WWU
MÜNSTER

Stand: 2. Februar 2021

Verschlüsseln und Entschlüsseln – Wie geheim sind Geheimbotschaften?

Ein Unterrichtsbaustein zur Förderung informatischer Bildung im Sachunterricht der Jahrgangsstufen 3–4

Arbeitsbereich Didaktik der Informatik der WWU Münster
Autor: Alexander Best

wissen.leben

DDI Arbeitsbereich Didaktik der Informatik

Urheberrechtserklärung

Dieser Unterrichtsbaustein ist eine Weiterentwicklung des in Kooperation mit Grundschullehrpersonen entwickelten, gleichnamigen Bausteins, der im Rahmen des Dissertationsprojekts von Alexander Best entwickelt wurde. Die Erstveröffentlichung kann unter der nachfolgenden Arbeit eingesehen werden:

Alexander Best (2020): Vorstellungen von Grundschullehrpersonen zur Informatik und zum Informatikunterricht. Dissertation, Westfälische Wilhelms-Universität Münster, S. 470–496. Online verfügbar unter https://ddi.wwu.de/2020_best_diss, zuletzt geprüft am 02.02.21.

Open Access

Zitieren dieses Werkes

Arbeitsbereich Didaktik der Informatik (2021): Verschlüsseln und Entschlüsseln – Wie geheim sind Geheimbotschaften? Unterrichtsbaustein, Westfälische Wilhelms-Universität Münster

Didaktisch-methodische Handreichung

Hinweis: Sämtliche Materialien stehen für eine maximale Klassenstärke von 30 Schülerinnen und Schülern am Arbeitsbereich Didaktik der Informatik der Westfälischen Wilhelms-Universität Münster (WWU) zur Verfügung und werden kostenlos an interessierte Grundschulen verliehen. Falls Sie dieses Angebot wahrnehmen möchten oder Fragen haben, erreichen Sie uns unter *grundschulinformatik@uni-muenster.de* oder alternativ über unser Sekretariat (Frau Andrea Lieske) unter +49 251 83-39397 (Tel.) bzw. +49 251 83-39369 (Fax). Sie finden unseren Arbeitsbereich am Institut für Didaktik der Mathematik und der Informatik, Corrensstr. 80, 48149 Münster.

Wir wünschen Ihnen viel Spaß und Erfolg bei der Durchführung.

Kernanliegen: Die Schülerinnen und Schüler erarbeiten sich das Prinzip der symmetrischen und asymmetrischen Verschlüsselung exemplarisch anhand der Caesar-Scheibe[1] (symmetrisch), der Skytalen (symmetrisch) und des Schlüssel-Schloss-Prinzips (asymmetrisch), stellen deren Ähnlichkeiten und Unterschiede heraus und nehmen begründet dazu Stellung, welches Verfahren sie persönlich einsetzen würden.

Paradigma: *Plugged* [ ] *Unplugged* [X]

Informatische Vorkenntnisse: Keine

Fachübergreifende Vorkenntnisse/Fähigkeiten: (a) Kooperatives Problemlösen, (b) Erfahrungen mit Rollenspielen, (c) psychomotorische Fähigkeiten zum Zusammenbau der Caesar-Scheibe und zur kooperativen Verwendung der Skytalen, (d) eigene Handlungen beschreiben, (e) eigene Entscheidungen begründen, (f) Lesekompetenz zum Vorlesen der Comics und der Aufgabenstellungen auf den Arbeitsblättern sowie (g) Unterscheidung zwischen Absender und Empfänger

Jahrgangsstufe: 3–4

Dauer: 120–135 min

[1] Die Begriffe „symmetrische Verschlüsselung“ und „asymmetrische Verschlüsselung“ sowie die konkreten Verfahren (Caesar, Skytalen, Schlüssel-Schloss-Prinzip) werden im didaktischen Kommentar erläutert.

Thema: Erarbeitung der Funktionsweise, Unterschiede und Schwachstellen symmetrischer und asymmetrischer Verschlüsselung am Beispiel der Caesar-Scheibe (symmetrisch), der Skytale (symmetrisch) und des Schlüssel-Schloss-Prinzips (asymmetrisch) sowie begründete Bewertung der drei Verfahren durch die Schülerinnen und Schüler

Themengebiet: Kryptologie

Inhalt: Symmetrische und asymmetrische Verschlüsselungsverfahren

Gegenstände: Caesar-Scheibe, Skytalen und Schlüssel-Schloss-Prinzip

Benötigte Materialien:

(1) Einstiegscomic „Caesar und sein General Strategus“
(2) Einstiegsfolie „Von Absender zum Empfänger“
(3) Caesar-Scheibe als Folie zur Demonstration/Präsentation am OHP
(4) Arbeitsblatt „Verschlüsseln und Entschlüsseln mit der Caesar-Scheibe“ (ein AB pro SuS)
(5) Schere zum Ausschneiden der inneren und äußeren Chiffrierscheibe (eine Schere pro SuS)
(6) Arbeitsblatt „Verschlüsseln und Entschlüsseln mit den Skytalen“ (ein AB pro Partnergruppe)
(7) Rote, blaue und grüne Skytalen (1 Set pro Partnergruppe)
(8) Rollenkarten für das Rollenspiel (jeweils für den Absender, den Dieb, den Empfänger)
(9) Schnüre zum Umhängen der Rollenkarten (drei Schnüre mit einer Länge von ca. 0,5 m)
(10) Kiste, Schloss, Schlüssel (ein Set pro Partnergruppe)
(11) Arbeitsblatt „Verschlüsseln und Entschlüsseln mit Schlüssel, Schloss und Kiste (leichte Variante)“ (ein AB pro SuS)
(12) Arbeitsblatt „Verschlüsseln und Entschlüsseln mit Schlüssel, Schloss und Kiste (anspruchsvolle Variante)“ (ein AB pro SuS)

Benötigte Medien: Tafel und OHP

Geförderte Kompetenzen – Informatik[2]

Inhaltsbereiche: INFORMATIK, MENSCH UND GESELLSCHAFT sowie INFORMATION UND DATEN

Prozessbereiche: BEGRÜNDEN UND BEWERTEN

Kompetenzerwartungen:

„Die Schülerinnen und Schüler

- nutzen und entwickeln Vereinbarungen, um Daten zu verschlüsseln und zu entschlüsseln
- nutzen und entwickeln Vereinbarungen zur Übermittlung von Nachrichten
- ergreifen Maßnahmen, um Daten vor ungewolltem Zugriff zu schützen“ (Gesellschaft für Informatik (GI) 2019, 13; 16)

[2] Angelehnt an die Kompetenzen für informatische Bildung der Gesellschaft für Informatik (GI) 2019.

