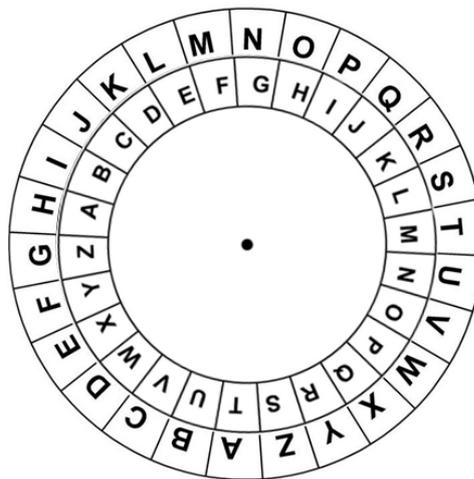


# Verschlüsselungen

## (LU 7)



### Inhaltsverzeichnis

<b>A Lernumgebung</b>	<b>2</b>
<b>B Hinweise für die Lehrkraft</b> (mit Bezug zum Rahmenlehrplan und mit Hinweisen zur Sprachbildung im Rahmen dieser Lernumgebung)	<b>3</b>
<b>C Arbeitsbögen / Materialien / Lösungen</b>	<b>10</b>
<b>D Anhang</b>	<b>22</b>



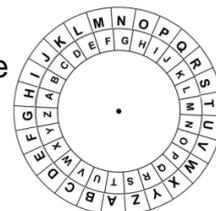
1. Schon die alten Ägypter haben Nachrichten verschlüsselt. Eine einfache Verschlüsselung ist der nach dem römischen Kaiser benannte Cäsar-Code.

Code A→C heißt:  
Beim Entschlüsseln  
wird aus dem C ein A.

Die Verschlüsselungsregel für die folgende Nachricht ist A→C.  
Entschlüssele die Nachricht.

RTKOC, FW JCUV FKG PCEJTKEJV TKEJVKI GPVUEJNWGUUGNV.

2. Zum Verschlüsseln mit dem Cäsar-Code kann man die Cäsar-Scheibe nutzen. Stelle sie her, wähle eine Verschlüsselungsregel und verschlüssele eine Nachricht.



3. Entschlüssele die Nachricht eines anderen Kindes.

Die häufigsten Buch-  
staben sind der  
Reihe nach  
E, R, I, N und S.



4. Jetzt ist der Schlüssel nicht vorgegeben. Nutzt zum Knacken des Codes die Häufigkeiten der einzelnen Buchstaben in der deutschen Sprache.

WXMEEQ. PG NU EF VM QUZ DUOTFUSQD SQTQUYOAPQ-QJBQDFQ.

5. Der französische Diplomat Blaise de Vigenère hat die Cäsar-Verschlüsselung weiter entwickelt. Man muss dem Empfänger der Nachricht ein Schlüsselwort übermitteln.

- a) In der Abbildung ist die Methode erklärt. Erkundet die Verschlüsselungsmethode und verschlüsselt eure Namen mit dieser Methode.
- b) Wählt ein eigenes Schlüsselwort und codiert eine Nachricht. Nutzt [M4](#) oder das Computerprogramm.

	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	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
2	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
3	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
4	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
5	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

1	2	3	4	5	1	2		3	4	5	1	2	3	4	5	1
G	E	H	E	I	M	E		N	A	C	H	R	I	C	H	T
S	E	A	L	M	Y	E		G	H	G	T	R	B	J	L	F

## 1 Einordnung innerhalb des Themenbereichs

Geheime Nachrichten faszinieren Kinder. Sie wecken ihre Neugierde und Motivation. Gleichzeitig beinhalten Fragen der Verschlüsselung vielfältige mathematische Aspekte.

„Informationen geheim halten und weitergeben zu können, ist von hoher Alltagsrelevanz. Man denke nur an die Vielzahl von Geheimnummern, die man für EC-Karten, das Homebanking oder die Programmierung von Autoradios benötigt. Zudem interessieren sich viele Kinder dafür, wie man Botschaften verschlüsseln und wieder entschlüsseln kann. ... Somit stellen Geheimschriften in doppelter Hinsicht ein lohnendes Unterrichtsthema im Schnittbereich von Mathematik und Sprache dar.“<sup>1</sup>

Inhaltlich steht in dieser Lernumgebung der Aspekt der Zuordnung im Mittelpunkt. Der Cäsar-Code<sup>2</sup> ist eine eindeutige Zuordnung: Jedem Buchstaben wird genau ein anderer Buchstabe zugeordnet und umgekehrt. Er lässt sich über die Häufigkeit der Buchstaben im Alphabet auch dann leicht entschlüsseln, wenn der Codierungsschlüssel nicht bekannt ist.

Der Vigenère-Code ist eine symmetrische, polyalphabetische Verschlüsselung. Sie ist nicht eindeutig: Einem Buchstaben in der Originalnachricht werden abhängig von der Position des Buchstabens in der Nachricht unterschiedliche Buchstaben zugeordnet.

Das in dieser Lernumgebung geförderte Verständnis für Zuordnungen kann zur Entwicklung des Grundverständnisses für funktionale Zusammenhänge beitragen. Die Kinder nutzen eine Verschlüsselungstabelle (Wertetabelle) zur Codierung und Decodierung. Zum Auffinden des Codierungsschlüssels bestimmen sie Häufigkeiten.

