

## Vorlage / Langentwurf / Unterrichtsstunde<sup>1</sup>

<b>Erstellt von:</b>	<input type="text"/>
<b>Matrikelnummer:</b>	<input type="text"/>
<b>Zeitung (Min.):</b>	<input type="text" value="90 Minuten"/>
<b>Klasse:</b>	<input type="text" value="4"/>
<b>Thema der Stunde:</b>	<input type="text" value="Wie können wir Botschaften verschlüsseln und entschlüsseln? Eine Einführung in verschiedene Verschlüsselungsverfahren."/>
<b>Thema der Reihe:</b>	<input type="text" value="Sicherer Umgang mit vertraulichen Informationen – Verschlüsseln und Entschlüsseln von (Geheim)Botschaften"/>

**Wichtiger Hinweis:** Bitte reichen Sie den Unterrichtsentwurf sowohl in gedruckter Form (Abgabe im Sekretariat Frau Andrea Lieske, Fliednerstr. 21, Raum 406B) sowie digital per E-Mail ([grundschulinformatik@uni-muenster.de](mailto:grundschulinformatik@uni-muenster.de)) ein.

---

<sup>1</sup> Diese Vorlage basiert auf dem Dokument „Schriftliche Arbeit mit Kommentar“ (Stand 03/2013) des Zentrums für schulpraktische Lehrerbildung Krefeld (ZfSL) / Seminar für das Lehramt an Gymnasien und Gesamtschulen.

## **Inhaltsverzeichnis:**

Deckblatt	S. I
Inhaltsverzeichnis	S. II
Schriftliche Planung des Unterrichts	
1. Ziele und angestrebte Kompetenzen	S. 1
2. Didaktische Schwerpunkte	S. 2
3. Geplanter Verlauf des Unterrichts – Artikulationsschema / Synopse	S. 6
Literaturverzeichnis	S. III
Anhang	S. IV
Versicherung	S. X

# 1. Ziele und angestrebte Kompetenzen

## Ein Stundenziel/Kernanliegen mit Indikator:

Die Schülerinnen und Schüler sollen die *Verschlüsselung* und *Entschlüsselung* von Informationen anhand von verschiedenen Verschlüsselungsverfahren kennenlernen und anwenden können sowie die Intention hinter der Anwendung solcher Verfahren auf verschiedene Daten verstehen.

Die Schülerinnen und Schüler zeigen dies, indem sie die Begriffe Verschlüsselung und Entschlüsselung sowie eine Methode der Verschlüsselung anhand eines Beispiels erklären können. Des Weiteren ist das Stundenziel erreicht, wenn die Schülerinnen und Schüler die Verwendung eines Verschlüsselungsverfahrens begründen können.

## Die Teilziele mit Indikator:

- Die SuS sollen die Begriffe *verschlüsseln* und *entschlüsseln* erklären können. Sie zeigen dies, indem sie die Begriffe anhand von Beispielen erläutern.
- Die SuS sollen (mindestens) ein spezielles Verschlüsselungsverfahren kennenlernen und dieses auf verschiedene Beispiele anwenden können. Sie zeigen dies, indem sie mit einem speziellen Verfahren aus einer verschlüsselten Botschaft eine unverschlüsselte Botschaft (Entschlüsselung) und aus einer unverschlüsselten Botschaft eine verschlüsselte Botschaft (Verschlüsselung) machen.
- Die SuS sollen die Intention hinter der Verwendung von Verschlüsselungsverfahren verstehen. Sie zeigen dies, indem sie die Vorteile einer verschlüsselten Botschaft gegenüber einer unverschlüsselten Botschaft benennen.

## Hierdurch sollen folgende Kompetenzen laut Lehrplan [MSW08] gefördert werden (je eine inhaltsbezogene und prozessbezogene Kompetenz):

In der geplanten Unterrichtsstunde soll insbesondere die prozessbezogene Kompetenz des Problemlösens bzw. kreativ Seins aus dem Lehrplan Mathematik für die Primarstufe gefördert werden. Hierbei sollen die SuS Zusammenhänge erkennen, Hypothesen aufstellen, eine Problemlösung durch systematisches Probieren, Reflektieren, Überprüfen und Erfinden herbeiführen. Zudem sollen sie zur Lösung von Problemstellungen entsprechende Regeln und Werkzeuge der Mathematik bzw. Informatik heranziehen. Da die Unterrichtsstunde ihren Schwerpunkt auf die Informatik legt, anstatt auf die Mathematik, entspricht keine inhaltsbezogene Kompetenz des Lehrplans Mathematik den direkten Anforderungen der Unterrichtsstunde. Im weiteren Sinn kann allerdings unter anderem der Schwerpunkt *Sachsituationen* aus dem Bereich *Größen und Messen* als Schlüsselkompetenz

der Unterrichtsstunde angesehen werden. In den Kompetenzerwartungen am Ende der Klasse 4 wird gefordert, dass die SuS zu „simulierten Situationen (...) und zu Sachaufgaben mathematische Fragen und Aufgabenstellungen [formulieren] und [diese] lösen“ [MSW08, S.66]. Zudem sollen die SuS in der Unterrichtsstunde zur erfolgreichen Bearbeitung der Sachaufgabe selbständig Hilfestellungen wie beispielsweise Tabellen oder Diagramme verwenden und eigene Sachaufgaben zu gegebenen Modellen der Mathematik bzw. Informatik aufstellen [vgl. MSW08].

Insgesamt liegt der Schwerpunkt der Stunde jedoch auf der informatischen Bildung, sodass zur Benennung der Kompetenzerwartungen die Bildungsstandards Informatik für den Primarbereich herangezogen werden sollten. Diese sind allerdings noch in Arbeit.

