

- **Technikfolgenabschätzung im Kleinen für die Grundschule: Sichere Kommunikation**

  Das Versenden und Empfangen von Nachrichten und damit verbunden auch die Frage nach sicherer Kommunikation lässt sich an historischen Technologien besonders gut aufgreifen, da diese durchschaubar sind. Freuden, Mühen, Vor- und Nachteile der jeweiligen Technologien lassen sich mit Grundschulkindern z. B. an folgenden Themen (im besten Fall erleben) und thematisieren:

„Brieftauben-Post“[10]

„Pferdekutschen-Post“

„Ballon-Post“

„Brief-Post mit Siegel“

„Telefon-Botschaften“

„Flaschen-Post“

„Fahrrad-Post“

Signalhorn-Post“

- **Freier Schreibanlass „Die geheime Botschaft“** (ab Klasse 5)
  Ausgehend von der historischen Abbildung Postzustellung Stuttgart 1888[12] schreiben die Kinder eine Geschichte in „Ich-Form“ im freien Stil, gegebenenfalls mit Happy End. Die Geschichte kann sowohl als Einzelarbeit wie auch als Partner:innenarbeit geschrieben werden. Kriterium: Die Geschichte könnte sich genauso abgespielt haben!

Mögliche Leitfragen für die Kinder:

- *Wer schreibt wem?* Soll man das überhaupt erfahren?
- *Worum* handelt es sich bei der geheimen Botschaft?
- *Weshalb* soll die Botschaft geheim gehalten werden?
- *Welche* Rolle spiele ich in dieser Geschichte?
- *Was* soll man über mich erfahren, was nicht?
- *Wie* und von wem wird die Botschaft überreicht? Kommt sie an?
- *Wo* spielt die Geschichte?

Postzustellung Stuttgart 1888

Zum Weiterlesen

Webseiten zu Kryptologie und Unterricht

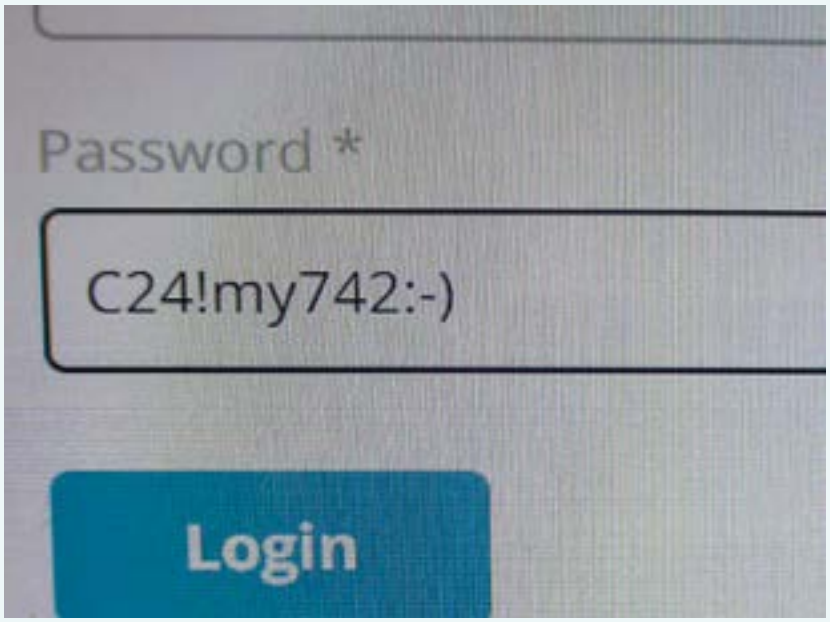
- Umfangreiches Dossier SPIONCAMP für den Kryptologie-Unterricht [ab ca. Klasse 5] von der Bergischen Universität Wuppertal
  https://ddi.uni-wuppertal.de/www-madin/material/spioncamp/dl/Alle-Stationen-hintereinander.pdf
- Informatik-Biber Schweiz. Workshop-Material zum Thema „Geheime Botschaften“.
  www.informatik-biber.ch/workshop-material-zum-thema-versteckte-botschaften-fuer-schlaue-biber/
- Stohr, Monika (2008). Unterricht in Kryptologie. Dissertation, LMU München: Fakultät für Mathematik, Informatik und Statistik
  www.edoc.ub.uni-muenchen.de/8456/1/Stohr_Monika.pdf

12 Ursprüngliche Bildquelle: Buch für Alle - 1888 nach J.G. Fuellhaas.

Ab Klasse 3
Ganze Klasse
Vorbereitung: Beschäftigung mit Praxisbeispiel 1 und 2
Durchführung: Ab 20 Min.

Praxisbeispiel 3

8.3 „Bitte Passwort eingeben“ – Die Krux, ein gutes Passwort zu wählen



Passwörter gehören im 21. Jahrhundert zum Alltag – je sicherer sie sind, desto besser

„Es ist so schwierig, dass ich es mir fast nicht merken kann. Aber ich habe einen Trick. Den verrate ich nicht!“
Carlo, 10 Jahre

Worum es geht

Einfache Passwörter sind leicht zu knacken, komplizierte vergisst man schnell. Was macht ein gutes und sicheres Passwort aus?

Für den Zugriff auf eigene Datensammlungen oder Daten darf man oft selbst ein Passwort wählen. Ein Passwort ist gut vergleichbar mit dem Schlüssel zur eigenen Wohnung oder sogar zur eigenen Schatzkiste. Wenn man ihn verliert, kommt man nicht mehr rein. Und er darf natürlich nicht in falsche Hände geraten. Mit dem Passwort verhält es sich auch so: Man darf es niemandem verraten. Aber was kann man tun, um es nicht zu vergessen?

Die beste Voraussetzung ist, wenn die Schüler:innen bereits Erfahrungen mit verschiedenen Verschlüsselungsmethoden gemacht haben (siehe Kapital 8.1 und 8.2). Wir zeigen, wie darauf aufbauend in Kombination mit einer Handvoll Sicherheitskriterien die Schüler:innen befähigt werden können, selbst sichere Passwörter zu kreieren.

Material für dieses Projekt

- Stift und Papier
- Kopiervorlage „Sichere Passwörter“, S. 188

Anleitung Schritt-für-Schritt

1 Passwörter selbst entwickeln

Die Lehrkraft macht eine kurze Einführung zu sicheren Passwörtern:
Die beste Sicherheitsstufe wird mit einem sehr komplizierten, langen und sinnlosen Passwort erreicht. Der Aufwand dafür, um es einzugeben, ist aber horrend!
Für ein gutes, also sicheres Passwort, eignen sich folgende Kriterien:

Das Passwort besteht aus
- Buchstaben und Ziffern
- Großbuchstaben und Kleinbuchstaben
- einem oder mehreren Interpunktionszeichen
- einem verschlüsselten Wort, das nicht auf Anhieb mit der Person in Verbindung gebracht wird
- maximal 12 Zeichen/Symbole

Die Schüler:innen entwickeln selbst Passwörter, am besten nicht für sich selbst, sondern für die Klassenkamerad:innen. Dabei geht es in erster Linie darum, dass sie sich aktiv mit den Sicherheitskriterien auseinandersetzen und diese anwenden lernen.