Das Ver- und Entschlüsseln ist ein Algorithmus, den die Lernenden schrittweise durchführen. Sie analysieren und beschreiben Algorithmen. Sie nutzen statistische Methoden zur systematischen Decodierung von verschlüsselten Nachrichten. Darüber hinaus werden die Kreativität, eine sorgfältige Arbeitsweise, die Konzentrationsfähigkeit und Ausdauer gefördert.

Für die Verschlüsselung können geeignete Apps genutzt werden. Die Verschlüsselungstabellen für den Vigenère-Code können die Schülerinnen und Schüler mit einem Tabellenkalkulationsprogramm erstellen. Die Themen Verschlüsselung von Daten und Datensicherheit werden diskutiert. Damit leistet die Lernumgebung einen wesentlichen Beitrag zur Medienerziehung.

Mit dieser Lernumgebung werden Inhalte und Kompetenzen der Leitideen [L4] *Gleichungen und Funktionen* und [L5] *Daten und Zufall* vermittelt und entwickelt.

**Niveaustufe C, D**

<sup>1</sup> Sundermann, Beate; Selter, Christoph: HFIFJN! Botschaften verschlüsseln wie Julius Caesar. In: Grundschulzeitschrift (2003) 163, S. 41

<sup>2</sup> Der Cäsar-Code ist eine symmetrische Verschlüsselung: Sender und Empfänger der Nachricht benutzen den gleichen Schlüssel. Bei asymmetrischen Verschlüsselungsverfahren nutzen Sender und Empfänger unterschiedliche Schlüssel. Weitere Informationen zu unterschiedlichen Verschlüsselungsverfahren und ihrer Geschichte in: Baumanns, Lukas; Dick, Janine; Rott, Benjamin: Verschlüsselung, Fehlerbeseitigung Kompression. In: Mathematik lehren (2020) 219, S. 2 - 7

## 2 Didaktisch-methodische Hinweise (praktische Hinweise zur Durchführung)

**Zeitungsumfang:** 4 bis 6 Unterrichtsstunden

### Einführung:

Für die Einführung sind zwei Varianten denkbar:

- Die Lehrkraft lässt die Schülerinnen und Schüler über ihre Erfahrungen mit geheimen Nachrichten berichten. Sicherlich kennen die Kinder Möglichkeiten, Nachrichten geheim zu übermitteln - entweder mit einem Code oder zum Beispiel mit Zaubertinte.
- Die Klasse erhält eine verschlüsselte Nachricht ([M1](#)), die sie entschlüsseln muss. Hierfür bietet sich eine Verschlüsselung mit dem Cäsar-Code, die Verwendung einer Bilderschrift, die Wort-Rückwärts-Methode oder eine Verschlüsselung mit einer eingefügten Silbe an. Einen Anhaltspunkt für die Entschlüsselung erhalten die Kinder über die Anrede mit dem Klassennamen. Sie werden darauf hingewiesen, dass die Umlaute ersetzt wurden. Die Nachricht kann gemeinsam im Unterrichtsgespräch aber auch in Partnerarbeit entschlüsselt werden.

### zu 1.:

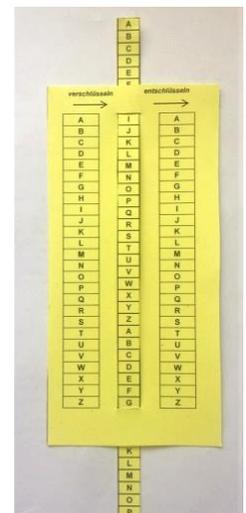
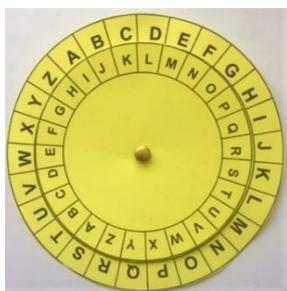
Nachdem darüber gesprochen wurde, warum Verschlüsselungen schon seit Tausenden von Jahren von den Menschen genutzt werden, entschlüsselt jedes Kind die erste Nachricht. Bei Bedarf wird einzelnen Kindern eine Entschlüsselungstabelle ([M2](#)) zur Verfügung gestellt.<sup>3</sup>

Für die Verschlüsselung dieser Nachricht wurde der Code A→C (+2) verwendet. Das heißt, dass beim Entschlüsseln aus dem C ein A, aus dem D ein B, aus dem E ein C usw. wird.

### zu 2.:

Anschließend stellt jedes Kind eine Cäsar-Scheibe<sup>4</sup> ([M3](#)) oder einen Verschlüsselungsstreifen ([M7](#)) her und verschlüsselt mindestens eine eigene Nachricht. Die Cäsar-Scheibe bzw. der Streifen können bei Bedarf mit einer Büroklammer fixiert werden.

Leistungsstärkere Schüler werden wahrscheinlich längere Nachrichten verschlüsseln. Da ein anderes Kind anschließend die Nachricht entschlüsseln soll, könnten die Kinder selbst den Schwierigkeitsgrad ihrer Aufgabe einschätzen und zum Beispiel mit Sternchen markieren. Aufgrund der unterschiedlichen Arbeitsgeschwindigkeit bietet sich ein Lerntempoduett an: Kinder, die eine Nachricht verschlüsselt haben, treffen sich an einer Haltestelle und tauschen ihre Nachrichten zum Entschlüsseln aus.