## 2. Didaktische Schwerpunkte

Die SuS haben sich bereits mit informatischen Themenbereichen auseinandergesetzt und arbeiten mit großem Interesse an Themen der Informatik. Zum Thema Ver- und Entschlüsselung wurde jedoch noch keine explizite Unterrichtsreihe durchgeführt. Dennoch kennen die SuS die Idee hinter diesen Verfahren aus zahlreichen Alltagsvorstellungen. Die SuS sind es gewohnt, sich im Sitzkreis zu treffen und in Gruppen zusammen zu arbeiten, sodass hierfür keine spezielle Anleitung erforderlich ist. Zudem kennen sie das in der Unterrichtsstunde verwendete Prinzip der Tippkarten, die erst nach ausreichendem systematischem Probieren zur Hilfe herangezogen werden dürfen.

**Lehr- und  
Lernausgangslage  
der SuS**

Die Kryptologie umfasst zwei Wissenschaften, die Kryptografie und die Kryptoanalyse. Erstere dient der Verschlüsselung von Informationen, „um deren Geheimhaltung zu sichern“ [KK10, S.1]. Zu den Zielen dieser Wissenschaft zählen unter anderem Vertraulichkeit, Integrität und Authentizität. Weiterführend bezeichnet die Kryptoanalyse die Entwicklung von Techniken und Methoden, die der Gewinnung von Informationen aus verschlüsselten Texten dienen. Sie „ist zur Überprüfung der Sicherheit kryptografischer Methoden unerlässlich“ [KK10, S.1]. In der geplanten Unterrichtsstunde wird nur die klassische Kryptologie thematisiert, die primär zur Aufgabe hat, die Vertraulichkeit von Nachrichten zu schützen. Auch wenn solche klassischen Verfahren in der heutigen Zeit nicht mehr zu empfehlen sind, kann hieran die Kryptologie verständlich dargestellt werden [vgl. KK10].

**Begrenzte  
Sachanalyse  
des U.-  
gegenstandes**

Zu den klassischen kryptografischen Verfahren gehören unter anderem auch die Zahlenschrift, die Caesar-Chiffre und die Schablonenschrift. Die Zahlenschrift ist ein einfaches Verschlüsselungsverfahren, bei dem jedem Buchstaben des Alphabets eine Zahl zugewiesen

wird. Durch verschiedene Varianten, wie zum Beispiel die Durchnumerierung des Alphabets in umgekehrter Reihenfolge oder eine Durchnumerierung nach geraden und ungeraden Zahlen, kann die Sicherheit des Verfahrens erhöht werden [vgl. J17]. Die Caesar-Chiffre ist eine der ältesten Verschlüsselungsverfahren und wird auch Verschiebe-Chiffre genannt. Julius Cäsar soll diese Chiffre bereits für militärische Zwecke benutzt haben [vgl. PP16]. Bei diesem Verfahren werden zwei normale Alphabete verwendet, ein Alphabet für den Klartext und ein Alphabet für den Geheimtext. Das Geheimtextalphabet ist zu dem Klartextalphabet um einige Stellen verschoben [vgl. Be12]. Demnach wird jedem Klartextbuchstaben durch Verschieben um eine festgelegte Anzahl an Positionen ein anderer Buchstabe – der Geheimtextbuchstabe – zugewiesen. Die Anzahl der verschobenen Positionen ergibt den Schlüssel [vgl. PP16]. Zur Vereinfachung dieses Verschlüsselungsverfahrens entwickelte Leon Battista Alberti 1470 eine Chiffriermaschine, die aus zwei übereinander gelegten, unterschiedlich großen Scheiben besteht. Die äußere Scheibe bildet die Klartextbuchstaben ab, während die innere Scheibe die Geheimtextbuchstaben anzeigt, indem sie verschoben wird. So kann mit Hilfe dieser Caesar-Scheibe jede beliebige Verschiebung eingestellt werden. Zur Ver- und Entschlüsselung mit der Schablone wird eine Fleißner-Schablone benötigt, die an ihren Seitenrändern von 1 bis 4 durchnummeriert ist. Die Schablone muss als erstes so auf das Briefpapier gelegt werden, dass die 1 oben liegt. In jedem Loch der Schablone darf nur ein Buchstabe stehen. Diese werden von links nach rechts, Zeile für Zeile ohne Lücke eingetragen und gelesen. Anschließend wird die Schablone weitergedreht und dasselbe durchgeführt, wenn die Seitenränder mit der Zahl 2, 3 und 4 oben liegen. Bleiben am Ende Löcher frei, werden dort beliebige Buchstaben eingetragen [vgl. J17].

Mit den SuS werden die Fachbegriffe der Kryptologie nicht explizit besprochen, da diese zu umfangreich für die Grundschule sind. Dennoch können durchaus die Begriffe Verschlüsseln und Entschlüsseln mit ihrer Bedeutung eingeführt werden. Auch die drei Verschlüsselungsverfahren können, wie oben dargestellt, vermittelt werden. Die Kinder sollten diese allerdings in Kombination mit einem expliziten Beispiel kennenlernen, damit die Verfahren anschaulicher und verständlicher werden.

Die Durchführung des informatisch geprägten Unterrichts lässt sich durch die Bildungsstandards der Sekundarstufe 1 und 2 sowie durch die noch nicht verbindlichen Bildungsstandards Informatik für den Primarbereich begründen. In diesen wird ausdrücklich formuliert, dass eine informatische Bildung zur Allgemeinbildung gehöre und sie ein anschlussfähiges, lebensbegleitendes Lernen ermöglichen soll. Insbesondere für das Berufsleben ist heutzutage ein grundlegendes Wissen über Informatik unverzichtbar [vgl. GI08]. Das Curriculum schreibt vor,

**Legitimation  
des Vorhabens  
durch  
curriculare  
Vorgaben**

dass „bedeutsame informatische Inhalte [...] dabei so vermittelt werden [sollen], dass sie von den Lernenden zur Problemlösung in gegenwärtigen und künftigen Lebenssituationen verwendet werden können.“ [GI08, S.12]