Geförderte Kompetenzen – Sachunterricht[3]

Perspektive: SOZIALWISSENSCHAFTLICHE PERSPEKTIVE

Perspektivbezogene Denk-, Arbeits- und Handlungsweisen: GESELLSCHAFTSBEZOGENE HANDLUNGEN PLANEN UND UMSETZEN

Kompetenzerwartungen:

„Die Schülerinnen und Schüler können:

- Regeln zur Zusammenarbeit und zur Verteilung aufstellen und begründen
- Handlungspläne in reale Handlungen umsetzen (z.B. bei Aktionen gegen Kinderarbeit, für nachhaltigen Konsum)
- Handlungen in Rollen- und Planspielen sowie Zukunftswerkstätten simulieren**“** (Gesellschaft für Didaktik des Sachunterrichts (GDSU) 2013, S. 33)

---

[3] Angelehnt an den Perspektivrahmen Sachunterricht der Gesellschaft für Didaktik des Sachunterrichts (GDSU) 2013.

Didaktischer Schwerpunkt

Relevanz für die Schülerinnen und Schüler: Die Schülerinnen und Schüler werden spätestens in der Sekundarstufe I Umgang mit Smartphones, PCs, Spielekonsolen und/oder anderen Informatiksystemen haben. Der alltägliche Gebrauch dieser Systeme findet i. d. R. unreflektiert statt. Den Schülerinnen und Schülern werden dabei die Begriffe *Verschlüsselung* und *Entschlüsselung* im Rahmen von Kommunikation, Datenspeicherung, Benutzerkonten oder ähnlichem begegnen. Hierfür bereitet die Unterrichtseinheit die Schülerinnen und Schüler sowohl im kognitiven wie im affektiven Bereich auf diese Situation vor. Durch die Auseinandersetzung mit drei unterschiedlichen kryptografischen Verfahren lernen sie die Grundprinzipien der Ver- und Entschlüsselung kennen. Darüber hinaus werden sie in Punkto Datenschutz sensibilisiert. Sie sollen erkennen, dass jede Verschlüsselung durch ihre Funktionsweise definiert wird und es unsichere und sichere Verschlüsselungsverfahren gibt. Die erworbenen Kompetenzen werden den Schülerinnen und Schülern so ein kritisches und fachliches Bewusstsein im Umgang mit Daten ermöglichen.

Relevanz für die Grundschule und den Sachunterricht: Die Schülerinnen und Schüler nehmen Informatiksysteme zunächst als Medien wahr. Diese Vorstellung behalten sie dann i. d. R. in ihrer gesamten Schullaufbahn bei. Sie wollen die Anwendung dieser Systeme beherrschen, haben aber kaum Kenntnisse über deren Funktionsweisen und die zugrundeliegenden Prinzipien sowie Strukturen. Dies ist besonders im Kontext der digitalen Kommunikation problematisch, da hier das unreflektierte Verwenden von sozialen Netzwerken, Instant Messaging- oder Chat-Programmen etc. schwerwiegende Folgen haben kann. Während die Schülerinnen und Schüler bereits sehr früh darüber aufgeklärt werden, dass persönliche Daten nicht an fremde Personen weitergegeben werden sollen, fehlt häufig eine sachgerechte Aufklärung in Bezug auf digitale Kommunikation. Dies kann zu unbedachtem Umgang mit den eigenen Daten in digitalen Umgebungen führen. Dieses Verhalten ist nicht nur auf Grundschulkinder beschränkt, sondern ebenso ein Problem, das in anderen Altersgruppen vorzufinden ist. Zur Sensibilisierung der Schülerinnen und Schüler gibt es zwei Vorgehensweisen: Entweder sie werden durch *Worst-Case*-Szenarien abgeschreckt oder sie werden über die Funktionsweise einiger Aspekte der digitalen Kommunikation aufgeklärt. Letzteres soll in diesem Unterrichtsbaustein erfolgen.

Didaktischer Kommentar: Die Schülerinnen und Schüler setzen sich in diesem Baustein mit der Verschlüsselung sowie Entschlüsselung von Botschaften bzw. Geheimbotschaften auseinander. In der Informatik wird dabei zwischen zwei grundlegenden Ansätzen unterschieden: Der symmetrischen und der asymmetrischen Verschlüsselung. Bei symmetrischen Verfahren wird eine Botschaft (z.B. ein Text) mit einem sogenannten Schlüssel verschlüsselt. Ein Schlüssel ist dabei typischerweise eine bestimmte Information, die benötigt wird, um anhand einer klaren Ablaufbeschreibung, man spricht von Algorithmus, eine unverschlüsselte Botschaft in eine Geheimbotschaft zu transformieren. Um diese Geheimbotschaft wieder zu entschlüsseln, wird bei symmetrischen Verfahren exakt derselbe Schlüssel benötigt. Solche Verfahren sind bereits seit der Antike bekannt. Die sogenannte Caesar-Chiffre arbeitet dabei mit einer simplen Ersetzungsstrategie (Substitution) von

Buchstaben zur Erzeugung eines „Geheimalphabets“. Der Schlüssel repräsentiert in diesem Verfahren die Information, um wie viele Stellen das Alphabet verschoben bzw. rotiert werden muss. Das Caesar-Verfahren kann dabei besonders gut mittels der Albertischeibe[4] (siehe) veranschaulicht werden, da das Verschieben der Buchstaben mit dem Drehen der Scheibe gleichgesetzt werden kann. So wird eine physische Handlung (enaktiv) mit einer kognitiven Operation verknüpft.