<sup>3</sup> Zur Verschlüsselung mit dem Cäsar-Code stehen eine Reihe von Apps zur Verfügung, z. B. <https://gc.de/gc/caesar/>. (Sie verlassen mit diesem Link die sicheren Seiten des Bildungsservers.) Bevor Apps eingesetzt werden, sollten die Kinder jedoch das Prinzip verstanden und auch selbst angewendet haben.

<sup>4</sup> Die Scheibe wird in einigen Quellen auch als Alberti-Scheibe bezeichnet. Der italienische Universalgelehrte Leon Battista Alberti soll sie als Erster im 15. Jahrhundert zum Dechiffrieren von Codes genutzt haben.

**zu 3.:**

Jedes Kind entschlüsselt die Nachricht eines anderen Kindes. Eventuell auftretende Fehler werden markiert und anschließend miteinander diskutiert. Da bisher keine Vereinbarung über die Verwendung der Cäsar-Scheibe (Leserichtung von innen nach außen oder von außen nach innen) getroffen wurde, müssen die Kinder unter Umständen experimentieren. Eine Festlegung wird in der folgenden Auswertungsphase diskutiert.

In dieser Phase wird auch besprochen, welchen Vorteil die Cäsar-Scheibe gegenüber einer normalen Entschlüsselungstabelle wie in Aufgabe 1 bietet. Sollten die Kinder nicht auf die Idee kommen, werden sie aufgefordert, eine kurze Nachricht mit einem neuen Schlüssel zu verschlüsseln. Dazu dürfen einige Kinder die Scheibe nutzen, die anderen müssen erst eine Tabelle ([M2](#)) erstellen.

**zu 4.:**

Im Regelfall ist der Schlüssel nicht vorgegeben. Dann kann mit Hilfe der Häufigkeit der einzelnen Buchstaben in der Nachricht versucht werden, den Schlüssel zu ermitteln. Die Schülerinnen und Schüler legen eine Häufigkeitstabelle an und ermitteln mit deren Hilfe Vermutungen über den Schlüssel. Bei Bedarf wird die Tippkarte ([M5](#)) eingesetzt. Für den Fall, dass die Kinder die Nachricht zufällig sehr schnell entschlüsseln ohne die Häufigkeit der Buchstaben zu untersuchen, enthält [M6](#) eine weitere Nachricht, die mit einem anderen Code verschlüsselt wurde.

Schnelle Schülerinnen und Schüler können weitere Nachrichten ver- bzw. entschlüsseln. Zum Verschlüsseln kann auch ein PC-Programm (z. B. <https://gc.de/gc/caesar/>) genutzt werden. Im Anschluss werden die Kinder aufgefordert, die Wirksamkeit des Cäsar-Codes als Geheimcode zu bewerten. Diese Diskussion wird auch genutzt, um das Thema Verschlüsselung von Daten und Datensicherheit zu diskutieren, das auch im Alltag von Grundschülerinnen und Grundschulern sehr relevant ist.

**zu 5.:**

Bevor die Aufgabe gelöst werden kann, muss das Prinzip der Vigenère-Verschlüsselung erfasst werden. Dazu stehen bei Bedarf Tippkarten ([M5](#)) zur Verfügung. Nachdem die Methode erfasst wurde, verschlüsseln die Partner ihre Namen.

Für eine eigene Verschlüsselung kann jedes Paar eine Verschlüsselungsmatrix ([M4](#)) erstellen. Da das aufwendig ist, steht eine Excel-Tabelle zur Verfügung, in der nur das Schlüsselwort eingegeben werden muss. Kann das Programm nicht genutzt werden, sollte das verschlüsselnde Paar seine Verschlüsselungsmatrix an das entschlüsselnde Paar weitergeben. Die verschlüsselte Nachricht kann zunächst in eine Tabelle eingetragen werden.

**Erweiterung:**

Sicherlich sind einige Kinder auch weiterhin vom Thema Geheimschrift fasziniert. Sie können Anregungen auf Internetseiten für Kinder nutzen. Material [M6](#) enthält eine Zusammenstellung interessanter Internetseiten (einschließlich QR-Codes für die Nutzung mit dem Tablet).

### 3 Bezug zum Rahmenlehrplan

#### 3.1 Prozessbezogene mathematische Standards der Lernumgebung<sup>5</sup>

(siehe Handreichung, Punkt 2)

Mathematisch argumentieren	Probleme mathematisch lösen	Mathematisch modellieren	Mathematische Darstellungen verwenden	Mit symbolischen, formalen und technischen Elementen umgehen	Mathematisch kommunizieren
1.1.2	2.1.1, 2.2.1		4.2.1	5.1.1	6.1.1, 6.4.1, 6.4.2

#### 3.2 Inhaltsbezogene mathematische Standards der Lernumgebung<sup>6</sup>

Themenbereich	Standards	Niveau
<b>Gleichungen und Funktionen</b>	Die Schülerinnen und Schüler können <ul style="list-style-type: none"> <li>Zuordnungen und Muster verschieden darstellen<sup>7</sup></li> <li>Bildungsregeln für Zuordnungen und Muster beschreiben</li> </ul>	C
<b>Daten und Zufall</b>	Die Schülerinnen und Schüler können <ul style="list-style-type: none"> <li>Daten sammeln und strukturieren</li> <li>Daten darstellen</li> <li>Kennwerte von Datenerhebungen bestimmen</li> </ul>	D