Bezieht man sich auf die Bildungsstandards Informatik für die Primarstufe, so kann die Unterrichtsstunde mit dem inhaltsbezogenen Kompetenzbereich *Information und Daten* legitimiert werden. Die Bildungsstandards empfehlen bezüglich dieses Kompetenzbereichs, dass die SuS am Ende der Klasse 4 „ein exemplarisches Verschlüsselungsverfahren [kennen], [...] systematische Verfahren an[wenden], um verschlüsselte Daten zu entschlüsseln [und] Vereinbarungen [entwickeln], um Daten zu verschlüsseln und entschlüsseln“ [GI17, S.9]. Ebenso kann die Unterrichtsstunde mit dem Kompetenzbereich *Informatik, Mensch und Gesellschaft* legitimiert werden, in dem es heißt: „Die SuS verschlüsseln Daten, um sie vor Dritten zu verbergen, [sie] entschlüsseln verschlüsselte Daten, [sie] erkennen, dass der Aufwand zum Entschlüsseln die Sicherheit deutlich macht [und] [sie] wenden einfache Verfahren zur Sicherung der Integrität von Daten an“ [GI17, S.11].

Die SuS sind bereits unbewusst mit der Ver- und Entschlüsselung von Daten vertraut. Sie erfahren solche Verfahren im übertragenen Sinn beispielsweise durch die von der Post übermittelten Postkarten und Briefe. Während eine Postkarte jeder lesen kann, bleiben die Informationen von Briefen durch die Verwendung von Umschlägen für Außenstehende verschlüsselt. Die SuS sollen die Wichtigkeit und Notwendigkeit von Verschlüsselungen in ihrer Umwelt erfahren. Insbesondere bei der Nutzung digitaler Medien, mit denen sie im Laufe ihres Lebens zunehmend in Kontakt kommen, sind ein grundlegendes Verständnis und basale Fertigkeiten zur Verschlüsselung von Nachrichten und Daten von Relevanz, da sie sich gerade über solche Medien rasant verbreiten können und private Informationen nicht für die Öffentlichkeit zugänglich sein sollten. Daher ist es wichtig die SuS im Laufe ihrer Entwicklung für die Notwendigkeit einer angemessenen Verschlüsselung ihrer Daten zu sensibilisieren. In der Grundschule sollte mit den klassischen Verschlüsselungsverfahren eine Basis geschaffen werden, auf der die weiterführenden Schulen aufbauen können.

Den Einstieg der Unterrichtsstunde bildet eine Geschichte bzw. das Vorlesen einer Postkarte. Diese soll die SuS motivieren und einen Anreiz zur Bearbeitung der folgenden Problemaufgabe liefern. Die Durchführung findet im Sitzkreis statt, sodass eine gemütliche und ruhige Atmosphäre geschaffen wird und die Kinder sich in die Geschichte hineinversetzen können. Bereits in der Einstiegsphase lernen die SuS ein Verschlüsselungsverfahren kennen, da nicht bekannt ist, ob die SuS bereits mit Geheimschriften vertraut sind. Durch den ersten Kontakt mit einem solchen Verfahren sollen die SuS auf die anschlie-

**Relevanz für  
die SuS**

**Begründung  
der wichtigsten  
Entscheidungen  
des  
geplanten  
Unterrichts**

Bende Entschlüsselung einer anderen Geheimschrift vorbereitet werden. Diese Entschlüsselung soll in Gruppenarbeit durchgeführt werden, sodass eine positive wechselseitige Beeinflussung der kindlichen Ideen erfolgen kann und ein zufrieden stellendes Ergebnis erzielt wird. Die Intention der eigenständigen Probierphase ist, das entdeckende Lernen zu fördern und alle Kinder kognitiv zu aktivieren. Während dieser Phase werden Tippkarten bereitgestellt, die jedoch erst herangezogen werden dürfen, wenn die SuS keine weiteren Ideen haben. Die Tippkarten sollen eine mögliche Überforderung und eine zu große Frustration der Kinder verhindern. Nach der kurzen Probierphase erhalten die Gruppen einen Informationstext zu ihrem jeweiligen Verschlüsselungsverfahren. Das Verschlüsselungsverfahren sollen sie sich mit Hilfe des Textes aneignen. Damit sie dieses in der anschließenden Präsentationsphase der gesamten Klasse vorstellen können, sollen sie sich einige Stichwörter aus dem Text notieren. Zudem ist es den Gruppen spätestens jetzt möglich, die Geheimschrift zu entschlüsseln, so dass ein Erfolgserlebnis in jeder Gruppe gewährleistet wird.

Damit die Kinder der Klasse auch den Rest der Stunde konzentriert weiterarbeiten können, wird eine kurze Bewegungspause eingebaut. Anschließend sollen die SuS ihre Verschlüsselungsverfahren vorstellen und ihre Ergebnisse zusammentragen. Dadurch wird gewährleistet, dass die gesamte Klasse alle Verschlüsselungsverfahren kennt und nicht nur das selbst Erarbeitete. Zudem kann nur durch das Zusammentragen aller entschlüsselten Schatzkarten-Teile der Schatz gefunden werden, der für die SuS in der Klasse versteckt wurde. Der echte Schatz soll die SuS auf eine weiterführende Auseinandersetzung mit der Thematik motivieren. In einer abschließenden Sicherungsphase soll das in der Stunde angeeignete Wissen noch einmal im Plenum zusammengetragen werden. Hierbei sollen insbesondere auch die Bedeutung und der Zweck solcher Verfahren im Fokus stehen. Durch die aufgegebene Hausaufgabe sollen sich die SuS weiterführend mit den Inhalten der Stunde auseinandersetzen. Zudem sollen sie sich auch einmal explizit der Verschlüsselung von Informationen widmen, da es in der Stunde überwiegend um die Entschlüsselung geht. Durch die Hausaufgabe kann überprüft werden, ob die SuS die Verschlüsselungsmethoden verstanden haben. Das Basteln der Hilfsmittel soll zur Vereinfachung der Hausaufgabe und der weiterführenden Arbeit mit den Verschlüsselungsverfahren dienen.