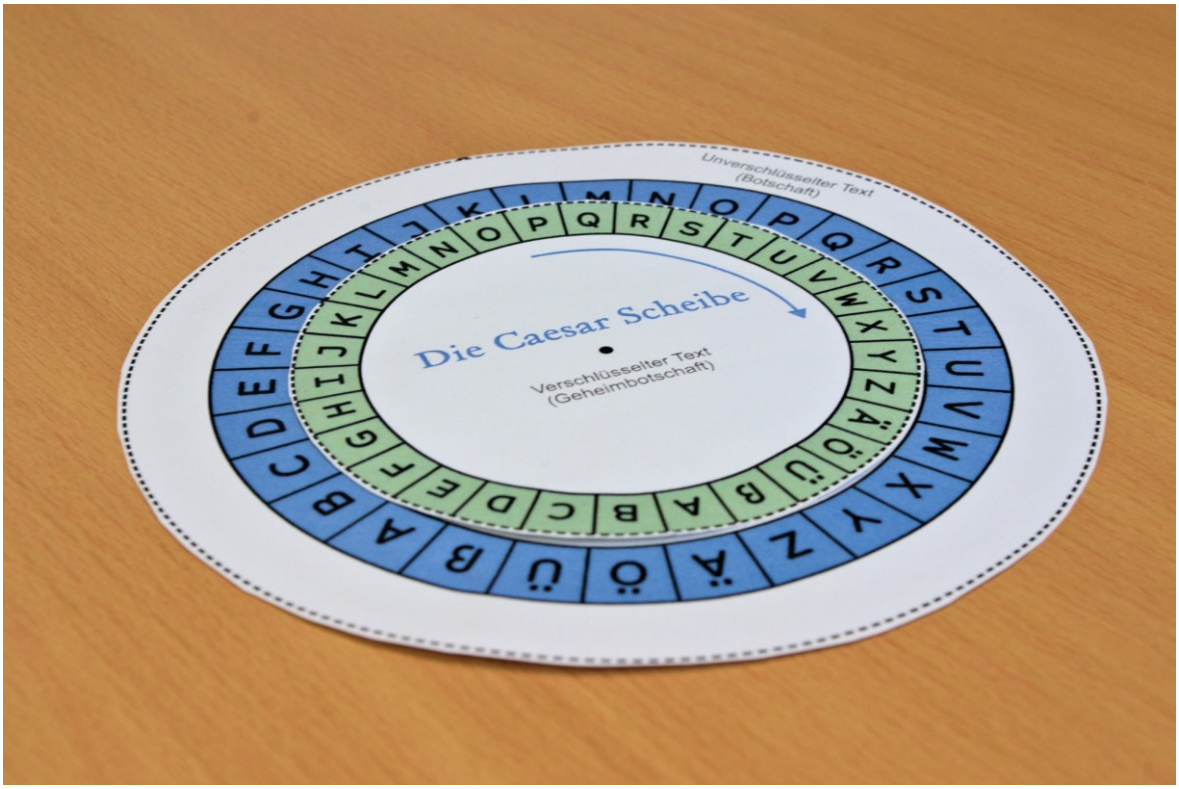


Abbildung 1: Caesar-Scheibe mit dreißig Buchstaben und einer Rotation um 26 Stellen

Anschließend wird ein weiteres Verfahren eingeführt: Das Verschlüsseln mit der Skytale (aus dem Griechischen σκυτάλη[5]: Stock oder Stab). Bei diesem Verfahren wird ein Papierstreifen um einen Stab (die Skytale) gewickelt. Anschließend kann ein Text horizontal in mehreren Zeilen entlang der Skytale geschrieben werden (siehe). Es handelt sich hierbei ebenfalls um ein in der Antike entwickeltes symmetrisches Verfahren. Während bei dem Caesar-Verfahren hingegen der Schlüssel durch die Information dargestellt wird, um wie viele Stellen das Alphabet verschoben werden muss, wird bei der Skytale der Schlüssel durch den Durchmesser des Stabes repräsentiert. Bei diesem Verfahren findet also keine Ersetzung von Buchstaben (Substitution), sondern eine Verschiebung/Versetzung (Transposition) statt. Nimmt man den beschriebenen Streifen von der Skytale, so kann der Text nicht ohne weiteres entziffert werden. Der nun verschlüsselte Text kann aber mit einer Skytale desselben Durchmessers leicht wieder entschlüsselt werden. Im Zuge der didaktischen Gestaltung werden die drei verwendeten

[4] Im Rahmen dieses Entwurfs wird sowohl der Begriff „Caesar-Verfahren“ als auch „Caesar-Scheibe“ bzw. „Caesar-Chiffre“ verwendet. Historisch korrekt wäre hier die Bezeichnung „Alberti-Scheibe“. Aus Gründen der didaktischen Gestaltung wird jedoch das zugrundeliegende Verfahren sowie die Verwendung der Chiffrierscheibe Gaius Julius Caesar zugeschrieben.

[5] Siehe „*A Greek-English Lexicon*“ von Liddell und Scott 1940.

Skytalen farblich markiert, sodass die Schülerinnen und Schüler sich nicht mit metrischen Angaben des Durchmessers auseinandersetzen müssen. Zudem erfordert das Umwickeln der Skytalen mit den Streifen ein kooperatives Vorgehen.

Abbildung 2: Drei Skytalen unterschiedlichen Durchmessers mit exemplarischen Geheimbotschaften

Vor dem Übergang zum asymmetrischen Verschlüsselungsverfahren stellen die Schülerinnen und Schüler die Vor- und Nachteile der beiden vorgestellten symmetrischen Verfahren anhand eines Rollenspiels gegenüber. Der grundlegende Nachteil symmetrischer Verfahren besteht darin, dass der Absender dem Empfänger sowohl die Geheimbotschaft als auch den Schlüssel, mit welchem die Botschaft von ihm verschlüsselt wurde, übermitteln muss. Der gleiche Schlüssel wird benötigt, um die Botschaft zu verschlüsseln und die Geheimbotschaft zu entschlüsseln. Wird nun der Schlüssel während der Übertragung abgefangen, so kann der Dieb jede damit verschlüsselte Geheimbotschaft wieder entschlüsseln. Dieses Problem kann im Rahmen des Rollenspiels mittels der Rollen „Absender“, „Dieb“ und „Empfänger“ von den Schülerinnen und Schülern nachvollzogen werden. Bei dem Caesar-Verfahren muss der Absender dem Empfänger bspw. mitteilen, um wie viele Stellen er das Alphabet verschoben hat und auch bei den Skytalen muss der Schlüssel (Stab oder Farbangabe) übermittelt werden, wobei Geheimbotschaften, welche über die beschriebenen Verfahren verschlüsselt wurden, auch ohne Wissen über den genauen Schlüssel durch simples Ausprobieren *(brute force)* vergleichsweise einfach entschlüsselt bzw. „geknackt“ werden können. Die wesentliche Sicherheit dieser beiden Verfahren ist daher nicht durch den eigentlichen Schlüssel gegeben, sondern durch die Tatsache, dass ein Dieb keine Kenntnis des zugrundeliegenden Verfahrens besitzt. Kennt er allerdings die Funktionsweise des Verfahrens, so stellt die eigentliche Verschlüsselung keine sehr große Sicherheit mehr dar.

An dieser Stelle erfolgt die Einführung eines asymmetrischen Verfahrens. Asymmetrische Verfahren beruhen auf dem sogenannten Kerckhoffs’schen Prinzip, welches besagt, dass die Sicherheit eines Verfahrens nicht auf deren Geheimhaltung beruhen sollte. Zur Auseinandersetzung mit dem Schlüssel-Schloss-Prinzip erhalten die Schülerinnen und Schüler

einen Schlüssel, ein Schloss und eine Kiste (siehe). Sie sollen das Prinzip dieses Verfahrens nun selbstständig entdecken können.

Abbildung 3: Repräsentation des öffentlichen und privaten Schlüssels durch ein physisches Schloss sowie den passenden Schlüssel (ABUS® ist eine eingetragene Wortmarke der ABUS August Bremicker Söhne KG)

Dazu müssen sie erkennen, dass der Schlüssel unter allen Umständen beim Empfänger bleiben muss. Der Absender erhält die Kiste und das *geöffnete* Schloss. Er kann nun in die Kiste eine Botschaft legen und diese anschließend, ohne selbst im Besitz des zugehörigen Schlüssels zu sein, mit dem Schloss verschließen. Auf diese Weise kann sichergestellt werden, dass eine dritte Person (hier: Dieb) trotz seiner Kenntnis über das Verfahren nicht in der Lage ist, die Botschaft zu lesen. Ausschließlich der Empfänger mit dem passenden Schlüssel kann die Kiste öffnen. Für jedes Schloss existiert ein Ersatzschlüssel, falls die Schülerinnen und Schüler ihren Schlüssel einschließen sollten. Der Ersatzschlüssel sollte stets bei der Lehrperson bleiben.