#### 3.3 Themen und Inhalte der Lernumgebung<sup>8</sup>

Themenbereich	Inhalte	Niveau
<b>Gleichungen und Funktionen</b>	Die Schülerinnen und Schüler <ul style="list-style-type: none"> <li>analysieren und beschreiben die Bildungsregeln von arithmetischen und geometrischen Mustern</li> <li>stellen Zuordnungen dar</li> </ul>	C D
<b>Daten und Zufall</b>	Die Schülerinnen und Schüler <ul style="list-style-type: none"> <li>erfassen und strukturieren selbst erhobene Messwerte</li> <li>stellen Messwerte in Tabellen und Diagrammen dar</li> </ul>	D

<sup>5</sup> vgl. Rahmenlehrplan Jahrgangsstufen 1-10, Teil C Mathematik, S. 19-21, Berlin, Potsdam 2015

<sup>6</sup> vgl. Rahmenlehrplan Jahrgangsstufen 1-10, Teil C Mathematik, S. 22-31, Berlin, Potsdam 2015

<sup>7</sup> Die inhaltsbezogenen mathematischen Standards sind unverändert aus dem Rahmenlehrplan übernommen worden. Kompetenzen, die mit dieser Lernumgebung nicht gefördert werden, sind grau gedruckt.

<sup>8</sup> vgl. Rahmenlehrplan Jahrgangsstufen 1-10, Teil C Mathematik, S. 31ff, Berlin, Potsdam 2015

3.4 Bezüge zum Basiscurriculum Sprachbildung<sup>9</sup>

<b>Standards des BC Sprachbildung</b>	Die Schülerinnen und Schüler können
<b>Rezeption/ Leseverständnis</b>	<ul style="list-style-type: none"> <li>aus Texten gezielt Informationen ermitteln (z. B. Fakten, Ereignisse, Themen)</li> </ul>
<b>Produktion/ Sprechen</b>	<ul style="list-style-type: none"> <li>Sachverhalte und Abläufe beschreiben</li> <li>Vermutungen äußern und begründen</li> <li>Arbeitsergebnisse aus Einzel-, Partner- und Gruppenarbeit präsentieren</li> </ul>

3.5 Bezüge zum Basiscurriculum Medienbildung<sup>10</sup>

<b>Standards des BC Medienbildung</b>	Die Schülerinnen und Schüler können
<b>Kommunizieren</b>	<ul style="list-style-type: none"> <li>ausgewählte Aspekte des Urheber- und Persönlichkeitsrechts sowie des Datenschutzes bei der medialen Kommunikation beschreiben und beachten</li> </ul>
<b>Präsentieren</b>	<ul style="list-style-type: none"> <li>eine Präsentation von Lern- und Arbeitsergebnissen sach- und situationsgerecht gestalten</li> <li>Einzel- und Gruppenarbeitsergebnisse vor einem Publikum präsentieren</li> </ul>

3.6 Bezüge zu übergreifenden Themen<sup>11</sup>

<ul style="list-style-type: none"> <li>Verbraucherbildung</li> </ul>
--

3.7 Bezüge zu anderen Fächern

<ul style="list-style-type: none"> <li>Deutsch</li> </ul>
---

<sup>9</sup> vgl. Rahmenlehrplan Jahrgangsstufen 1-10, Teil B Fachübergreifende Kompetenzentwicklung, S. 6-10, Berlin, Potsdam 2015

<sup>10</sup> vgl. Rahmenlehrplan Jahrgangsstufen 1-10, Teil B Fachübergreifende Kompetenzentwicklung, S. 15-22, Berlin, Potsdam 2015

<sup>11</sup> vgl. Rahmenlehrplan Jahrgangsstufen 1-10, Teil B Fachübergreifende Kompetenzentwicklung, S. 24ff, Berlin, Potsdam 2015

## 4 Sprachbildung

### 4.1 Sprachliche Stolpersteine in den Aufgabenstellungen

Aufgabe	Originaltext	Sprachliche Alternativen
1	Eine einfache Verschlüsselung ist der nach dem römischen Kaiser benannte Cäsar-Code.	Eine einfache Verschlüsselung ist der Cäsar-Code.
<p><i>Es muss sichergestellt werden, dass die Lernenden folgende Begriffe/Wörter verstehen:</i>                  Ägypter, Nachricht, römischer Kaiser, Cäsar-Code, Buchstabe, Cäsar-Scheibe, Diplomat, Empfänger, Cäsar-Verschlüsselung, Experte, Code knacken, Computerprogramm, verschlüsselt wurde mit dem Code, die folgende Nachricht</p>		

### 4.2 Wortliste zum Textverständnis

Die Lehrkraft muss sich vergewissern, dass die Schülerinnen und Schüler folgenden Fachwortschatz verstanden haben, bevor sie die Lernumgebung bearbeiten.

Nomen	Verben	Sonstige
die Verschlüsselungsregel/ der Schlüssel das Schlüsselwort der Code die Häufigkeit die Methode	verschlüsseln entschlüsseln codieren	häufigste

### 4.3 Fachbezogener Sprachschatz und themenspezifische Redemittel

Im Rahmen dieser Lernumgebung wenden die Schülerinnen und Schüler folgende Sprachmittel aktiv an. Diese dienen als Grundlage für die gemeinsame Erarbeitung eines Sprachspeichers während der Ergebnissicherung.

Die Verschlüsselungsregel / der Schlüssel / der Code ist...