### 3. Geplanter Verlauf des Unterrichts – Artikulationsschema/Synopse

Dauer (Min.)	Unterrichtsphase	Unterrichtsinhalt	Sozial-/ Aktionsform	Materialien/ Medien/ Werkzeuge	didaktisch-methodischer Kommentar
10-15 Min.	Einstieg	<p>Die Lehrkraft erzählt eine kleine Geschichte bzw. liest einen Brief vom Klassentier Felix vor:</p> <p>→ Das Klassentier Felix ist wieder auf großer Weltreise. Aus Italien hat er der Klasse einen Brief geschrieben, indem er davon berichtet, dass er eine Flaschenpost mit einer echten Schatzkarte gefunden hat. Der Schatz scheint im Klassenraum der Klasse versteckt zu sein. Die Schatzkarte ist in 3 Teile zerrissen und jeder Teil ist in einer anderen Geheimschrift geschrieben. Den ersten Teil hat Felix bereits entschlüsselt, aber die beiden restlichen Teile sollen von der Klasse selbst entschlüsselt werden. Deswegen bittet er die Klasse, die Schatzkarte vollständig zu entschlüsseln, um den Schatz zu finden.</p> <p>Die Lehrkraft zeigt den ersten Schatzkartenteil, den Felix bereits entschlüsselt hat und erklärt das Verschlüsselungsverfahren.</p>	Plenum (Sitzkreis)	<ul style="list-style-type: none"> <li>• Brief von Felix</li> <li>• 2 Schatzkartenteile in verschlüsselter Form</li> <li>• 1 Schatzkartenteil in verschlüsselter Form</li> </ul>	<p>Das Vorlesen der Geschichte soll im Sitzkreis stattfinden, so dass eine gemütliche Atmosphäre entsteht. Der Einstieg mit einer Geschichte soll die SuS motivieren und ihnen einen Anreiz zur Bearbeitung der folgenden Problemaufgabe liefern. Die Vorstellung des ersten Schatzkartenteils und damit die Vorstellung des ersten Verschlüsselungsverfahrens soll den SuS eine erste Idee von Geheimschriften sowie ihrer Ver- und Entschlüsselung geben und einen ersten Ansatz für ihre eigenen Verschlüsselungsversuche liefern. Insbesondere durch den Einbezug des eigenen Klassentiers soll eine hohe Motivation erzeugt werden.</p>

Dauer (Min.)	Unterrichtsphase	Unterrichtsinhalt	Sozial-/ Aktionsform	Materialien/ Medien/ Werkzeuge	didaktisch-methodischer Kommentar
15 Min.		<p>Die SuS werden in 4er-Gruppen eingeteilt. Jede Gruppe erhält einen Teil der Schatzkarte und ggf. die notwendigen Entschlüsselungs-Materialien (Fleißner-Schablone).</p> <ol style="list-style-type: none"> <li>1. Schatzkarte in Schablonenschrift</li> <li>2. Schatzkarte mit Caesar-Chiffre</li> </ol> <p>Sie versuchen eigenständig die geheime Botschaft zu entschlüsseln sowie die jeweilige Verschlüsselungsmethode zu verstehen.</p> <p>→ Tippkarten bieten eine kleine Hilfestellung, wenn die SuS keine Ideen haben</p>	Gruppenarbeit	<ul style="list-style-type: none"> <li>• 2 Schatzkarten-Teile</li> <li>• Fleißner-Schablone</li> <li>• Tippkarten</li> </ul>	<p>Durch die eigenständige Probierphase soll eine kognitive Aktivierung der SuS erfolgen. Zudem soll das entdeckende Lernen gefördert werden. Die Tippkarten verhindern dabei die Überforderung und Frustration der Kinder.</p>
15 Min.	Erarbeitung	<p>Nach der kurzen eigenständigen Testphase erhält jede Gruppe einen kleinen Informationstext und weitere Hilfsmittel (Caesar-Scheibe) zu ihrem jeweiligen Verschlüsselungsverfahren. Sie lesen den Text durch, notieren sich Stichwörter und versuchen anschließend ihren Schatzkarten-Teil vollständig zu entschlüsseln.</p>		<ul style="list-style-type: none"> <li>• Informationstexte zu den Verschlüsselungsmethoden</li> <li>• Hilfsmittel (Caesar-Scheibe)</li> </ul>	<p>Die SuS sollen sich ihr Verschlüsselungsverfahren aneignen, sich zur Sicherung einige Notizen machen und ein Erfolgserlebnis bei der endgültigen Entschlüsselung verspüren.</p>
5 Min.	Pause	<p>Nach der langen ersten Erarbeitungsphase dürfen die SuS eine Runde über den Schulfhof laufen.</p>			<p>Die SuS sollen sich kurz bewegen, um anschließend konzentriert weiterarbeiten zu können.</p>