Geplanter Verlauf des Unterrichts

Artikulationsschema

Phase (Zeitangaben ggfs. anpassen)	**Unterrichtsinhalte**	**Sozial-/ Arbeitsform**	**Material/Medien**	**Didaktisch-methodischer Kommentar**
(Vorausblickender) Einstieg I (~ 10 min)	Kurzvortrag: SuS lernen heute einen kleinen Ausschnitt des Faches Informatik kennen ⇢ Tafelanschrieb „Informatik“. Lehrer LoL legt die Folie „Caesar und sein General Strategus“ auf den OHP und lässt eine/einen SoS die Folie laut vorlesen. SuS erarbeiten die Aspekte „Botschaft“ und „Geheimbotschaft“ als Möglichkeit, um das Problem zu lösen. Caesars genaues Vorgehen wird anhand einer weiteren Folie skizziert, damit die SuS den Prozess der **Verschlüsselung** (Botschaft ⇢ Geheimbotschaft), der Übermittlung vom Absender zum Empfänger und der **Entschlüsselung**	LV SV UG LV	• Tafel (Anschrieb des Begriffs „Informatik“) • Folien mit dem Comicstrip „Caesar und sein General Strategus“ sowie der anschließenden Erläuterungsfolie	Sämtlich Aufgabenstellungen werden durch eine Schülerin oder einen Schüler laut vorgelesen ⇢ Ansprechen verschiedener Inputkanäle ⇢ SuS mit Leseschwäche werden kognitiv entlastet. **Motivation** der SuS durch das Medium Comic, durch die Verwendung der (bekannten) Figur Caesar sowie einer Problemorientierung (SuS müssen knobeln). **Zieltransparenz:** Aus dem Comicstrip und dem Ausblick (Gelenkstelle) sollten die SuS erkennen, dass das Kernanliegen der Stunde das Verschlüsseln von Botschaften und Entschlüsseln von Geheimbotschaften ist. **Sinntransparenz:** Der Sinn sollte den SuS aus der Geschichte des Comicstrips deutlich werden: Geheimbotschaften machen es möglich, Nachrichten zu verfassen, die nicht von jedem gelesen

	(Geheimbotschaft ⇢ Botschaft) nachvollziehen können (drei grundlegende Schritte) ⇢ Erläutert durch die/den LoL. **Gelenkstelle: „…** und wie Caesar seine Botschaften verschlüsselt hat und wie Strategus die Geheimbotschaften wieder entschlüsseln konnte, das sollt ihr jetzt selbst herausfinden!“			werden können. **Organisationstransparenz:** Die SuS erhalten das Arbeitsblatt eins mit der Caesar-Scheibe. Der Ablauf der Erarbeitungsphase ist aus den Arbeitsaufträgen ersichtlich. Die Fachbegriffe in dieser Stunde sind: **Botschaft**, **Geheimbotschaft**, **Verschlüsseln**, **Entschlüsseln**, **Absender** und **Empfänger** (die letzten beiden Begriffe sind wahrscheinlich bereits bekannt). Es sollte immer auf diese Begriffe zurückgegriffen werden; nicht auf „Verfahren“ o. ä. Idealerweise werden die Begriffe in einem Wortspeicher festgehalten. Beim Einstiegsvortrag sollte ausschließlich der Begriff „Informatik“ verwendet werden. Die SuS sollen keine Assoziation zu den Begriffen PC, Computer, Smartphone etc. herstellen.
Erarbeitung I (~ 20 min)	SuS erhalten je ein Aufgabenblatt (⇢ Die Aufgaben werden von einer Schülerin oder einem Schüler laut vorgelesen). Sobald die Mehrheit der SuS mit der zweiten Aufgabe fertig ist, findet eine kurze	EA	• Aufgabenblatt mit Vordruck der Caesar-Scheibe (Zusammenbau ⇢ Aufgabe eins) und der Geheimbotschaft (Entschlüsselung ⇢ Aufgabe zwei)	Möglichkeit zur zeitlichen Orientierung für die SuS: „Aufräummusik“ oder „Herunterzählen“. Die Scheibe ist so gestaltet, dass die Drehrichtung festgelegt ist und die kleinere Scheibe zur Verschlüsselung dient.

	Zwischensicherung statt (siehe nächste Phase).		• Schere • Folie „Caesar-Scheibe“ • OHP	Die größte Denkleistung in dieser Phase ist für die SuS herauszufinden, welche Bedeutung die hochgestellte Zahl vor der Geheimbotschaft hat. Sie gibt an, um wie viele Stellen die innere Scheibe rotiert werden muss, um die Geheimbotschaft zu entschlüsseln.
Sicherung I (~ 15 min)	OHP: Eine Schülerin oder ein Schüler verdeutlicht kurz die Funktionsweise der Caesar-Scheibe und löst die Geheimbotschaft auf (Aufgabe zwei). Anschließend dürfen die SuS sich 5–10 min eigene Geheimbotschaften schicken. **Gelenkstelle:** Kurzer Lehrervortrag zu den Skytalen, die noch früher als die Caesar-Scheibe entwickelt und eingesetzt wurden.	SuS-Präsentation am OHP PA	s. o.	Verwendung/Wiederholung der Fachbegriffe „Verschlüsseln“ und „Entschlüsseln“ während der SuS-Präsentation.
Erarbeitung II (~ 25 min)	SuS erhalten jeweils zu zweit drei Skytalen unterschiedlicher Dicke (farblich markiert) und ein AB mit vordefinierten Linien zum Ausschneiden (Beispiel-Geheimbotschaften und leere Streifen).	PA	• Drei Skytalen pro Partnergruppe (rot, grün, blau) • Streifen mit Geheimbotschaften (Arbeitsblatt zwei in DIN A3)	Die SuS erhalten zunächst nur das Arbeitsblatt. Die Aufgaben werden von einer Schülerin oder einem Schüler laut vorgelesen. Anschließend dürfen sie sich die Skytalen nehmen. Die Skytalen werden nach Farben

	Sobald die Mehrheit der Partnergruppen mit der Aufgabe eins fertig ist, findet eine Zwischensicherung statt (siehe nächste Phase).		• Schere • Ggfs. Tesafilm zur Fixierung der Streifen auf den Skytalen	kategorisiert, da der Durchmesser den SuS wahrscheinlich noch nicht vertraut ist ⇢ Hier könnte man evtl. zwischen dritter und vierter Klasse differenzieren. In dieser Phase müssen die SuS ihre motorischen Fähigkeiten kooperativ einsetzen. Das Wickeln der Streifen um die Skytale ist in Einzelarbeit sehr schwierig. Zudem müssen die SuS etwas experimentieren, um die richtige Wickeltechnik zu finden.
Sicherung II (~ 15 min)	Eine Schülerin oder ein Schüler erläutert die Funktionsweise der Skytale und wie die entschlüsselten Botschaften lauten („SKYTALE“, „HALLO FREUNDE“, „WIE GEHT ES DIR?“) Es folgt die Bearbeitung von Aufgabe zwei.	SuS-Präsentation PA/GA	s. o.	Aufgabe zwei hat hier, analog zur Arbeit mit der Caesar-Scheibe, einen sichernden und handelnd-motivierenden Charakter, da die SuS das Verfahren nun selbstständig durchführen können (Einübung) und die Lehrperson durch Beobachtung der handelnden SuS auf den Grad des Verständnisses schließen kann. Bei schwächeren Lerngruppen: Nach der Präsentation gibt die Lehrperson den Impuls an das Plenum, dass die SuS auf die leeren Streifen nicht einfach ihre Botschaft schreiben können. Dann könnte sie schließlich jeder lesen. Die leeren Streifen müssen zunächst um die Skytale gewickelt werden und erst dann kann die Geheimbotschaft geschrieben werden.
(Wiederholender)	Hier sollten folgende Punkte	UG	• Caesar-Scheibe	Falls die beiden Stunden aufeinander