2 Sicherheitsprüfung nach Kriterien

Die entstandenen Passwörter werden in der Klasse oder in Kleingruppen einem Sicherheitscheck unterzogen. Wesentlich dabei ist, dass zur Prüfung mindestens die oben genannten fünf Kriterien herangezogen werden und die Schüler:innen altersangemessen diskutieren und begründen lernen:
a) Inwiefern ist ein Kriterium erfüllt oder nicht erfüllt?
b) Wie sicher ist ein Passwort?

Hier geht es besonders um den gemeinsamen prüfenden Blick auf die geschaffenen Passwörter und den Austausch in der Gruppe dazu. Für manche Kinder in der 3. Klasse kann dies eine sehr anspruchsvolle Aufgabe sein, während dieses systematische Vorgehen, Begründen und Prüfen älteren Kindern erfahrungsgemäß schon leichter fällt.

3 Strikte Geheimhaltung der Passwörter

Wichtig ist, dass
- die in der Klasse entwickelten Passwörter NICHT verwendet werden und
- das eigene Passwort nie jemandem verraten wird.

Daran sollte die Lehrperson abschließend noch einmal erinnern.

Wussten Sie schon?

Obwohl Hacker:innen (vom englischen *hacking* = hacken/herumhacken, auch auf der Tastatur) im Volksmund oft mit krimineller Energie in Verbindung gebracht werden, sitzen diese tatsächlich mehrheitlich in Entwicklungsabteilungen großer Tech-Konzerne zur Optimierung der Sicherheitssysteme. Sie machen Sicherheitslücken ausfindig, die eine wiederum andere Entwicklungsabteilung mit noch ausgeklügelteren Methoden zu schließen versucht.

Hintergrundinfos zum Kapitel

Didaktische Überlegungen

Der Aufbau dieses Kapitels führt

- vom Gesprochenen zum Geschriebenen,
- über die Auseinandersetzung mit Rätselhaftem und
- ausgewählten historischen Methoden des Ver- und Entschlüsselns
- hin zum eigenständigen Erstellen von sicheren Passwörtern.

Die vorgeschlagenen Aufgabenstellungen ermöglichen eine spielerische und für das Grundschulalter angemessene und anschlussfähige Auseinandersetzung mit den Grundzügen des Handwerks von Kryptograf:innen, Informatiker:innen und Hacker:innen. Die Freude am Rätseln und Knobeln sowie am Herstellen von geheimen Nachrichten soll dabei im Zentrum stehen.

Der informatische Schwerpunkt liegt bei allen drei Praxisbeispielen dieses Kapitels auf exemplarisch ausgewählten, regelhaften kryptografischen Verfahren zur Geheimhaltung von Nachrichten. Die dabei entwickelten oder entdeckten „Rezepte“ lassen sich auf alle Texte bzw. im informatischen Sinne auf alle „Probleme derselben Klasse“ übertragen.

Wir empfehlen einen Abstecher in die Verfahren der Steganografie (vom griechischen *steganos* = bedeckt, verschleiert). Überaus spannend finden Grundschulkinder erfahrungsgemäß das Schreiben mit selbst gemachter Geheimtinte. Dabei wird erlebbar, wofür steganografische Techniken verwendet werden: Informationen werden so verborgen, dass sie für Uneingeweihte nicht ersichtlich sind.

Interessanterweise fließen in der heute zukunftsversprechenden sog. molekularen Kryptografie stegano- und kryptografische Konzepte zusammen.

Die Einführung von Fachbegriffen hat es in sich. Tendenziell plädieren Didaktiker:innen aus den Ingenieurs-Wissenschaften gerne eher für die frühe Integration von Fachbegriffen in den Unterricht, anders als Allgemeindidaktiker:innen und Pädagog:innen. Aus pädagogischer Perspektive empfehlen wir bei der Einführung von Fachbegriffen – um das Lernen von Worthülsen zu vermeiden – folgende Faustregel: Kein Begriff ohne Be-Greifen!

Wenn immer möglich sollte sich die Begriffsbildung insbesondere jüngeren Kindern aus der Tätigkeit heraus erschließen oder zumindest auf Erlebtes referenzieren. Je älter die Kinder, desto mehr Fachbegriffe können eingeführt werden, sofern diese auch wirklich begriffen und gedanklich durchdrungen werden können.

Begrifflichkeiten wie

- **Klartext** = ursprünglicher Text, den jede:r lesen kann,
- **Geheimtext** (häufig auch Chiffrierung genannt) = verschlüsselter Text, den nur lesen kann, wer den Schlüssel/Code dazu kennt,
- **chiffrieren** = Verschlüsseln z. B. einer Nachricht, die geheim bleiben soll,
- **dechiffrieren** = Entschlüsseln z. B. einer geheimen Nachricht,
- **Verschlüsselungs-Algorithmus** (häufig auch Code genannt) = Rezept, womit eine Nachricht für Nichteingeweihte unverständlich gemacht werden kann oder mit dem sich eine verschlüsselte Nachricht entschlüsseln lässt, können schrittweise dem Entwicklungsstand der Schüler:innen angepasst eingeführt werden.

Beim lautmalerischen Experimentieren beim Rückwärtsschreiben oder Rückwärtssprechen (= Rückwärtsisch) macht es wenig Sinn, bei der Arbeit mit den Kindern von Klartext und Geheimtext zu sprechen, während beim Verschlüsseln mit der Alberti-Maschine die Benennung dessen, was beim Verschlüsseln tatsächlich getan wird (z. B. „Ich verschlüssle mit einer Verschiebung um 2“) sinnvoll ist.

Mit Blick auf den Kinder- und Jugendschutz: Geheimhaltung relativieren
Die Geheimhaltung der Passwörter (Kapitel 8.3) gilt als Gold-Kriterium, wenn es um Passwort-Sicherheit geht. Der Vergleich, dass Passwörter wie Geheimnisse gehütet werden müssen, ist jedoch mit Vorsicht zu genießen: Er ist nur dann zutreffend, wenn es um die Geheimhaltung von „guten“ Geheimnissen geht. Für Grundschulkinder ist es nicht selbstverständlich, den Unterschied zwischen guten und schlechten Geheimnissen zu kennen und einen entsprechenden Umgang mit ihnen zu haben. Daher wird aus einer medienpädagogischen Perspektive, die Hand in Hand geht mit Medienprävention, die Thematisierung von guten und schlechten Geheimnissen als generell wichtig erachtet – auch unabhängig von den Themen Medien und Mediennutzung.