Dauer (Min.)	Unterrichtsphase	Unterrichtsinhalt	Sozial-/ Aktionsform	Materialien/ Medien/ Werkzeuge	didaktisch-methodischer Kommentar
20 Min.	Auswertung/ Präsentation	<p>Zwei Gruppen (eine Gruppe zur Schablone- schrift und eine Gruppe zur Caesar- Chiffre) stellen nacheinander ihre Ver- schlüsselungsmethode vor. Sie erklären un- ter Einbezug der Hilfsmittel, wie ihr Verfah- ren funktioniert.</p> <p>Die Gruppen tragen ihre Ergebnisse zu- sammen, sodass die gesamte Schatzkarte als Klartext vorliegt. Die SuS folgen den Anweisungen der Schatzkarte und können so tatsächlich den Schatz finden und öff- nen (mit einem Schlüsselentschlüsseln).</p>	Plenum	<ul style="list-style-type: none"> <li>Ggf. Informati- onstexte, Hilfs- mittel, etc.</li> <li>Schatzkarte</li> <li>Bunte Box</li> <li>Schlüssel für die Schatztruhe</li> <li>Schatztruhe mit einer Überra- schung drin</li> </ul>	Die SuS stellen ihre Verschlüs- selungsverfahren vor, sodass alle Kinder auch das Ver- schlüsselungsverfahren der jeweils anderen Gruppe ken- nen. Zudem soll hierdurch die Kompetenz des Darstellens gefördert werden. Durch die Suche des tatsäch- lich versteckten Schatzes sol- len die SuS für den Rest der Stunde und für eine weiterfüh- rende Auseinandersetzung mit der Thematik motiviert werden.
10 Min.	Sicherung und Haus- aufgabe	<p>Abschließend wird zusammenfassend die Bedeutung der beiden Begriffe <i>Verschlüs- selung</i> und <i>Entschlüsselung</i> thematisiert sowie der Zweck, der hinter der Verwen- dung solcher Verschlüsselungsverfahren steckt.</p> <p>Die Lehrkraft erklärt die Hausaufgabe:  → <b>Hausaufgabe:</b> Die SuS schreiben eine Antwort an Felix, in der sie u. a. erzäh- len, dass sie den Schatz gefunden ha- ben. Da nicht jeder von dem Schatz</p>	Plenum (Sitzkreis)	<ul style="list-style-type: none"> <li>Hausaufgaben- Zettel</li> </ul>	Das in der Stunde angeeigne- te Wissen der SuS soll noch einmal zusammenfassend im Plenum zusammengetragen werden, um eine allgemeine Ergebnissicherung zu gewähr- leisten. Durch die Hausaufgabe sollen die SuS sich weiterführend mit den Inhalten der Stunde aus- einandersetzen. Zudem sollen sie sich auch einmal explizit
10-15 Min.			Plenum		

Dauer (Min.)	Unterrichtsphase	Unterrichtsinhalt	Sozial-/ Aktionsform	Materialien/ Medien/ Werkzeuge	didaktisch-methodischer Kommentar
		<p>wissen soll, schreiben sie den Brief in Geheimschrift. Die SuS dürfen selbst entscheiden, welche der Geheimschriften sie verwenden möchten.</p> <p>Um die Hausaufgabe zu vereinfachen, basteln die SuS sich in den letzten 10 Minuten selbst das Hilfsmittel zu dem Verschlüsselungsverfahren, in dem sie Felix antworten möchten (Fleißer-Schablone oder Caesar-Scheibe).</p>	<p>Einzelarbeit</p>	<ul style="list-style-type: none"> <li>• Bastelanleitung</li> <li>• Bastelvorlagen zum Ausschneiden</li> <li>• Schere</li> <li>• Stifte</li> <li>• Reiszwecken</li> </ul>	<p>der Verschlüsselung von Informationen widmen, da es in der Stunde überwiegend um die Entschlüsselung ging. Durch die Hausaufgabe kann überprüft werden, ob die SuS die Verschlüsselungsmethoden verstanden haben. Das Basteln der Hilfsmittel soll zur Vereinfachung der Hausaufgabe und der weiterführenden Arbeit mit den Verschlüsselungsverfahren dienen.</p>

## Literaturverzeichnis:

- [Be12] Beutelspacher, Albrecht (Hrsg.): Geheimsprachen. Geschichte und Techniken, 5. Auflage, C. H. Beck, München, 2012.
- [GI08] Gesellschaft für Informatik e.V. (Hrsg.): Grundsätze und Standards für die Informatik in der Schule, Bildungsstandards Informatik für die Sekundarstufe 1, LOG IN, Berlin, 2008, <http://www.informatikstandards.de/>, Stand: 25.02.2017.
- [GI17] Gesellschaft für Informatik e. V. (Hrsg.): Bildungsstandards Informatik für den Primarbereich – zur Diskussion, Version 542, <http://metager.to/gibspdf>, Stand: 25.02.2017.
- [J17] Jungschar, [http://www.jungschar.biz/w/?page\\_id=2241](http://www.jungschar.biz/w/?page_id=2241), Stand: 25.02.2017 (Reinschmidt, Günter: Häuptlingsbuch Geheimschriften).
- [KK10] Karpfinger, C.; Kiechle, H. (Hrsg.): Kryptologie. Algebraische Methoden und Algorithmen, Vieweg + Teubner, Wiesbaden, 2010.
- [MSW08] Ministerium für Schule und Weiterbildung des Landes NRW (Hrsg.): Richtlinien und Lehrpläne für die Grundschule in NRW, Lehrplan Mathematik, Ritterbach Verlag, Frechen, S. 53-67, 2008, [http://www.schulentwicklung.nrw.de/lehrplaene/upload/lehrplaene\\_download/grundschule/grs\\_faecher.pdf](http://www.schulentwicklung.nrw.de/lehrplaene/upload/lehrplaene_download/grundschule/grs_faecher.pdf), Stand: 07.07.2016.
- [PP16] Paar, Christof; Pelzl, Jan (Hrsg.): Kryptografie verständlich. Ein Lehrbuch für Studierende und Anwender, Springer, Berlin u.a., 2016.