Einstieg II (~ 5–10 min)	wiederholt werden: • Funktionsweise der Caesar-Scheibe • Funktionsweise der Skytalen • Wozu brauchte man beides? ⇢ Geheime Botschaften übermitteln • Verschlüsseln: Botschaft ⇢ Geheimbotschaft ⇢ Absenden • Entschlüsseln: Empfangen ⇢ Geheimbotschaft ⇢ Botschaft **Gelenkstelle:** „L: Was ist denn eurer Meinung nach das Wichtigste an einer Geheimbotschaft? ⇢ S: Nur der Empfänger darf sie lesen. ⇢ L: Jetzt wollen wir einmal überprüfen, ob Geheimbotschaften, die mit der Caesar-Scheibe und der Skytale geschrieben wurden, auch wirklich geheim sind. Dafür brauche ich drei Freiwillige: Einen Absender, einen Empfänger und einen Dieb!“		• Skytale	folgen, muss keine Wiederholung stattfinden. Der überleitende Impuls (Gelenkstelle) ist jedoch notwendig.
Problematisierung (~ 10 min)	Es werden zunächst die Rollen Absender, Empfänger und Dieb verteilt (Rollenkarten). Der Dieb	Rollenspiel	• OHP • Folie „Caesar-Scheibe“	Die Rollen werden mit „Absender (Caesar)“, „Empfänger (Strategus)“ und „Dieb“ bezeichnet. So können die SuS die

	muss anschließend den Raum verlassen (alternativ Kopfhörer/Augen verbinden). Der Absender denkt sich nun eine kurze Botschaft aus und um wie viele Stellen er die Caesar-Scheibe verschieben will. Die übrigen SuS dürfen ihm dann die Geheimbotschaft zu seiner Botschaft diktieren. Die Schülerin oder der Schüler schreibt die Geheimbotschaft auf ein Blatt Papier. Nun wird der Dieb hereingebeten. Anschließend soll der Absender die Geheimbotschaft an einen Ort legen (z.B. Pult oder OHP), an dem sie der Empfänger abholt. Vorher nimmt sich der Dieb jedoch die Geheimbotschaft. Frage an die SuS: „Kann der Dieb etwas mit der Nachricht anfangen?“ Lehrperson und SuS stellen fest, dass bei den Skytalen dasselbe Problem existiert: Besitzt ein Dieb die drei Skytalen oder kennt deren Durchmesser, dann ist auch jede Geheimbotschaft zu	 UG	• Blatt Papier für die Geheimbotschaft • Rollenkarten für Absender, Empfänger und Dieb	Figuren Caesar und Strategus wiedererkennen, gleichzeitig werden die Begriffe Absender und Empfänger wieder präsent gemacht. Der Dieb sollte durch die/den LoL oder einen starke/n SuS gespielt werden. Derjenige sollte in der Lage sein die Geheimbotschaft schnell zu entschlüsseln. Zur Erhöhung der Authentizität sollte derjenige auch vor den Klassenraum gehen, damit er/sie beim Verschlüsseln nicht dabei ist. Ziel ist es, dass die SuS erkennen, dass die Nachricht sicher ist, falls der Dieb das Verfahren nicht kennt. Kennt er es aber, so ist die Nachricht nicht sicher.

	knacken! **Zusammenfassung:** „Das ist ja schon ein großer Nachteil. Wenn jemand herausbekommt, wie man eine Nachricht verschlüsselt und entschlüsselt, dann ist keine Nachricht mehr sicher!“ **Gelenkstelle:** „Wir halten einmal fest: Es kann immer passieren, dass ein Dieb kommt und eine Botschaft stiehlt. Wir müssen also einen Weg finden, sodass der Dieb mit der gestohlenen Botschaft nichts anfangen kann, sondern nur der Empfänger, für den die Botschaft bestimmt ist. Diesen Weg sollt ihr jetzt selbst herausfinden!“			
Erarbeitung III (~ 15 min)	SuS erhalten zu zweit ein Schloss mit Schlüssel, eine Kiste, ein Blatt Papier (oder sie benutzen eigene Blätter) für die Botschaft sowie ein Aufgabenblatt.	PA	• Schloss und Schlüssel • Kiste • (Blatt für die Botschaft)	Wichtig ist, dass die SuS sich in dieser Phase zunächst nicht mehr auf die vorherigen Verfahren beziehen. Am besten wird explizit darauf hingewiesen, dass sie bei diesem Verfahren die Caesar-Scheibe und die Skytalen nicht mehr brauchen (Caesar-Scheiben weglegen; Skytalen zurückgeben).
Präsentation/ Sicherung III (~15 min)	Eine Gruppe spielt vor, wie mit Hilfe von Schlüssel, Schloss und Kiste eine	SuS-Präsentation	Arbeitsblatt drei	Sollte keine Gruppe das exakte Ergebnis herausgefunden haben, so kann ein bestehendes Ergebnis durch gezielte