Beim Entschlüsseln wird aus dem ... ein ...

Die Nachricht ist ...

der Klartext /der Geheimtext

Dem A ist das ... zugeordnet

Ich vermute, dass...

Der häufigste Buchstabe ist ...

Die Buchstaben ... kommen besonders häufig vor.

Meine Vermutung war richtig / hat sich bestätigt / war falsch / hat sich nicht bestätigt.

4.4 Sprachliche Hilfen (*entfällt*)

**5 Material für den Einsatz dieser Lernumgebung**

Phase / Aufgabe	Anzahl	Name des Materials	Vorbereitung / Hinweise
gesamte Lernumgebung	pro Kind	Lernumgebung ( <a href="#">LU</a> )	kopieren
	einmal	Wortkarten zum Aufbau des Sprachspeichers ( <a href="#">M8</a> )	kopieren, ggf. vergrößern
Einführung	pro Paar	verschlüsselte Nachricht für den Einstieg ( <a href="#">M1</a> )	kopieren, schneiden
Aufgabe 1	nach Bedarf	Verschlüsselungstabelle ( <a href="#">M2</a> )	einzusetzen nur bei Bedarf, liegt in differenzierter Form vor
Aufgabe 2	pro Kind	Cäsar-Scheibe ( <a href="#">M3</a> ), eine Musterklammer, eine Büroklammer <i>oder alternativ</i> Codierungsstreifen ( <a href="#">M7</a> ), eine Büroklammer	auf Karton kopieren
Aufgabe 3	nach Bedarf	Verschlüsselungstabelle ( <a href="#">M2</a> )	kopieren
Aufgabe 4	nach Bedarf	Tippkarten ( <a href="#">M5</a> )	kopieren
		Zusatzaufgabe und Links zu Kinder-Internetseiten zum Thema (inklusive QR-Codes) ( <a href="#">M6</a> )	kopieren
Aufgabe 5	pro Paar	Tabelle für die Vigenère-Verschlüsselung ( <a href="#">M4</a> )	<i>oder alternativ</i> Möglichkeit zur Nutzung des Excel-Programms
	nach Bedarf	Tippkarten ( <a href="#">M5</a> ),	kopieren

**6 Evaluation** (siehe Handreichung, Punkt 6)

**Nachricht an die Schülerinnen und Schüler für den Einstieg:**

**Originalnachricht:**

LIEBE SCHUELERINNEN UND SCHUELER DER KLASSE **5A!**  
HEUTE WERDET IHR LERNEN; WIE MAN NACHRICHTEN VERSCHLUESSELN KANN.  
VIEL SPASS DABEI.

**Verschlüsselt wurde mit dem Cäsar-Code  $A \rightarrow D^{12}$ . Bitte passen Sie den Klassennamen an.**

OLHEH VFKXHOHULQQHQ XQG VFKXHOHU GHU NODVVH **5D!**

KHXWH ZHUGHW LKU OHUQH; ZLH PDQ QDFKULFKWHQ YHUVF

KOXHVVHOQ NDQQ. YLHO VSDVV GDEHL

**Verschlüsselung durch eine zusätzliche Silbe: Bitte passen Sie den Klassennamen an.**

LIETABETA SCHÜTALETARINTANENTA UNDTA SCHÜTALERTA DERTA KLASTASETA **5ATA!**

HEUTATETA WERTADETTA IHRTA LERTANENTA, WIETA MANTA NACHTARICHTATENTA

VERTASCHLÜSTASELNTA KANNTA. VIELTA SPASSTA DATABEITA

**Verschlüsselung in Wort-Rückwärts-Methode: Bitte passen Sie den Klassennamen an.**

EBEIL NENNIRELEUHCS DNU RELEUHCS RED ESSALK **A5!**

ETUEH TEDREW RHI NENREL, EIW NAM NETHCIRHCAN NLESSEULHCSREV NNAK.  
LEIV SSAPS IEBAD.

<sup>12</sup> Beim Entschlüsseln wird aus dem D ein A, aus dem E ein B usw.

Verschlüsselung mit Schriftart Wingdings: Bitte passen Sie den Klassennamen an.

☹️👉👈👉👈    💧👉👈⊕👉☹️👈⚙️👉☠️☠️👉☠️    ⊕☠️👉    💧👉👈⊕👉☹️👈⚙️

E	👉
N	☠️
S	💧
L	☹️

👉👈⚙️    😊☹️👉💧💧👈    5👉!