Bezug zur Kulturgeschichte der Medien

Die Anfänge der Kryptologie (Wissenschaft des geheimen Schreibens, vom griechischen *kryptós* = verborgen) reichen weit in die Geschichte zurück. Bei dieser Kunstform geht es im Wesentlichen darum, Botschaften nach der Anwendung von genau definierten Regeln so zu verändern, dass sie nur noch für Eingeweihte verständlich sind. Dem Entschlüsseln von (geheimen) Texten ohne Kenntnis des Schlüssels widmet sich die Kryptoanalyse, ein Teilgebiet der Kryptologie.

Historische Dokumente aus dem Jahr 1000 belegen Abschnitte über Kryptografie, die zum Schutz von Steuerunterlagen dienen sollte. Andere Quellen berichten bereits von der Anwendung kryptografischer Verfahren 3000 Jahre v. Chr. oder wie aus vorchristlicher Zeit ein Familienrezept in verschlüsselter Form von einer Generation an die nächste weitergegeben wurde. Simon Singh erwähnt zudem, dass der Gedanke nach mehr Gerechtigkeit in allen Bereichen menschlicher Tätigkeit in den blühenden Zeiten des Zusammenspiels von Kunst und Wissenschaft während des Goldenen Zeitalters der frühen islamischen Kultur tragend war und u. a. auch die Weiterentwicklung kryptologischer Methoden ankurbelte.[13]

Oben links im Bild: Krypto-Tool für mechanische Verschlüsselung

13 Simon Singh (2004) vgl. S. 33 f.

Das Schützen von persönlichen und personenbezogenen Daten sowie das Bedürfnis nach sicherer Kommunikation mit „ausgewählten wenigen statt mit allen“ ist seit Menschengedenken (lange vor der Erfindung von Tinte und Papier) aktuell!

Alte und ewig junge kryptografische Methoden?

Mit Caesar (S. 168) oder mit der Skytale (S. 169) verschlüsselte Daten hatten in der Antike Hochkonjunktur, sind aber im Computer-Zeitalter mit Leichtigkeit knackbar. Dennoch: Im Kern fußen die heute gängigen Methoden der Verschlüsselung zum Schutz von digitalen Datenbanken und Datensammlungen sowie für die Gewährung vertraulicher digitaler Kommunikation im Internet (etwa beim e-Banking oder online-Shopping) auf einer Weiterentwicklung derselben Prinzipien.

Versteckte Kryptografie bei der Datenübertragung beim online-Shopping

Die angewendeten Methoden sind fast unvorstellbar komplizierter und komplexer geworden! Wie Jens Gallenbacher in seinem Buch *Abenteuer Informatik* klärend schreibt, gehen die heutigen Herausforderungen bei der sicheren Datenübertragung im Internet aber „deutlich über das Finden von statistisch nicht knackbaren Verfahren hinaus!“[14] Eine darauf bezogene Auseinandersetzung ist für höhere Klassenstufen sinnvoll und setzt das Begreifen des Grundlegenden voraus, das in diesem Kapitel in aufs Wesentliche konzentrierter Form beschrieben ist.

Zum Weiterlesen

- Kessel, Carola (2023). 50 Codes und Geheimschriften. Moses. [Kartenset für Kinder ab 8 Jahren]
- Gallenbacher, Jens (2021). Abenteuer Informatik. IT zum Anfassen für alle von 9 bis 99 – vom Navi bis Social Media. Springer. [Ein Blick hinter die Kulissen der Fachwissenschaft Informatik mit hohem Allgemeinbildungsgrad, für Schüler:innen, Lehrkräfte, Professor:innen und IT-Expert:innen; insbesondere Kap. 12.]
- Hromkovič, Juraj / Lacher, Regula (2019). Einfach Informatik. Lösungen finden 5/6. Klett und Balmer. [Informatik-Lehrmittel für die 5./6. Klasse aus der Reihe einfach informatik.]

Webseiten mit Beiträgen zu „Gute /schlechte Geheimnisse“

- Gute Geheimnisse – Schlechte Geheimnisse.
  Was tun bei belastenden (Online)Erfahrungen?
  www.ajs.nrw/medien/medienkompetenzrahmennrw/methoden/gute-geheimnisse-schlechte-geheimnisse/
- Programm „Mein Körper gehört mir!“
  Präventionsangebote sexualisierter Gewalt im pädagogischen Kontext
  www.kinderschutz.ch/angebote/praeventionsangebote/mein-koerper-gehoert-mir