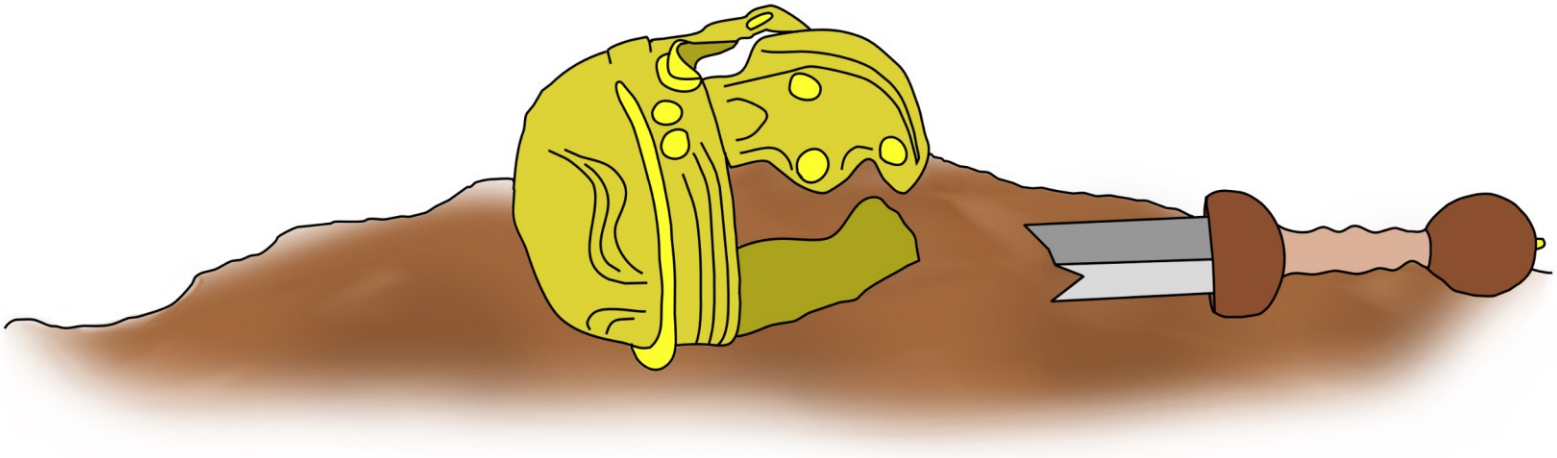
	Botschaft/Geheimbotschaft verschickt werden kann. Anschließend wird das Arbeitsblatt drei bearbeitet und die Ergebnisse besprochen.	EA		Impulse abgewandelt werden. Das Arbeitsblatt drei liegt in einer (a) einfachen und (b) erweiterten Fassung vor.
Reflexion (~5 min)	SuS diskutieren abschließend folgende Frage: „Ihr habt jetzt drei Möglichkeiten kennengelernt, mit denen ihr eine geheime Botschaft verschicken könnt: Die Caesar-Scheibe, die Skytalen und die Kiste mit Schlüssel und Schloss. Welches würdet ihr selbst benutzen, um einer Freundin oder einem Freund eine Geheimbotschaft zu schicken?“	UG	—	In dieser Phase sollen die SuS abschließend die gewonnenen Erkenntnisse reflektieren und die drei Verfahren bewerten. Dabei sollen sie ihre Aussagen begründen.
Optionaler Transfer (~ 5 min)	Hier kann eine Anbindung an kryptografische Prozesse im Alltag der Kinder anhand von Informatiksystemen erfolgen, falls dies gewünscht ist. Dazu zählen bspw. verschlüsselte E-Mail-Kommunikation oder Instant Messaging-Applikationen, welche mit einer Verschlüsselung arbeiten. Grundsätzlich ist dies jedoch nicht nötig, um die ausgewiesenen Kompetenzen dieses Bausteins zu fördern.	—	—	—

Unterrichtsmaterialien

siehe nächste Seiten

Folie 1 – „Caesar und sein General Strategus“

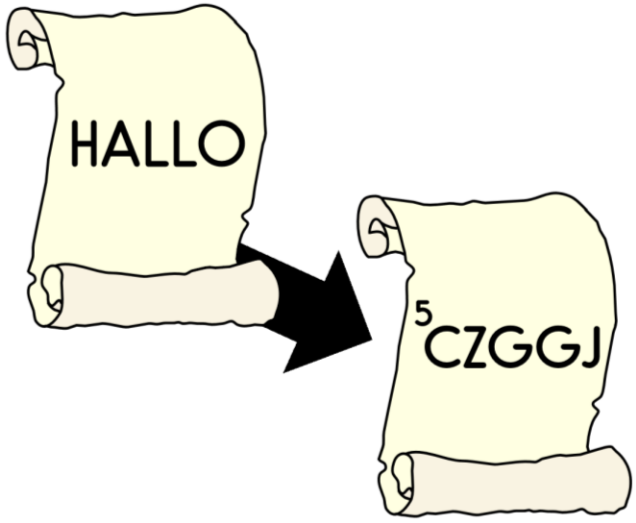
...ABER DIE RÖMER WURDEN BESIEGT!



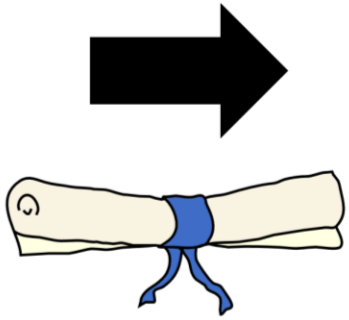
Wie konnte das passieren, wenn Caesar den perfekten Plan hatte?