👉👈⊕⚙️👈    ⊕👈⚙️👉👈⚙️    🖐️👉⚙️    ☹️👈⚙️☠️👈☠️📄    ⊕🖐️👈    💣👉☠️

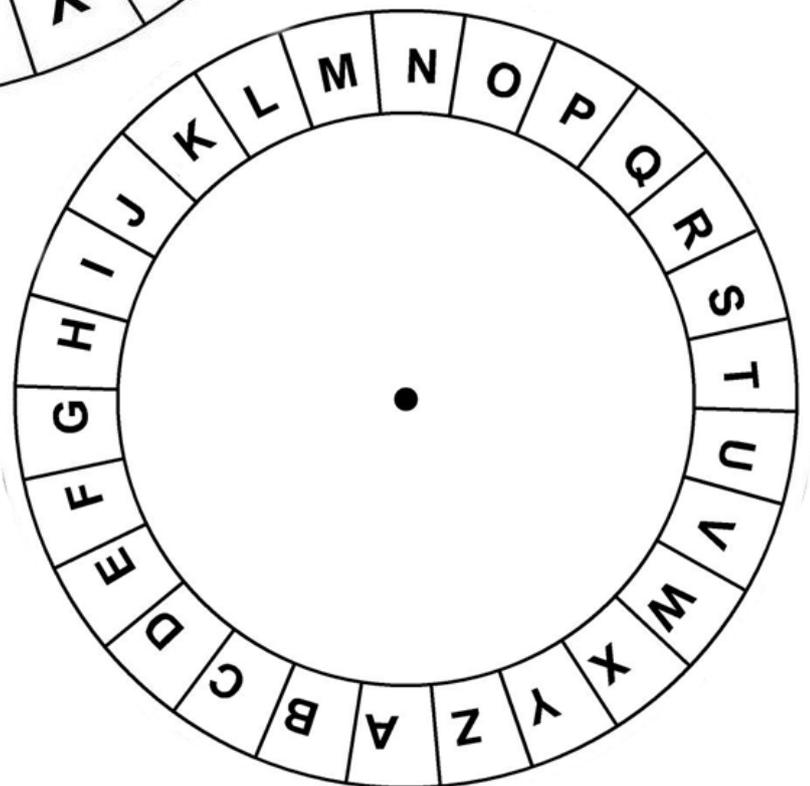
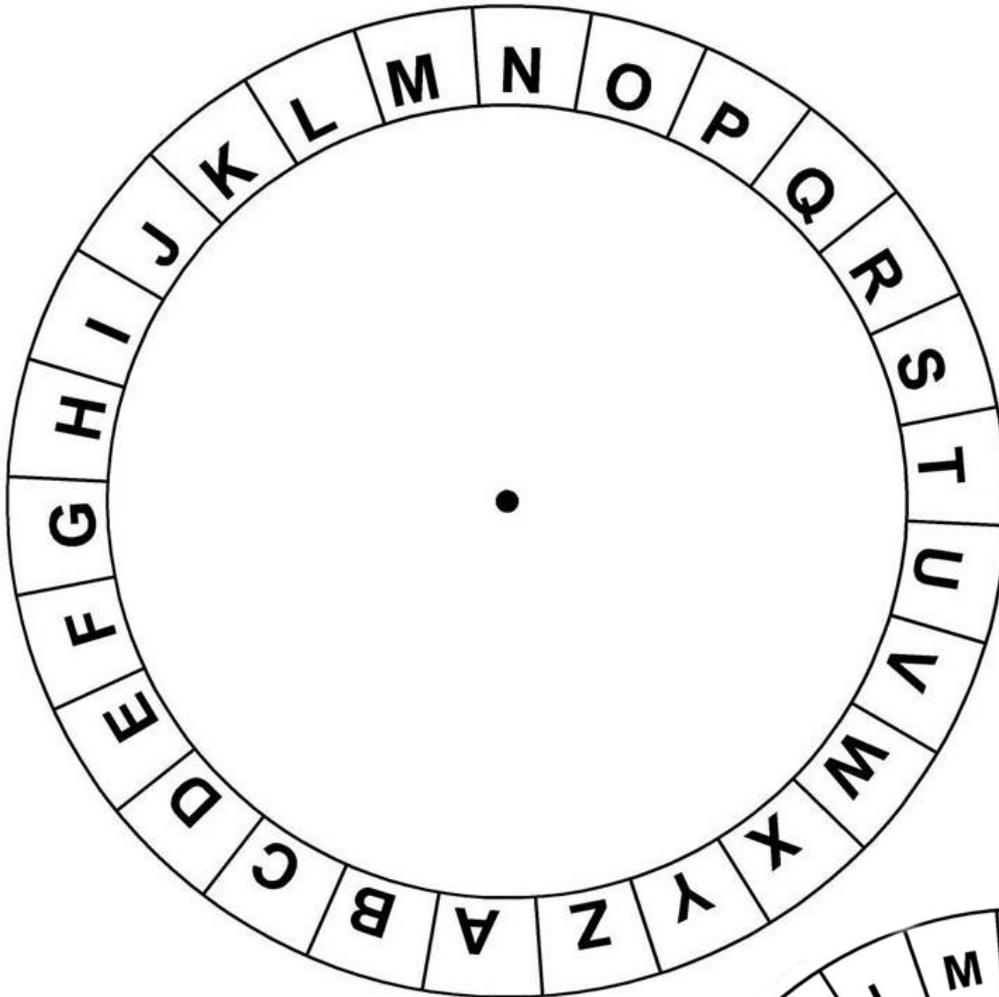
☠️👉👈👉⚙️🖐️👉👈⚙️👈☠️    ⊕👈⚙️💧👉☹️⊕👈💧👈☹️☠️    😊👉☠️☠️📄

⊕🖐️👈☹️    💧👉👈💧💧    🖐️👉👈👈🖐️



**Cäsar-Scheibe:**

Bitte auf Karton kopieren. Beide Scheiben mit einer Musterklammer verbinden.



Schreibe dein Schlüsselwort hier senkrecht ein!

Vigenère-Code

Wählt euer Schlüsselwort und erstellt eure eigene Code-Tabelle.

Codewort: \_\_\_\_\_

	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																										
2																										
3																										
4																										
5																										
6																										
7																										
8																										
9																										
10																										

	1	2	3																							
Originaltext																										
Verschlüsselter Text																										

Material zur Differenzierung

Tipp zu Aufgabe 4:



- Fertigt eine Häufigkeitstabelle an.