14 Jens Gallenbacher (2021) S. 292

Bezug zum Medienkompetenzrahmen NRW

1. BEDIENEN / ANWENDEN	2. INFORMIEREN / RECHERCHIEREN	3. KOMMUNIZIEREN / KOOPERIEREN	4. PRODUZIEREN / PRÄSENTIEREN	5. ANALYSIEREN / REFLEKTIEREN	6. PROBLEMLÖSEN / MODELLIEREN
1.1 Medienausstattung (Hardware)	2.1 Informationsrecherche	3.1 Kommunikations- und Kooperationsprozesse	4.1 Medienproduktion und Präsentation	5.1 Medienanalyse	6.1 Prinzipien der digitalen Welt
Medienausstattung (Hardware) kennen, auswählen und reflektiert anwenden; mit dieser verantwortungsvoll umgehen	Informationsrecherchen zielgerichtet durchführen und dabei Suchstrategien anwenden	Kommunikations- und Kooperationsprozesse mit (digitalen) Werkzeugen zielgerichtet gestalten sowie mediale Produkte und Informationen teilen	Medienprodukte adressatengerecht planen, gestalten und präsentieren; Möglichkeiten des Veröffentlichens und Teilens kennen und nutzen	Die Vielfalt der Medien, ihre Entwicklung und Bedeutungen kennen, analysieren und reflektieren	Grundlegende Prinzipien und Funktionsweisen der (digitalen) Welt identifizieren, kennen, verstehen und bewusst nutzen
1.2 (Digitale) Werkzeuge	2.2 Informationsauswertung	3.2 Kommunikations- und Kooperationsregeln	4.2 Gestaltungsmittel	5.2 Meinungsbildung	6.2 Algorithmen erkennen
Verschiedene (digitale) Werkzeuge und deren Funktionsumfang kennen, auswählen sowie diese kreativ, reflektiert und zielgerichtet einsetzen	Themenrelevante Informationen und Daten aus Medienangeboten filtern, strukturieren, umwandeln und aufbereiten	Regeln für (digitale) Kommunikation und Kooperation kennen, formulieren und einhalten	Gestaltungsmittel von Medienprodukten kennen, reflektiert anwenden sowie hinsichtlich ihrer Qualität, Wirkung und Aussageabsicht beurteilen	Die interessengeleitete Setzung und Verbreitung von Themen in Medien erkennen sowie in Bezug auf die Meinungsbildung beurteilen	Algorithmische Muster und Strukturen in verschiedenen Kontexten erkennen, nachvollziehen und reflektieren
1.3 Datenorganisation	2.3 Informationsbewertung	3.3 Kommunikation und Kooperation in der Gesellschaft	4.3 Quellendokumentation	5.3 Identitätsbildung	6.3 Modellieren und Programmieren
Informationen und Daten sicher speichern, wiederfinden und von verschiedenen Orten abrufen; Informationen und Daten zusammenfassen, organisieren und strukturiert aufbewahren	Informationen, Daten und ihre Quellen sowie dahinterliegende Strategien und Absichten erkennen und kritisch bewerten	Kommunikations- und Kooperationsprozesse im Sinne einer aktiven Teilhabe an der Gesellschaft gestalten und reflektieren; ethische Grundsätze sowie kulturellgesellschaftliche Normen beachten	Standards der Quellenangaben beim Produzieren und Präsentieren von eigenen und fremden Inhalten kennen und anwenden	Chancen und Herausforderungen von Medien für die Realitätswahrnehmung erkennen und analysieren sowie für die eigene Identitätsbildung nutzen	Probleme formalisiert beschreiben, Problemlösestrategien entwickeln und dazu eine strukturierte, algorithmische Sequenz planen; diese auch durch Programmieren umsetzen und die gefundene Lösungsstrategie beurteilen
1.4 Datenschutz und Informationssicherheit	2.4 Informationskritik	3.4 Cybergewalt und -kriminalität	4.4 Rechtliche Grundlagen	5.4 Selbstregulierte Mediennutzung	6.4 Bedeutung von Algorithmen
Verantwortungsvoll mit persönlichen und fremden Daten umgehen; Datenschutz, Privatsphäre und Informationssicherheit beachten	Unangemessene und gefährdende Medieninhalte erkennen und hinsichtlich rechtlicher Grundlagen sowie gesellschaftlicher Normen und Werte einschätzen; Jugend- und Verbraucherschutz kennen und Hilfs- und Unterstützungsstrukturen nutzen	Persönliche, gesellschaftliche und wirtschaftliche Risiken und Auswirkungen von Cybergewalt und -kriminalität erkennen sowie Ansprechpartner und Reaktionsmöglichkeiten kennen und nutzen	Rechtliche Grundlagen des Persönlichkeits- (u.a. des Bildrechts), Urheber- und Nutzungsrechts (u.a. Lizenzen) überprüfen, bewerten und beachten	Medien und ihre Wirkungen beschreiben, kritisch reflektieren und deren Nutzung selbstverantwortlich regulieren; andere bei ihrer Mediennutzung unterstützen	Einflüsse von Algorithmen und Auswirkung der Automatisierung von Prozessen in der (digitalen) Welt beschreiben und reflektieren

Medienkompetenzrahmen NRW https://www.schulministerium.nrw/medienkompetenzrahmen-nrw

8.4 Medienbildung in der Aus- und Weiterbildung von Lehrer:innen: Freude, Computational Thinking und die Krux mit dem Forschungsstand

Interview mit Dr.in Paula Bleckmann, Professorin für Medienpädagogik

„Ich empfehle mit Nachdruck, Digitale Bildung mehr an Entdeckungsfreude orientiert zu gestalten und weniger aus Angst vor Risiken, was aber oft gemacht wird. Warum verschlüsseln wir? Erst einmal, weil es Spaß macht. Und nicht primär aus Angst vor Datenklau und Cybergrooming.“ Paula Bleckmann

Paula Bleckmann im Interview

Wir haben Sie bei einem mehrtägigen Blockseminar mit Pädagogik-Studierenden an der Alanus Hochschule besucht. Es fällt auf, dass Sie die Mehrheit der Vorlesungen sehr handlungsorientiert gestalten. Ist dies Zufall?

Es ist das Gegenteil von Zufall. Es ist ein didaktisches Konzept, bei dem im besten Fall zwei Ebenen übereinstimmen sollen. Nämlich der Inhalt dessen, was vermittelt wird, und dann die Art, wie es den Studierenden nahegebracht wird. Es geht mir darum, den angehenden Lehr- und KiTa-Fachkräften gleichzeitig Inhalte wie auch Vermittlungswege an die Hand zu geben, die später bei der Arbeit mit den Kindern genauso wie für einen Elternabend hilfreich sein können.

Eine praktische und zugleich zukunftsorientierte Herangehensweise, die vielleicht sogar die Kluft zwischen Theorie und Praxis in der Lehrkräfte-Ausbildung schließt? Was meinen Sie dazu?

Dieser Versuch muss unternommen werden. Im allerbesten Fall bekommen die Studierenden im Seminar die Rolle der Lehrkraft, die bestimmte handlungsorientierte Aktivitäten aus der aktiven Medienarbeit und der informatischen Bildung selbst anleitet. Der Transfer fällt viel leichter, wenn auf Hochschulebene handlungsorientiert unterrichtet wird. Für mich ist es wunderbar, wenn im Rückmeldebogen von einer berufsbegleitenden Studierenden steht: „Die Praxisbeispiele im Seminar haben Freude gemacht! Das kann ich nächste Woche im Unterricht genauso umsetzen.“

Worum geht's, wenn Sie mit dem Turm der Medienmündigkeit arbeiten?

Das Wichtigste ist die Erkenntnis, dass die Basis für den späteren selbstbestimmten Umgang mit digitalen Medien überhaupt nicht am Bildschirm erwerbbar sein kann, sondern im realen Leben mit allen Sinnen erworben wird, im direkten Weltkontakt und im sozialen Miteinander. Besonders im unmittelbaren Kontakt mit anderen Menschen. Das ist etwas, was in der Arbeit mit den Studierenden immer wieder zu „Aha“-Erlebnissen führt.

Turm der Medienmündigkeit[15]

Was sind weitere Themen-Highlights in der Arbeit mit den Studierenden?

Spontan denke ich an die Seminareinheiten zum Thema Geheimsprachen und Kryptografie, das analoge Sortiernetzwerk, die Solarfotografie und die Binäre Murmeladdiermaschine, insbesondere auch der Kartentrick mit den Zahlen von 0 bis 31. Da ist für die Studierenden besonders prägend, dass etwas, was uns erst wie Zauberei erscheinen musste, irgendwann als schlichte Mathematik wirklich verstanden und durchdrungen wird.