Folie 2 – „Verschlüsseln, Versenden, Entschlüsseln“

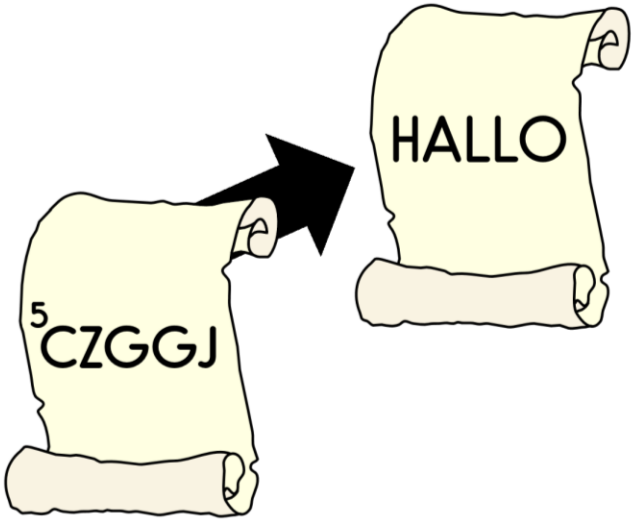
I. Verschlüsseln

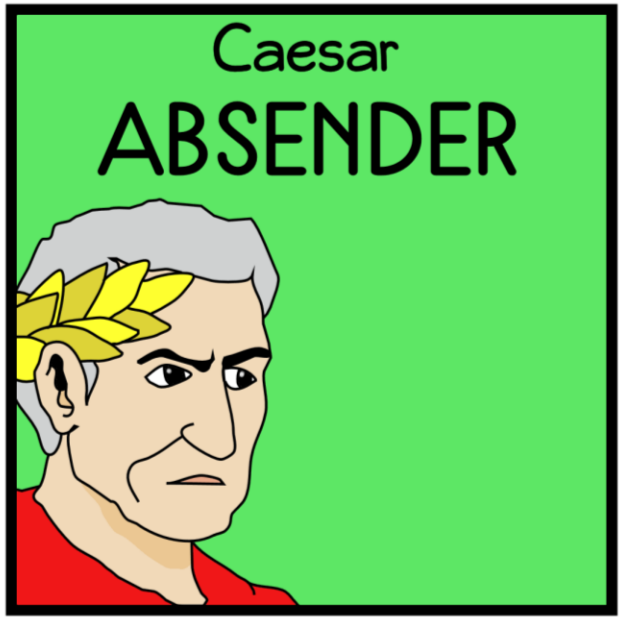


II. Versenden

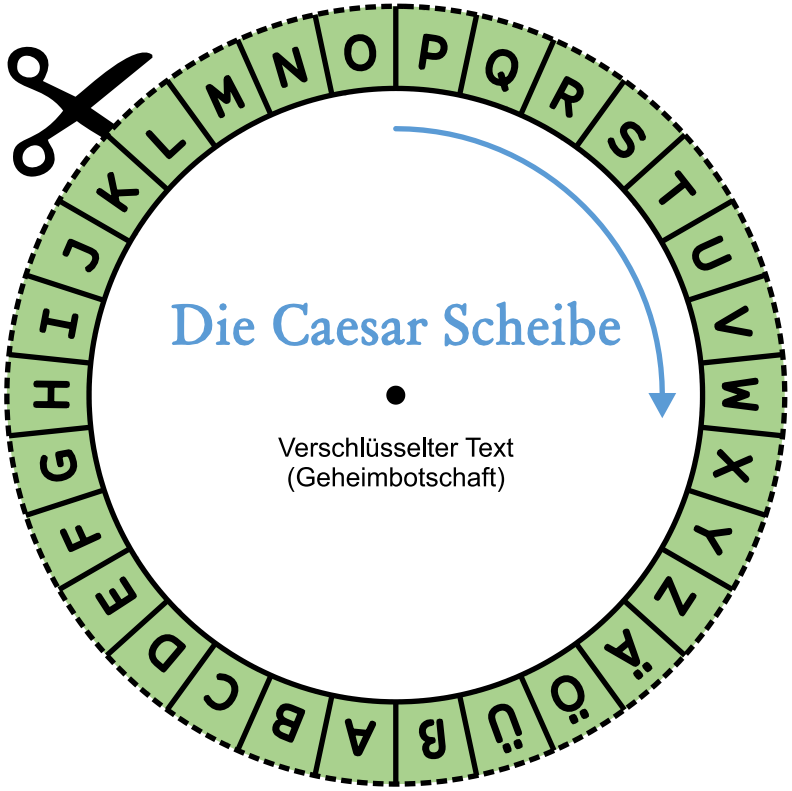


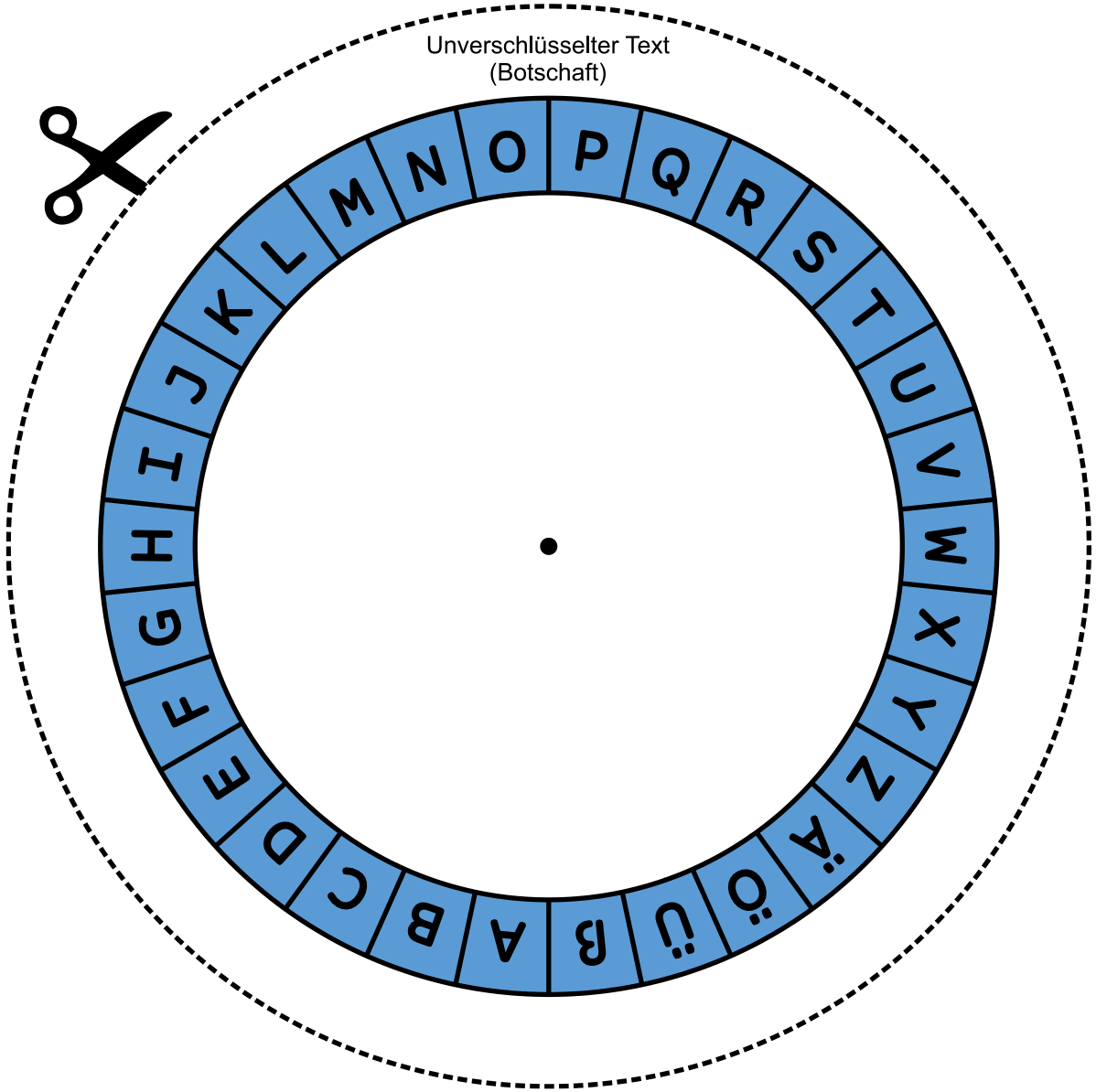
III. Entschlüsseln





Folie 3 – „Caesar-Scheibe“



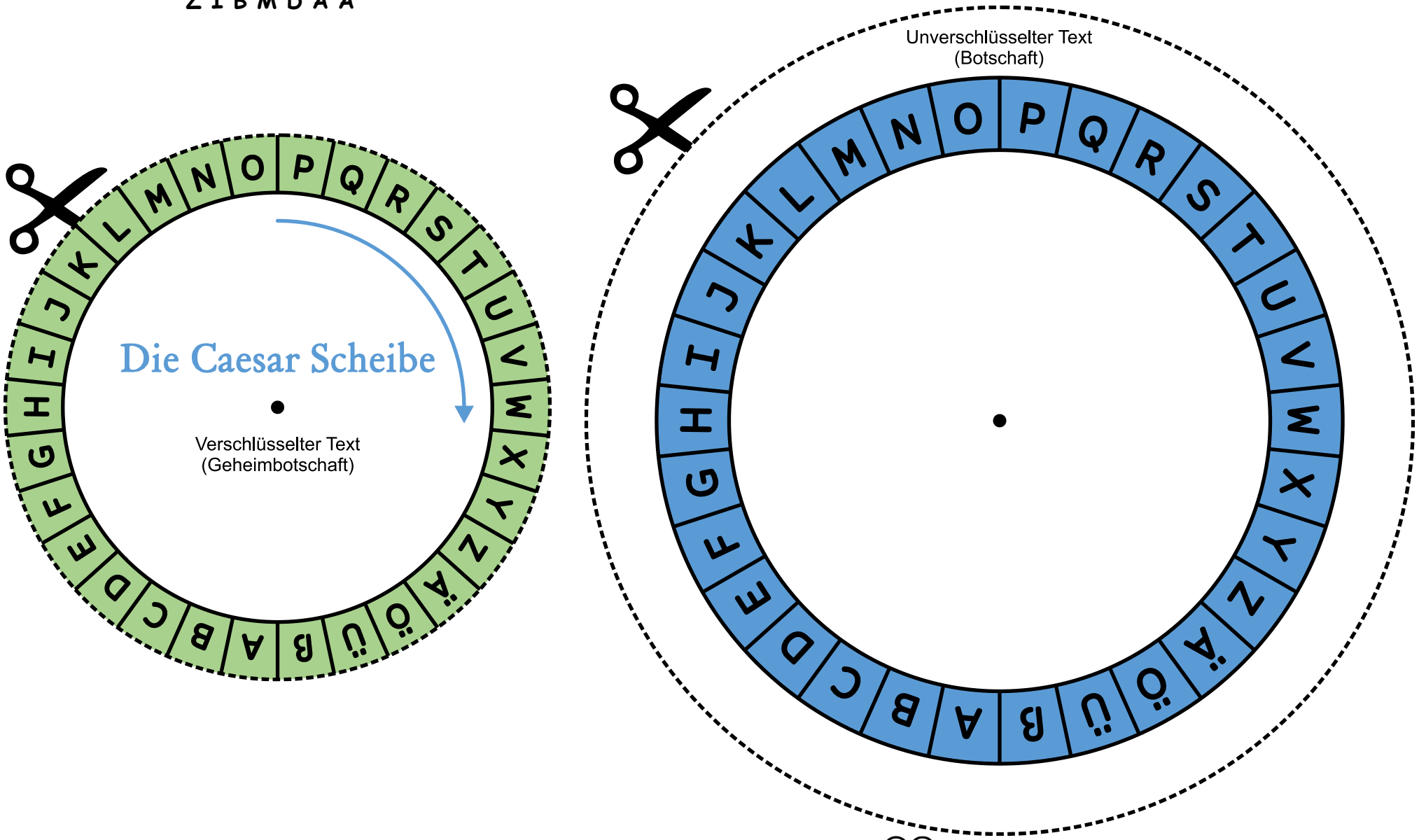


Arbeitsblatt 1 – „Caesar-Scheibe“

Aufgabe 1: Baue dir deine eigene Caesar-Scheibe und finde heraus, wie du damit eine Geheimbotschaft schreiben kannst.

Aufgabe 2: Hier ist eine Geheimbotschaft von Caesar an seinen General Strategus. Was wollte Caesar ihm mitteilen?

^{5}Z I B M D A A



Arbeitsblatt 2 – „Skytalen“

Aufgabe 1: Schneidet die drei Streifen mit den verschlüsselten Geheimbotschaften aus und entschlüsselt sie mit den Skytalen.
Aufgabe 2: Schneidet die drei leeren Streifen aus und schreibt auf jeden Streifen eine verschlüsselte Geheimbotschaft. Denkt daran, dass ihr dafür die Skytalen braucht!
Aufgabe 3: Sucht euch eine andere Partnergruppe und entschlüsselt gegenseitig eure Geheimbotschaften.

S L K E Y T A

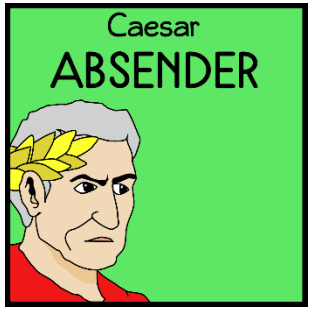
H F D A R E L E L U O N

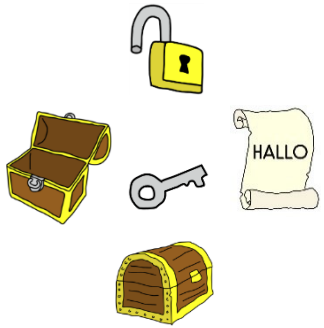
W G E D I E S I E H R T

Absender (Caesar)

Arbeitsblatt 3a – „Sicherung“

Aufgabe 1: Wer soll Botschaft, Schlüssel, Schloss, offene Kiste und verschlossene Kiste bekommen? Zeichne eine Linie für jeden Gegenstand zu Caesar oder Strategus!



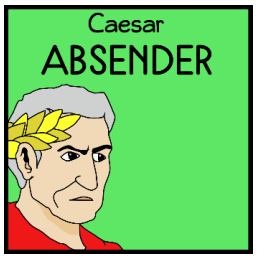


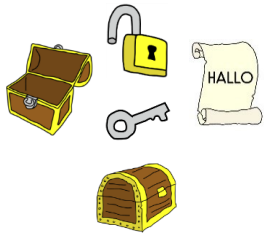
Aufgabe 2: Was müssen Caesar und Strategus unbedingt beachten, damit die Botschaft geheim bleibt? Kreuze an!

	Die verschlossene Kiste mit der Botschaft darf nicht von einem Dieb gestohlen werden!