## Anhang:

### Brief von Klassentier Felix:

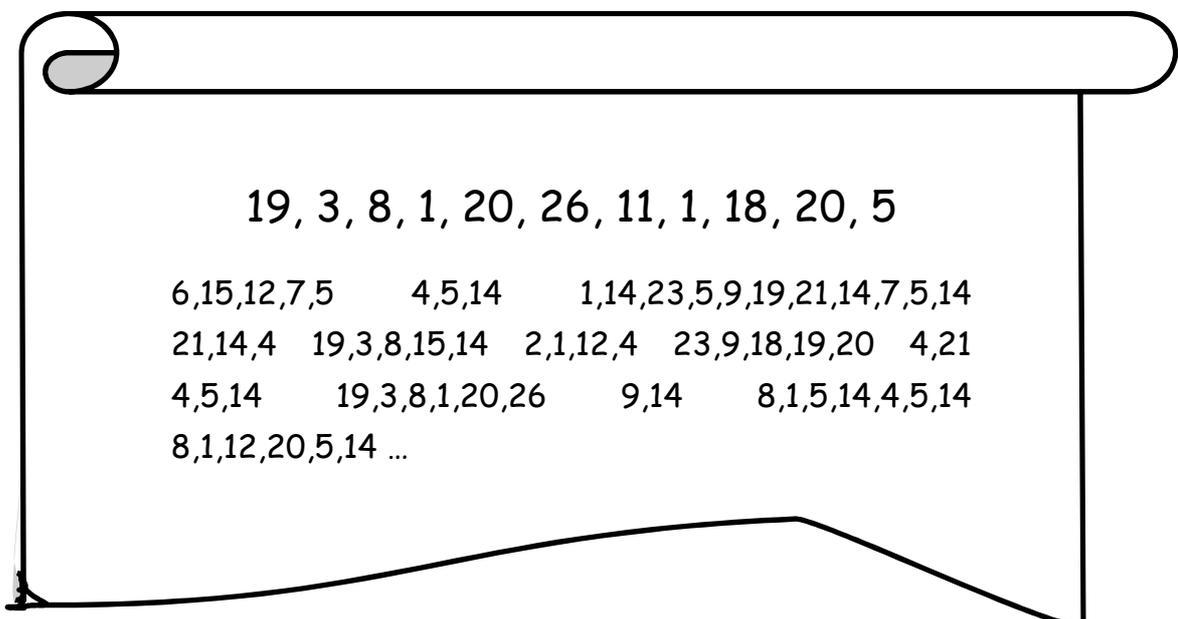
„Liebe Klasse 4a,

das Fernweh hat mich mal wieder ins Ausland verschlagen. Derzeit bin ich in Italien, einem wunderschönen Land mit netten Menschen und sehr gutem Essen. Tagsüber liege ich entweder am Meer und lasse mir die Sonne auf den Bauch scheinen oder ich gucke mir die wunderschönen Städte Italiens an. Vor ein paar Tagen, als ich mal wieder am Strand das Leben genießen wollte, blinkte etwas Auffälliges im Sand. Es sah aus wie eine gewöhnliche Flaschenpost, doch als ich sie öffnete, bemerkte ich, dass diese Flaschenpost das größte und abenteuerlichste Ereignis meines und vielleicht auch eures Lebens werden könnte. In ihr befanden sich 3 Teile einer echten Schatzkarte. Könnt ihr euch das vorstellen – eine echte Schatzkarte? Ich habe sie mit in den Brief gelegt, denn ich brauche unbedingt eure Hilfe! Der Schatz scheint direkt in eurer Klasse versteckt zu sein. Doch ganz so einfach ist es nicht, denn die Schatzkarte wäre natürlich keine echte Schatzkarte, wenn sie nicht in einer Geheimschrift geschrieben wäre. Und anstatt eine einzige Geheimschrift zu verwenden, wurde jedes Schatzkarten-Teil auch noch auf eine andere Art und Weise verschlüsselt. Einen der 3 Schatzkarten-Teile habe ich bereits für euch entschlüsselt, doch bei den restlichen beiden seid ihr gefragt. Könnt ihr die Geheimschriften der Karten entschlüsseln und den Schatz finden?

Meldet euch bei mir, wenn ihr den Schatz gefunden habt! Ich vermisse euch sehr...

Sonnige Grüße, euer Felix“

### Verschlüsselte Schatzkarten-Teile



1.

N	L	I	H	A	N
D	D	U	E	E	R
F	A	N	R	K	Z
T	M	U	S	C	A
H	N	M	F	S	E
B	E	R	E	L	C

2.

V	A	Ö	E	N	F
F	E	K	R	N	B
I	U	N	S	T	S
T	E	T	S	I	E
E	E	E	C	I	B
O	K	X	J	T	N

(Der Schlüssel ist E bzw. 5)

PEYJ DYQ VIKEP YRXIV HIV YLV. DMIL HMI YR-  
XIVWXI FSB LIVEYW, HELMRXIV JMRHIWX HX  
HMI WGLEXDXVYLI. SIJJRI WMI QMX HIQ  
WGLPYIWWIP YRH HIV WGLEXD KILSIVX H MV.

## Entschlüsselter Schatzkarten-Teil 1



## Tippkarten

 **Tippkarte** für die Schablonenschrift

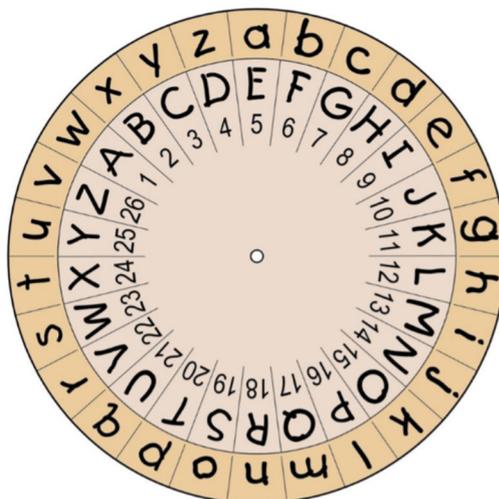
Achte auf die Zahlen am Rand der Schablone und lies die Buchstaben Zeile für Zeile von oben nach unten.

 **Tippkarte** für die Caesar-Verschlüsselung:

Jeder Buchstabe steht für einen anderen Buchstaben des Alphabets. Schreibe dir das Alphabet am besten auf 2 Papierstreifen (auf jeden Streifen einmal) und verschiebe sie zueinander, um die Lösung zu finden.