15 Von Paula Bleckmann (2012).

Wie erklären Sie sich das positive Echo bei den Studierenden?

Genauso wie bei den Kindern, die den Zaubertrick mit Freunden oder in der Familie immer und immer wieder gerne vorführen wollen. Ich glaube, sie werden damit für eine kurze Zeit quasi zum „Täter“ statt zum „Opfer“ und genießen den Rollenwechsel, den sie dabei für einen Moment selbst herbeiführen können.

Kinder erleben: Ich lebe in einer Welt, die in weiten Teilen nicht durchschaubar und verständlich ist, die erst einmal wie Magie wirkt. Und dann zaubern sie und freuen sich über die Erkenntnis: Hier habe ich etwas, womit ich Menschen total verblüffen kann. Es ist aber ein Zauber, der keiner ist.

„Zauber, der keiner ist“: Ist das vielleicht das neue Geheimrezept für nachhaltige Lernprozesse in der Erwachsenenbildung?

Das müssen wir uns näher anschauen: Erstens, indem ich etwas tue, was für andere auf den ersten Blick nach Zauberei ausschaut, verstehe ich, dass ein binärer Suchalgorithmus dahintersteckt, dass es eigentlich ganz schlichte Mathematik ist und keine Zauberei. Das ist die Ebene des Informatikunterrichts.

Zweitens ist es ein tolles Beispiel für die Elternzusammenarbeit. Und drittens spielt für mich da etwas Übergeordnetes mit hinein, das schwerer zu fassen ist: nämlich die Demystifizierung, also die Entzauberung von Digitaltechnologie, die durch solche persönlichen „Aha“-Effekte bewirkt wird.

Ich möchte, dass alle Studierenden in diesen Seminaren zum Beispiel beim Thema Geheimsprachen diese „Aha“-Effekte selbst erlebt haben, damit wir dann die Frage stellen können: „Was haben Sie denn getan, um zu entschlüsseln?“

Dabei machen Sie es den Studierenden nicht ganz einfach! Was hat es mit dem „Erklär-Verbot“ auf sich?

Als wir das Thema Geheimschriften behandelt haben, stand eine verschlüsselte Botschaft an der Tafel und ich habe tatsächlich gesagt: „Sie sind eingeladen, das zu lesen. Bitte nicht vorsagen, nicht reinrufen oder erklären – wir haben gerade ‚Erklär-Verbot‘. Sie zeigen mir, dass Sie verstanden haben, was da steht, indem Sie es einfach tun.“

Ist es nicht furchtbar schwer, sich an das Erklär-Verbot zu halten? Oder anders: Was hilft, damit man sich an das Erklär-Verbot halten kann?

Doch, natürlich, es ist schwer! Das sind ja angehende Pädagog:innen, quasi von Beruf „Erklärer:innen“. Es ist in fast jedem Kurs so, dass eine Person direkt reinruft, weil es so viel Freude macht, dieses „Aha“-Erlebnis zu haben, dass daraus ein großes Mitteilungsbedürfnis folgt.

Sich mit Erklären zurückzuhalten, ermöglicht aber ein viel nachhaltigeres Lernen. Das ist ein Grundzug meines Unterrichtens und mag vielleicht auch an das exemplarisch-genetisch-sokratische Lernen von Martin Wagenschein erinnern.

Die Freude also als Antrieb für nachhaltiges Lernen?

Hier antworte ich „Ja, aber …“: Einerseits ist mir dieser am Freudvollen orientierte Zugang zu informatischen Themen wichtig, die zum Teil mit Vorurteilen behaftet sind. Ich empfehle mit Nachdruck, digitale Bildung mehr an Entdeckungsfreude orientiert zu gestalten und weniger aus Angst vor Risiken, was aber oft gemacht wird. Warum verschlüsseln wir? Erst einmal, weil es Spaß macht. Und nicht primär aus Angst vor Datenklau und Cybergrooming. Klar, später ist digitale Selbstverteidigung mit sicheren Passwörtern auch wichtig.

Bildmanipulation geht auch analog: zum Beispiel mit dem Zerrspiegel

Kommen wir zum „Aber“?

Freude ist der Lernmotor. Das große Aber ist: In der Erwachsenenbildung muss nach der Freude auch die Selbstreflexion kommen. Es ist sehr wichtig, mit Studierenden nach solchen freudigen „Aha“-Erlebnissen einen Stopp einzulegen, zu beschreiben und beim Ver- und Entschlüsseln zu fragen: „Du hast verschlüsselt und entschlüsselt. Du hast es als sehr beglückend empfunden, dass Du etwas selbst herausgefunden hast, ohne dass Dir jemand auf die Sprünge geholfen hat. Würdest du dann nicht den anderen auch gönnen wollen, dass sie selbst darauf kommen?“ Und: „Wie hast Du es geschafft, das Rätsel zu lösen, obwohl Du anfänglich erst einmal nur ‚Bahnhof‘ verstanden hast?“

Dieses Reflektieren kann hilfreich sein für die professionelle Perspektiv-Übernahme für die spätere Arbeit im Beruf.

Im konkreten Fall: Was tun die Studierenden, um das „Kauderwelsch“ zu entschlüsseln, das Sie an die Tafel geschrieben haben?

Die strategischen Lösungsansätze sind meistens sehr ähnlich. Es wird erst versucht, ein Muster zu erkennen. Das ist die sogenannte *pattern recognition*. Dann wird das lange Kauderwelsch in handhabbare Unterabschnitte zerlegt, das

nennt man *decomposition*. Schließlich trennt man Unwichtiges von Wichtigem – *abstraction*. Es wird auch versucht, Regeln zu formulieren und diese anzuwenden, also *algorithm design*.

Sind das nicht Strategien, die wir aus unserem Lebensalltag gut kennen?

Ja, das stimmt. Diese vier eben beschriebenen Tätigkeiten sind auch das, was kleine Kinder fast ununterbrochen üben, wenn sie sprechen lernen. Mustererkennung gerade dann, wenn sich Muster darbieten, durch Verse und Reime oder Lieder, die immer wieder gesungen werden – in einer guten Balance aus Erstmaligem und Neuem. Interessanterweise sind aber diese vier Tätigkeiten auch Bestandteile des *Computational Thinking*. Nach den Informatikprofessoren Curzon und McOwan ist dies das gehypte Konzept – Fähigkeiten, die Kinder brauchen, um später Top-Programmierer:innen zu werden.

Computational Thinking. Heißt das „denken wie ein Computer"?

Ganz sicher nicht, schon allein, weil Computer gar nicht denken können. Computational Thinking heißt, Probleme so umzuformulieren, dass sie als Folge von Handlungsanweisungen durch andere Menschen, aber auch durch Maschinen Schritt für Schritt abgearbeitet werden können. Das müssen ganz und gar nicht nur Programmierer können. Es ist für Mütter, Väter, Unternehmensberaterinnen, Bauern und Bäcker:innen genauso hilfreich.

Und im Bereich Elternzusammenarbeit: Welches Rüstzeug möchten Sie da den Studierenden mit auf den Weg geben?

Erstens möchte ich Studierenden vermitteln, wie man Erlebnisräume ohne Moral und Zeigefinger schaffen kann, in denen man sich ein eigenes Urteil bilden darf. Das ist die Grundlage, damit später mit Eltern in möglichst wertfreier Atmosphäre über so etwas wie Digitalrisiken für Kinder gesprochen werden kann. Zu erleben, warum Dinge wie wirken, ist viel wichtiger, als zu wissen, welche exakte Wirkstärke laut Forschungsstand aktuell gemessen wird.

Zweitens will ich zu einer differenzierten Reflexion der eigenen Medienbiografie anregen. Jasmin Zimmer hat in ihrer Doktorarbeit gezeigt, dass man nicht bestimmt oder determiniert ist durch die eigene Medienkindheit oder -jugend in Bezug auf die medienbildnerische Professionalisierung. Entscheidend ist, wie differenziert jemand reflektiert, was passiert ist, als er oder sie klein war. Was haben die eigenen Eltern gut gelöst und würde man das auch so machen oder wovon will man sich distanzieren?

Ihre Ansätze für digitale Bildung und Elternzusammenarbeit sind spannend, aber auch unkonventionell. Was bedeutet dies für Studienabgänger:innen?

Es kann sein, dass sie in Situationen kommen, in denen sie für ihre Haltung angegriffen werden und sich rechtfertigen müssen, weil das dem Mainstream widerspricht. Ich möchte dafür sorgen, dass sie als Studienabgänger:innen auch dafür gerüstet sind und verstehen lernen, weshalb das so ist. In den Seminaren spreche ich das direkt an: „Sie haben jetzt vieles gelernt, vieles erfahren. Machen Sie sich darauf gefasst, dass das nicht alle so sehen, dass Sie mit dieser Haltung auch als rückständig kritisiert werden können."

Was ist dran an dem Vorwurf, dass mit diesem Ansatz und dieser (medien-) pädagogischen Haltung aktuelle Entwicklungen verschlafen werden?

Fakt ist, dass in der Welt außerhalb der Hochschulen viele Wissensbestände stark zurückgedrängt werden. Studierende müssen auch verstehen lernen, wer digitale Bildungspolitik beeinflusst. Ich nenne da gerne das Beispiel der Tabakkonzerne und deren Strategien, Forschung zu schädlichen Wirkungen des Rauchens zu unterdrücken. Was rückständig ist und was fortschrittlich, kann man oft erst 20 Jahre später fundiert beurteilen. Da darf man auch an FCKWs und das Ozonloch denken.

In der Debatte um Digitale Bildung ist ein Beispiel aus Schweden interessant: Eine Bildungsministerin positioniert sich als fortschrittliche Frühdigitalisiererin und führt quasi eine Tablet-Pflicht ein. Ihre Nachfolgerin gibt ein wissenschaftliches Gutachten in Auftrag und schafft aufgrund der berichteten Forschungslage diese Regelungen wieder ab. Da ist der Schritt zurück ein Fortschritt.

Warum wird denn nicht von Anfang an der Forschungsstand berücksichtigt?

Es ist wichtig zu wissen, wie große IT-Firmen sogenanntes public perception management betreiben. Die Behauptung „Da steckt doch die IT-Industrie dahinter!“ kann erst einmal wie eine Verschwörungstheorie wirken. Deshalb finde ich es so wichtig, faktenbasiert zu unterrichten: Wir ziehen dann die Dissertation von Jesper Balslev hinzu oder die Netzwerkanalysen von Annina Förschler. Das dient auch der Selbstvergewisserung: Man hat Dinge gelernt, die sehr wahrscheinlich nicht Teil des Mainstream-Wissens sind, und man versteht, warum dieses Wissen unterdrückt wird.

Wie muss man sich das in der praktischen Vermittlung vorstellen?

Sehr beliebt ist das Rollenspiel, bei dem ich mir eine blonde Perücke aufsetze und eine amerikanische Marketing-Fachfrau spiele. Die Dame vermittelt den Studierenden, wie man möglichst viel Geld mit der Vermarktung von digitalen Medienprodukten an Kinder und Jugendliche verdienen kann. Ein Schockerlebnis für viele Studierende, was aber oft auch als Augenöffner erlebt wird.

Als Augenöffner für was?

Es zeigt sich darin, wie viel Einflussnahme von gigantischen multinationalen Konzernen es Eltern und Lehrkräften schwer macht, sich so zu verhalten, wie sie es eigentlich als richtig erachten. Das spielt mit hinein in die Bildungspolitik, die es entsprechend schwer hat, eine kritische, mündigkeitsorientierte Digitale Bildung in den Bildungsplänen zu verankern.

Nehmen wir an, Sie haben einen Wunsch frei. Was sollte, wenn es um Digitale Bildung geht, zwingend berücksichtigt werden?

Als Forscherin würde ich mir wünschen, dass es weiterhin auch analoge Kontrollgruppen gibt und dass die analoge Praxis weiterentwickelt und auch finanziell gefördert wird. Meine Hypothese ist, dass Lernen ohne Bildschirm für KiTa und Grundschule langfristig besser wirkt, dass mehr „slow thinking“, wie es

beispielsweise meine Studierenden bei analogen Unterrichtszenarien mit Erklär-Verbot üben, besser wirkt. Ich könnte natürlich unrecht haben. Aber wie sollen Forscher:innen in 20 Jahren überhaupt noch überprüfen, ob meine Hypothese stimmte oder diejenige der Verfechter der Frühdigitalisierung, wenn es nur noch Digital-KiTas und Tablet-Grundschulen gibt?