A	I
B	I
C	
D	III

Link zum Cäsar-Verschlüsselungsprogramm

<https://gc.de/gc/caesar/>



Aufgabe 5 Tipp 1:



Betrachtet die Zeilen der Verschlüsselungstabelle. Beginnt mit der zweiten Zeile. Was fällt euch auf?

	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	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
2	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
3	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
4	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
5	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

Aufgabe 5 Tipp 2:



Die farbig markierten Felder zeigen euch, wie die ersten fünf Buchstaben verschlüsselt wurden.

	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	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
2	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
3	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
4	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
5	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

1	2	3	4	5	1	2		3	4	5	1	2	3	4	5	1
G	E	H	E	I	M	E		N	A	C	H	R	I	C	H	T
S	E	A	L	M	Y	E		G	H	G	T	R	B	J	L	F

zu 4.

**Zusätzliche Entschlüsselungsaufgabe mit unbekanntem Code:**

BCNUUN MRA EXA, MD VDNBBCNBC NRWN PJWI FRLQCRPN

WJLQARLQC ENABLQUDNBBNUW.

FDNAMNBC MD MJID MNW LJNBJALXMN KNWDCINW?

KNPADNWMN MNRWN VNRWDWP.

**Interessante Kinder-Internetseiten<sup>13</sup> zum Thema: Geheime Botschaften**

<p><a href="https://t1p.de/vhl5">https://t1p.de/vhl5</a></p> 	<p><a href="https://t1p.de/u4sb">https://t1p.de/u4sb</a></p> 
<p><a href="https://t1p.de/wql7">https://t1p.de/wql7</a></p> 	<p><a href="https://t1p.de/oxfs">https://t1p.de/oxfs</a></p> 

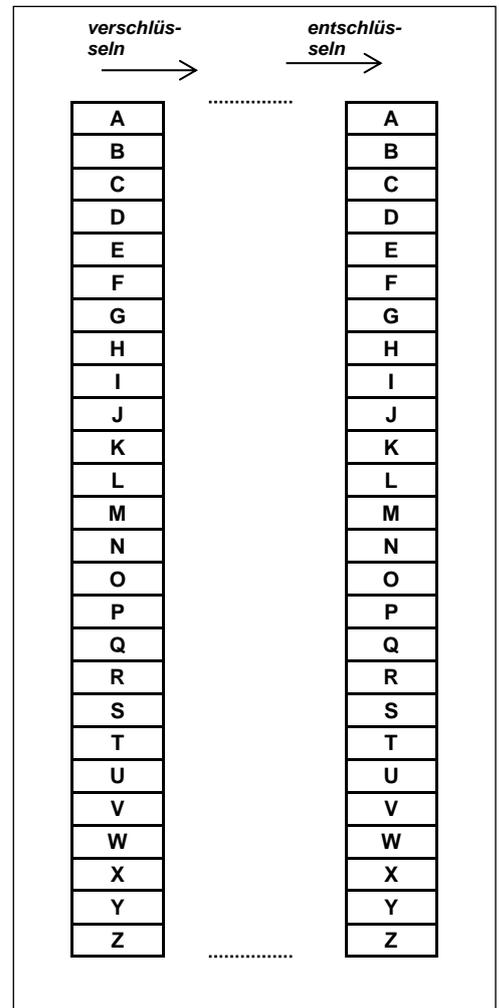
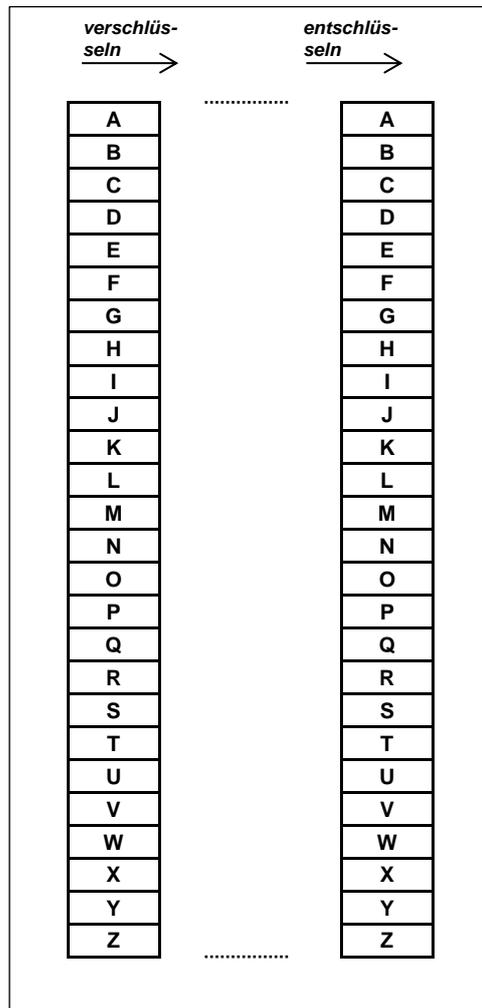
<sup>13</sup> Sie verlassen mit diesem Link die sicheren Seiten des Bildungsservers.

# C Material: Verschlüsselungen (TK Gleichungen und Funktionen – LU 7/M7)

Verschlüsselungstreifen:

Material für zwei Streifen: Auf Karton kopieren oder laminieren und eventuell vergrößern. Dann Streifen und Karten einzeln ausschneiden und an der gepunkteten Linie einschneiden. Buchstabenstreifen durchziehen.