	Strategus darf seinen Schlüssel niemals verleihen, verschenken oder verlieren!
	Caesar muss eine Geheimschrift benutzen!

Arbeitsblatt 3b – „Erweiterte Sicherung“

Aufgabe 1: Wer soll Botschaft, Schlüssel, Schloss, offene Kiste und verschlossene Kiste bekommen? Zeichne eine Linie für jeden Gegenstand zu Caesar oder Strategus!





Aufgabe 2: Wie kann Caesar seinem General Strategus eine Nachricht schicken? Sortiere die Schritte von 1 bis 8!

Schritt	Anleitung
	Absender verschließt die Kiste mit dem Schloss.
	Absender bekommt das offene Schloss.
	Empfänger liest die Botschaft.
	Empfänger bekommt den Schlüssel.
	Absender legt seine Botschaft in die Kiste.
	Empfänger bekommt die verschlossene Kiste.
	Absender bekommt die leere Kiste.
	Empfänger öffnet die Kiste mit dem Schlüssel.

Aufgabe 3: Was müssen Caesar und Strategus unbedingt beachten, damit die Botschaft geheim bleibt? Kreuze an!

	Die verschlossene Kiste mit der Botschaft darf nicht von einem Dieb gestohlen werden!
	Strategus darf seinen Schlüssel niemals verleihen, verschenken oder verlieren!
	Caesar muss eine Geheimschrift benutzen!

Literaturverzeichnis

Sämtliche Quellenangaben wurden zuletzt am 02.02.2021 geprüft.

Gesellschaft für Didaktik des Sachunterrichts (GDSU) (2013): Perspektivrahmen Sachunterricht. Zweite, vollständig überarbeitete und erweiterte Ausgabe. Kempten: Klinkhardt.

Gesellschaft für Informatik (GI) (2019): Kompetenzen für informatische Bildung im Primarbereich. Empfehlungen der Gesellschaft für Informatik e. V. erarbeitet vom Arbeitskreis »Bildungsstandards Informatik im Primarbereich«. Die Empfehlungen wurden am 31. Januar 2019 vom Präsidium der GI verabschiedet. In: LOG IN (Beilage) 39 (191/192), I-28. Online verfügbar unter https://dl.gi.de/handle/20.500.12116/29621.