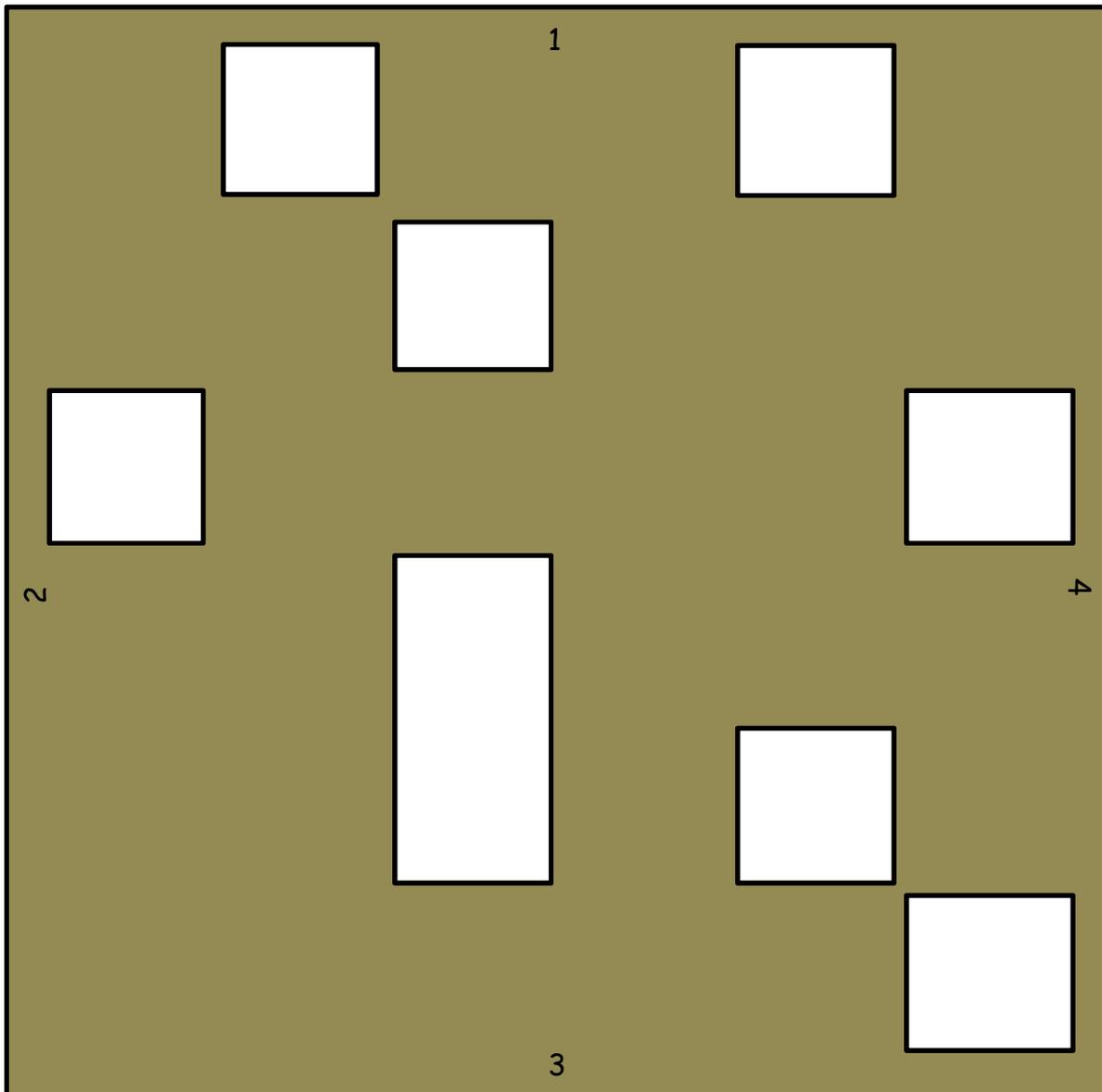
## Hilfsmittel

### 1. Caesar-Scheibe



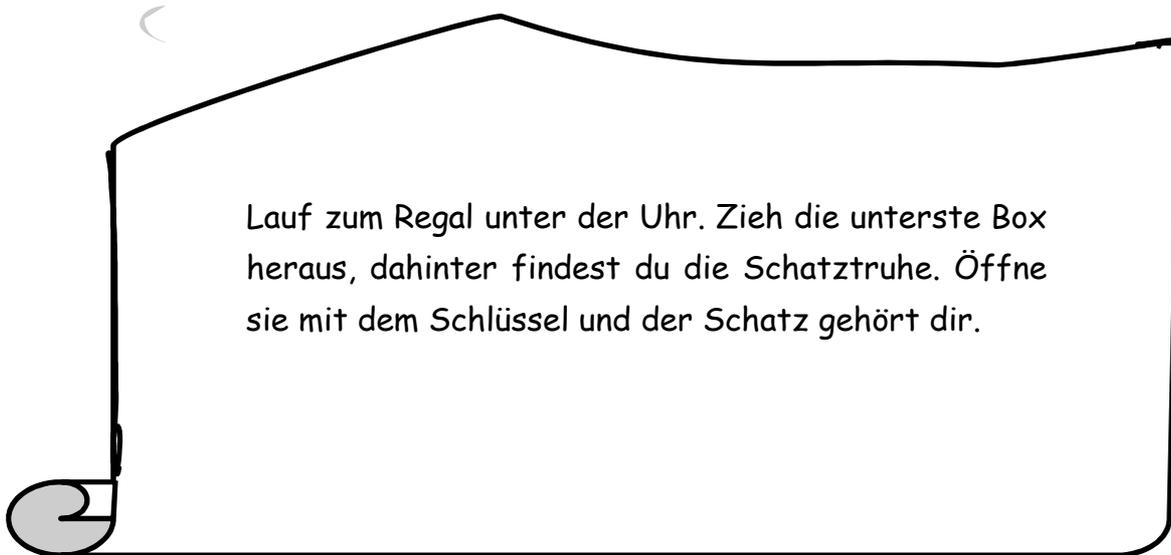
Quelle: [J17]

2. Fleißner-Schablone:



Erwartete Ergebnisse der SuS zur Erarbeitungsphase

Lauf zum Schrank neben der Tafel. In dem Schrank ist eine bunte Box versteckt. Öffne sie...