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



Wortkarten für den Aufbau des Sprachspeichers

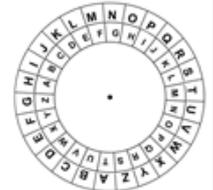
der **Code**

E  $\leftrightarrow$  

A  $\leftrightarrow$  D

der **Cäsar-Code**

die **Cäsar-Scheibe**



Dem **A** ist das ... zugeordnet

Das **A** wird zum ...

verschlüsseln

entschlüsseln

die Vermutung

ich vermute

die Häufigkeit

der **Klartext**

der **Geheimtext**

zu 1.

PRIMA, DU HAST DIE NACHRICHT RICHTIG ENTSCHLUESSELT.

zu 4.

Häufigkeitstabelle

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	1		3	3	3	1			1			2	1	2	2	9		2	2	5	1	1	1	1	1

Es handelt sich hier um eine Verschiebung um + 12 (A → M)

KLASSE. DU BIST JA EIN RICHTIGER GEHEIMCODE-EXPERTE.

**Zusätzliche Aufgabe:**

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
7	9	7	9	2	2			3	5	2	6	9	23		4	4	7			4	2	11	2		

Es handelt sich hier um eine Verschiebung um + 9 (A → J)

STELLE DIR VOR, DU MUESSTEST EINE GANZ WICHTIGE NACHRICHT VER-  
 SCHLUESSELN. WUERDEST DU DAZU DEN CAESARCODE BENUTZEN?  
 BEGRUENDE DEINE MEINUNG.

**Quellen:**

<https://qc.de/qc/caesar/> [11.03.2021] <sup>14</sup>

[https://www.stopkidsmagazin.de/GEHEIM\\_SCHRIFT/geheim\\_schrift.html](https://www.stopkidsmagazin.de/GEHEIM_SCHRIFT/geheim_schrift.html) [11.03.2020] <sup>15</sup>

Senatsverwaltung für Bildung, Jugend und Wissenschaft Berlin / Ministerium für Bildung, Jugend und Sport des Landes Brandenburg (Hrsg.): Rahmenlehrplan Jahrgangsstufen 1-10, Teil B. Berlin, Potsdam 2015

Senatsverwaltung für Bildung, Jugend und Wissenschaft Berlin / Ministerium für Bildung, Jugend und Sport des Landes Brandenburg (Hrsg.): Rahmenlehrplan Jahrgangsstufen 1-10, Teil C Mathematik, Berlin, Potsdam 2015

Sundermann, Beate; Selter, Christoph: HFIFJN! Botschaften verschlüsseln wie Julius Caesar. In: Grundschulzeitschrift (2003) 163, S. 41-43

**Weitere Literatur**

Steinweg, Anna Susanne (2013): Algebra in der Grundschule. Berlin, Heidelberg: Springer

Baumanns, Lukas; Dick, Janine; Rott, Benjamin: Verschlüsselung, Fehlerbeseitigung & Kompression. In Mathematik lehren (2020) 219, S. 2-7

Beutelspacher, Albrecht: Unverständlich, sinnlos, zufällig? In Mathematik lehren (2020) 219, S. 8-10

Brauner, Uli: Kryptoanalyse. In Mathematik lehren (2020) 219, S. 16-19

Heckmann, Lars: Verschlüsselte Botschaften. Codierung von Texten als Einstieg in das Thema Zuordnungen. In Mathematik (2015) 30, S. 6-7

Kaufmann, Sabine: WFSTDIMVFTTFMVOHFO. Verschlüsselungen - so aktuell wie eh und je. In Mathematik differenziert (2017) 4, S. 16-19

Müller, Dorothea, Humbert, Ludger: Informatik ohne Computer. In: Grundschulunterricht (2018) 1, S. 22-24

<sup>14</sup> Sie verlassen mit diesem Link die sicheren Seiten des Bildungsservers.

<sup>15</sup> Sie verlassen mit diesem Link die sicheren Seiten des Bildungsservers.

**Bildnachweise/Abbildungen:**

Seite	Titel	Bildquelle (Titel/Urheber/Lizenz/Link zur Lizenz/Urprungsort)
1, 2, 18	Cäsarscheibe	Cäsarscheibe, Michael Jung, <a href="#">CC BY SA 4.0</a> , LU Verschlüsselungen
4	Foto „Cäsarscheibe“	Foto „Cäsarscheibe“, Solveg Schlinske, <a href="#">CC BY SA 4.0</a> , LU Verschlüsselungen
4	Foto „Verschlüsselungsstreifen“	Foto „Verschlüsselungsstreifen“, Solveg Schlinske, <a href="#">CC BY SA 4.0</a> , LU Verschlüsselungen
13	Bastelvorlage Cäsarscheibe	Bastelvorlage Cäsarscheibe, Michael Jung, <a href="#">CC BY SA 4.0</a> , LU Verschlüsselungen
2	Symbole Einzel-, Partner- und Gruppenarbeit	Symbole Einzel-, Partner- und Gruppenarbeit, Solveg Schlinske, <a href="#">CC BY SA 4.0</a> , LU Sehenswürdigkeiten
15	Glühlampe	Glühlampe, Laura Jahn, <a href="#">CC BY SA 4.0</a> , LU Kernaufgaben