Zum Weiterlesen

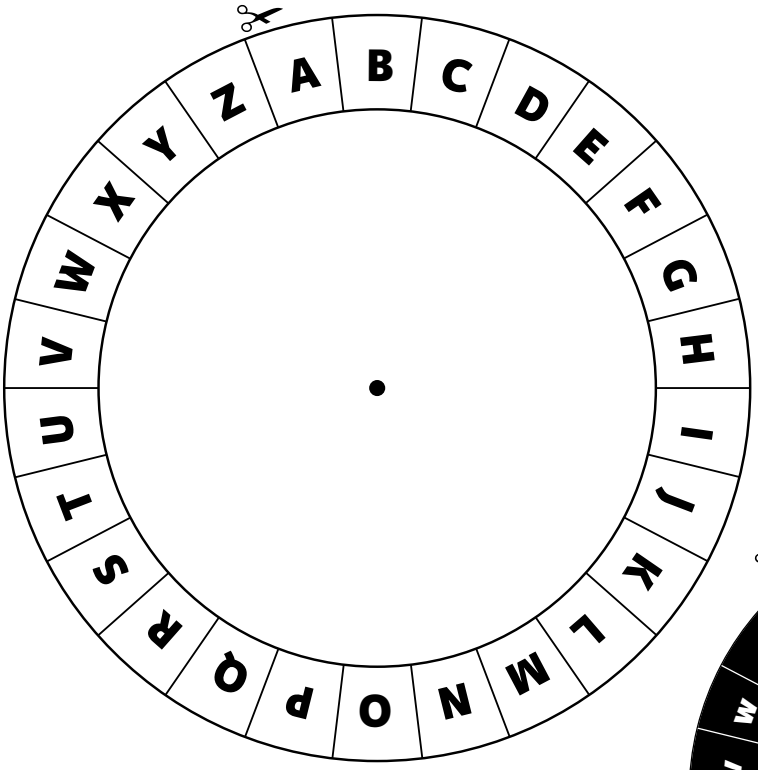
- Bleckmann, Paula (2020). Medienmündig:
  Wie unsere Kinder selbstbestimmt mit dem Bildschirm umgehen lernen. 7. Auflage. Klett-Cota.
- Zimmer, Jasmin (vsl. 2024). Bildung und digitale Medien in der Kita. Eine Grounded Theory zu Haltungen und Praxis pädagogischer Fachkräfte. Brill | Schöningh.

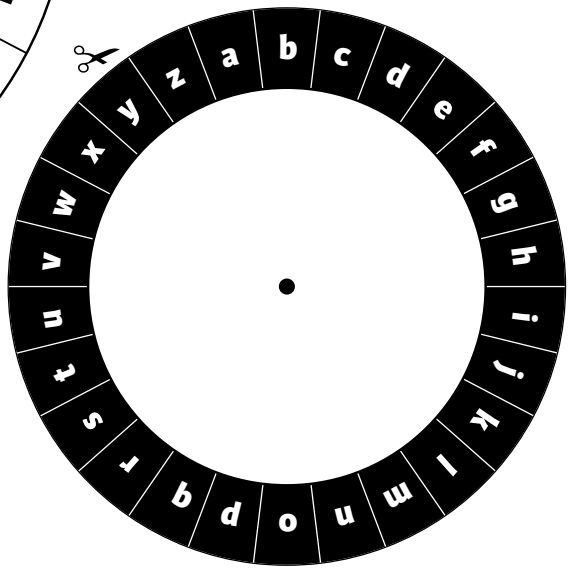
Webseiten

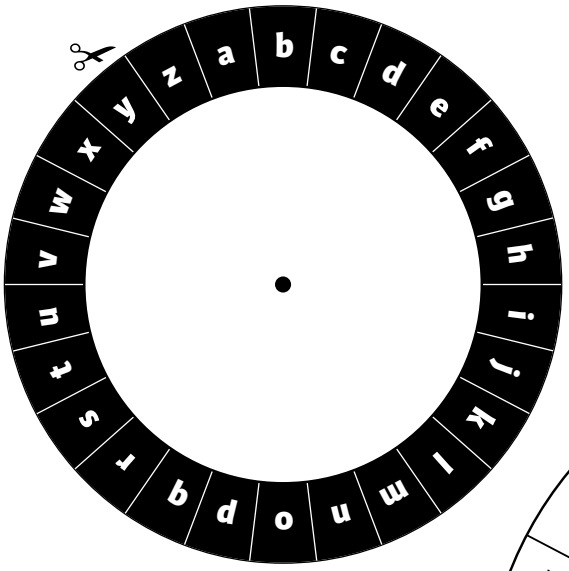
- Balslev, Jesper (2020). Evidence of a potential: The political arguments for digitizing education 1983–2015. Ph.D. dissertation. Department of Communication and Arts, Roskilde University (DK).
  www.jesperbalslev.dk/evidence-of-a-potential-ph-d-thesis/
- Förschler, Annina (2018). Das ‚Who is who?' der deutschen Bildungs-Digitalisierungsagenda – eine kritische Politiknetzwerk-Analyse. Pädagogische Korrespondenz 58 (2). S. 31–52.
  Budrich Academic Press.
  www.doi.org/10.25656/01:21106

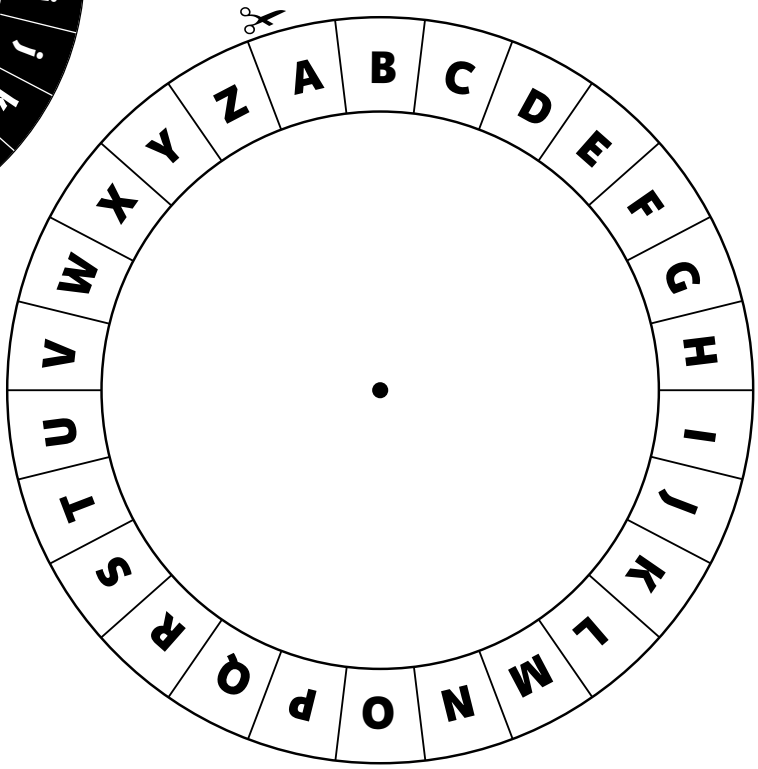
Anhang 1

Kopiervorlage „Alberti-Maschine zum Selbermachen“



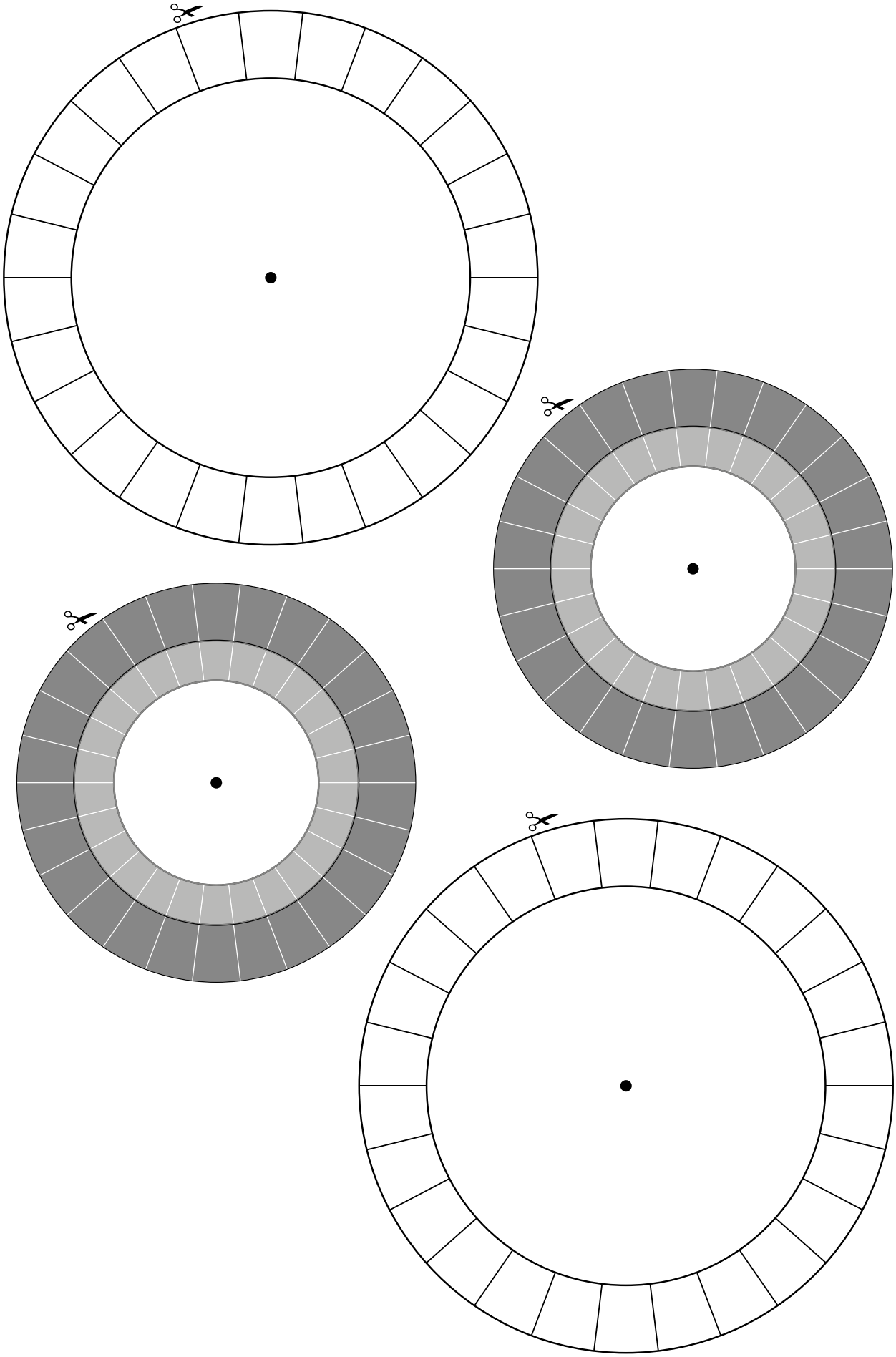






Anhang 2

Kopiervorlage blanko „Alberti-Maschine zum Selbermachen“



Anhang 3

Kopiervorlage „Sicheres Passwort“

Checkliste Passwort

Mein sicheres Passwort besteht aus

- ☐ **Buchstaben und Ziffern** (abcDEFghi 76540)
- ☐ **Großbuchstaben und Kleinbuchstaben** (DJdjaojoUOIOKOA)
- ☐ **einem oder mehreren Interpunktionszeichen** (,:.!?;)
- ☐ **einem verschlüsselten Wort, das nicht auf Anhieb mit der Person in Verbindung gebracht wird**
- ☐ **maximal 12 Zeichen/Symbole** (**********)

Checkliste Passwort

Mein sicheres Passwort besteht aus

- ☐ **Buchstaben und Ziffern** (abcDEFghi 76540)
- ☐ **Großbuchstaben und Kleinbuchstaben** (DJdjaojoUOIOKOA)
- ☐ **einem oder mehreren Interpunktionszeichen** (,:.!?;)
- ☐ **einem verschlüsselten Wort, das nicht auf Anhieb mit der Person in Verbindung gebracht wird**
- ☐ **maximal 12 Zeichen/Symbole** (**********)

Bildnachweise zu diesem Kapitel

Seite	157	© skynesher / www.istockphoto.com
	160	© Illustration Birgit Köhl-Tömmes
	161	© Illustration Birgit Köhl-Tömmes
	162	© Brigitte Pemberger
	163	© Illustrationen Birgit Köhl-Tömmes
	164	© Illustration Birgit Köhl-Tömmes
	165	© Illustration Birgit Köhl-Tömmes
	168	© Brigitte Pemberger
	169	© Brigitte Pemberger
	170	© Brigitte Pemberger
	171	© Grafissimo / www.istockphoto.com
	171	© Photoholyday / www.pixabay.com
	171	© Philipp / www.pixabay.com
	171	© Wolfgang Eckert / www.pixabay.com
	171	© Felix Lichtenfeld / www.pixabay.com
	171	© Marc Manhart / www.pixabay.com
	171	© Mariusz Czarnas / www.pixabay.com
	171	© Cometary / www.istockphoto.com
	172	© Grafissimo / www.istockphoto.com
	173	© Brigitte Pemberger
	176	© Moussa81 / www.istockphoto.com
	177	© Preis_King / www.pixabay.com
	178	© Medienkompetenzrahmen NRW, www.medienkompetenzrahmen.nrw
	179	© Charlotte Fischer
	180	© Paula Bleckmann
	182	© Brigitte Pemberger
	187	© Illustration Birgit Köhl-Tömmes