## Informationstexte zu den Verschlüsselungsverfahren

### *Schablonenschrift*

Für die Verschlüsselung und Entschlüsselung mit der Schablonenschrift brauchst du eine Fleißner-Schablone. Diese hat eine bestimmte Anzahl an Löchern, die so auf der Schablone angeordnet sein müssen, dass jeder Buchstabe der zu entschlüsselnden Nachricht nur einmal gelesen wird. Die Schablone ist zudem an ihren Seitenrändern von 1 bis 4 durchnummeriert. Sie muss als erstes so auf das Briefpapier gelegt werden, dass die 1 oben liegt. In jedem Loch der Schablone darf nur ein Buchstabe stehen. Die Buchstaben werden von links nach rechts und Zeile für Zeile eingetragen und auch gelesen. Anschließend wird die Schablone weitergedreht und die Zahl 2 liegt oben. Auch hier wird in jedes Loch ein Buchstabe eingetragen. Genau das Gleiche wird gemacht, wenn die Zahl 3 und die Zahl 4 oben liegen. Es kommt oft vor, dass am Ende Löcher frei bleiben, weil die Nachricht wenige Buchstaben hat als die Anzahl der Löcher. Dann werden die restlichen Löcher mit beliebigen Buchstaben aufgefüllt.

### *Caesar-Verschlüsselung*

Die Caesar-Verschlüsselung ist eine der ältesten Verschlüsselungsverfahren. Sie wird auch Verschiebe-Chiffre genannt. Schon Julius Cäsar soll diese Verschlüsselung benutzt haben. Bei diesem Verfahren wird jedem Buchstaben ein anderer Buchstabe zugewiesen. Dies passiert durch gleichmäßiges Verschieben der Buchstaben zweier Alphabete. Wichtig für die Entschlüsselung ist, dass man die Anzahl der verschobenen Positionen kennt. Nur durch sie weiß man, welcher Geheimschrift-Buchstabe zu welchem Buchstaben gehört. Zur Vereinfachung des Verschlüsselungsverfahrens wurde eine sogenannte Chiffriermaschine entwickelt, die Caesar-Scheibe. Sie besteht aus zwei übereinander gelegten, unterschiedlich großen Scheiben. Die äußere Scheibe zeigt die Klartextbuchstaben ab, wäh-

rend die innere Scheibe die Geheimentextbuchstaben anzeigt, indem sie verschoben werden kann. So kann mit Hilfe der Maschine jede beliebige Verschiebung eingestellt werden.

### Hausaufgabenzettel



Schicke Felix eine Postkarte als Antwort. Darin sollst du unter anderem erzählen, dass ihr den Schatz gefunden habt. Da natürlich nicht jeder von dem Schatz wissen soll, musst du den Brief in Geheimschrift schreiben. Wähle selbst, welche der Geheimschriften du verwenden möchtest. Zur Bearbeitung der Hausaufgabe dient dir das entsprechende Hilfsmittel (entweder Fleißner-Schablone oder Caesar-Scheibe).

### Bastelanleitung



Schneide die Bastelvorlage an den vorgegebenen Linien aus!

(Fleißner-Schablone): Schneide auch die Löcher der Schablone aus. Nummeriere nun die 4 Seitenränder von 1 bis 4 durch. Schneide dir anschließend einige Blätter in der entsprechenden Größe als Briefpapier zurecht.

(Caesar-Scheibe): Beschrifte beide ausgeschnittenen Scheiben im Uhrzeigersinn mit dem Alphabet, sodass am Ende in jedem Feld ein Buchstabe steht. Leg die kleine Scheibe auf die große Scheibe und steche mit einem spitzen Gegenstand ein Loch in die Mitte der Scheiben. Durch das Loch schiebst du eine Reiszwecke und befestigst sie. Schon ist die Caesar-Scheibe fertig.

## Versicherung:

„Ich versichere, dass ich den Unterrichtsentwurf eigenständig verfasst, keine anderen Quellen und Hilfsmittel als die angegebenen benutzt und die Stellen des Unterrichtsentwurfs, die anderen Werken dem Wortlaut oder Sinn entnommen worden sind, in jedem einzelnen Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe. Das Gleiche gilt auch für beigegebene Zeichnungen, Kartenskizzen und Darstellungen. Anfang und Ende von wörtlichen Textübernahmen habe ich durch An- und Abführungszeichen, sinngemäße Übernahmen durch direkten Verweis auf die Verfasserin oder den Verfasser gekennzeichnet.“

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift

## Verwertungsrechte:

„Ich erkläre mich damit einverstanden, dass der von mir verfasste Unterrichtsentwurf durch den Arbeitsbereich Didaktik der Informatik der Westfälischen Wilhelms-Universität Münster verwertet werden darf. Dazu gehören die Nutzung und/oder die Veränderung in zukünftigen Lehrveranstaltungen sowie für zukünftige digitale und/oder gedruckte Veröffentlichungen.“

Dabei soll folgende Einschränkung gelten (bitte ankreuzen):

Der Unterrichtsentwurf soll anonymisiert werden (Vor- und Nachname).“

Die folgenden Daten werden unabhängig von dieser Einschränkung grundsätzlich aus dem Dokument entfernt: E-Mail Adresse, Anschrift und Matrikelnummer.

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift