Informatikunterricht in der Gemeinschaftsschule

Cäsars Verschlüsselung auf der Spur

Esra Borali

Auf eine Zeitreise ins Antike Rom nimmt Esra Borali, Anwärterin aus Kurs 2019, ihre Informatiklerngruppe mit. Die Siebtklässler entschlüsseln Cäsars Code und lernen dabei auf äußerst motivierende Art, Verschlüsselungsverfahren zu beschreiben und Verschlüsselungen anzuwenden.

Dass Nachrichten verschlüsselt werden müssen, sodass sie nur dem Empfänger vorbehalten sind, ist keine Erfindung der Moderne. Verschlüsselungsverfahren sind für unseren Alltag, besonders im Umgang mit Medien und dem Internet elementar, auch wenn sie sich meist im Hintergrund abspielen und ohne dass wir davon etwas mitbekommen. Bereits bei den alten Römern wurden verschlüsselte Botschaften ausgetauscht, die durch spezielle Verschlüsselungsverfahren erzeugt wurden. Die Cäsar-Verschlüsselung stellt dabei eine exemplarische symmetrische Verschlüsselungsmethode dar, das Thema meiner geplanten Lehrprobenstunde. Da durch die Corona-Schutzmaßnahmen die geplante Prüfungsstunde nicht abgehalten, sondern nur geplant und ausführlich reflektiert wurde, kann nur die Stundenplanung im Folgenden genauer beschrieben werden.

Stundenziel

Meine geplante Stunde hatte zum Ziel, dass die Schüler das Cäsar-Verschlüsselungsverfahren beschreiben und die Verschlüsselung und Entschlüsselung mithilfe der Cäsar-Scheibe anwenden.

Lernvoraussetzungen

Die Cäsar-Verschlüsselung lässt sich der Einheit „Informationsgesellschaft und Datensicherheit“ zuordnen. In dieser Einheit werden die Schüler unter anderem dafür sensibilisiert, wie und warum sie ihre Daten schützen sollten. Mit der Cäsar-Verschlüsselung wird ein einfaches symmetrisches Verschlüsselungsverfahren thematisiert und außerdem findet eine historische Betrachtung der Thematik statt. Den Schülern sind Begriffe wie Klartext, Geheimtext, Schlüssel, verschlüsseln und entschlüsseln bereits aus vorangegangen Stunden bekannt. Es wurde allerdings noch nicht auf ein spezifisches Verschlüsselungsverfahren eingegangen, sodass diese Stunde zur Vertiefung dient. Da die geplante Stunde in einer Gemeinschaftsschule stattfindet und die einzelnen Schüler auf ihrem jeweiligen Niveau arbeiten, ist die Selbstkontrolle eingeübt und auch das Benutzen von Hilfskärtchen ritualisiert.

Einstieg

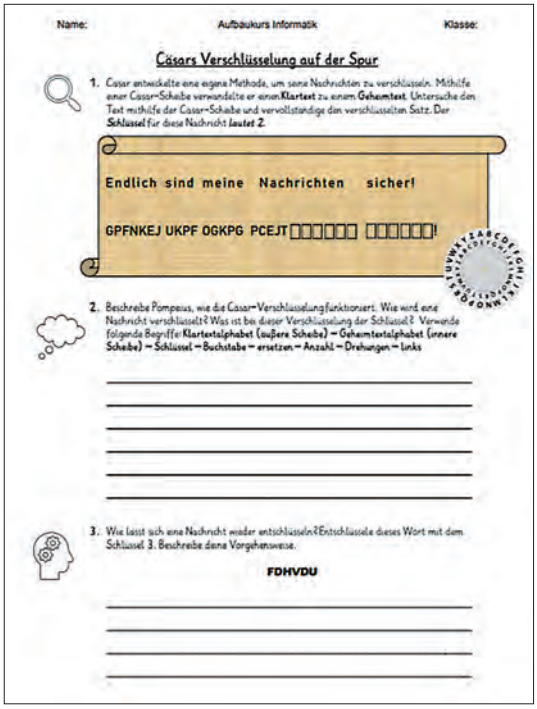
Die gesamte Einheit wird durch den moderierenden Charakter Judy Krypto begleitet. Judy Krypto stellt über Präsentationsfolien Fragen, erteilt Arbeitsaufträge und verteilt nach jedem Abenteuer, das die Schüler durch die Lerneinheit hinweg erleben ein Souvenir. Die beschriebene Stunde stellt ein Abenteuer in Form einer Zeitreise dar. Das Ganze wird über eine Prezi-Präsentation visuell unterstützt, wodurch der Motivationsaspekt in dieser Phase im Fokus steht.

Die Lerngruppe befindet sich im alten Rom, Cäsar ist entrüstet darüber, dass seine Angriffsversuche erneut gescheitert sind, weil seine Nachrichten abgefangen wurden. In seiner Verzweiflung sucht er nach einer Methode seine Nachrichten zu verschlüsseln, ohne auf erfundene Zeichen zurückzugreifen. Cäsar kommt zu einer Lösung und entwickelt eine Methode, um seine Nachrichten zu verschlüsseln.

Diese Methode ist den Schülern allerdings noch unbekannt. Ein Abschnitt der verschlüsselten Nachricht und das damit verbundene Geheimnis sollen die Schüler kognitiv aktivieren.

Erarbeitungsphase

Um den unterschiedlichen Lerntempi gerecht zu werden, sollen die Schüler nun in Einzelarbeit Cäsars Verschlüsselungsmethode unter Angabe des halb verschlüsselten Textes selbstständig entdecken. Dafür wird jedem Einzelnen neben dem Arbeitsblatt auch eine Cäsar-Scheibe zur Verfügung gestellt, womit die Nachricht verschlüsselt wurde. In dieser Phase sind die Schüleraktivität und der Anteil echter Lernzeit zentral. Unter der Beachtung der unterschiedlichen Niveaus stehen gestufte Hilfskärtchen zur Verfügung, sodass selbst entschieden werden kann, wie viel Hilfe zum Verstehen der Verschlüsselungsmethode mit der Cäsar-Scheibe tatsächlich benötigt wird. Durch die Beschreibung der Verschlüsselung mithilfe vorgegebener Schlüsselbegriffe werden die Schüler dazu angehalten die Umgangssprache durch informatische Fachtermini zu ersetzen. Die bereits bekannten Begriffe werden außerdem in den Kontext Cäsar-Verschlüsselung eingebettet und bekommen dadurch eine konkrete Bedeutung. Schnelle Schüler können sich an der Haltestelle bereits über ihre Ergebnisse austauschen.


Name: Aufbaukurs Informatik Klasse:

Cäsars Verschlüsselung auf der Spur

1. Cäsar entwickelte eine eigene Methode, um seine Nachrichten zu verschlüsseln. Mithilfe einer Cäsar-Scheibe verwandelte er einen **Klartext** zu einem **Geheimtext**. Untersuche den Text mithilfe der Cäsar-Scheibe und vervollständige den verschlüsselten Satz. Der **Schlüssel** für diese Nachricht **lautet 2**.

Endlich sind meine Nachrichten sicher!

GPFNKEJ UKPF OGKPG PCEJT□□□□□□ □□□□□□!

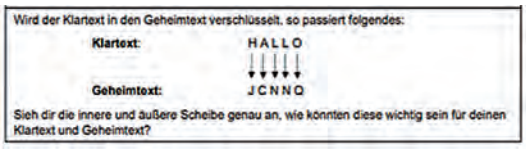
2. Beschreibe Pompeius, wie die Cäsar-Verschlüsselung funktioniert. Wie wird eine Nachricht verschlüsselt? Was ist bei dieser Verschlüsselung der Schlüssel? Verwende folgende Begriffe: **Klartextalphabet (äußere Scheibe) – Geheimtextalphabet (innere Scheibe) – Schlüssel – Buchstabe – ersetzen – Anzahl – Drehungen – links**

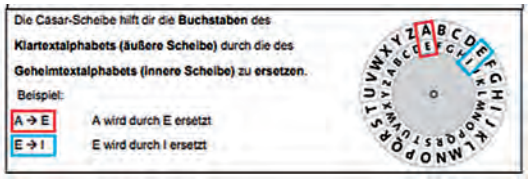
3. Wie lässt sich eine Nachricht wieder entschlüsseln? Entschlüssele dieses Wort mit dem Schlüssel 3. Beschreibe deine Vorgehensweise.

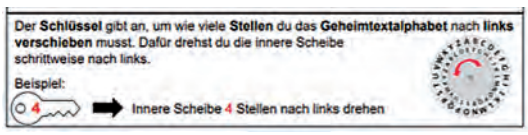
FDHVDU

Sicherung

Die anschließende Sicherungsphase dient der Auswertung, Korrektur und Ergänzung des Erarbeitungsblatts. Die Ergebnisse werden angeglichen, indem einzelne Schüler ihr Arbeitsblatt über einen Visualizer präsentieren und ihre Vorgehensweise mithilfe der Cäsar-Scheibe nochmals audiovisuell darstellen. Dadurch kann gewährleistet werden, dass jeder die Vorgehensweise bei der Verschlüsselungsmethode versteht und inhaltlich gleiche Lösungen verschriftlicht werden.



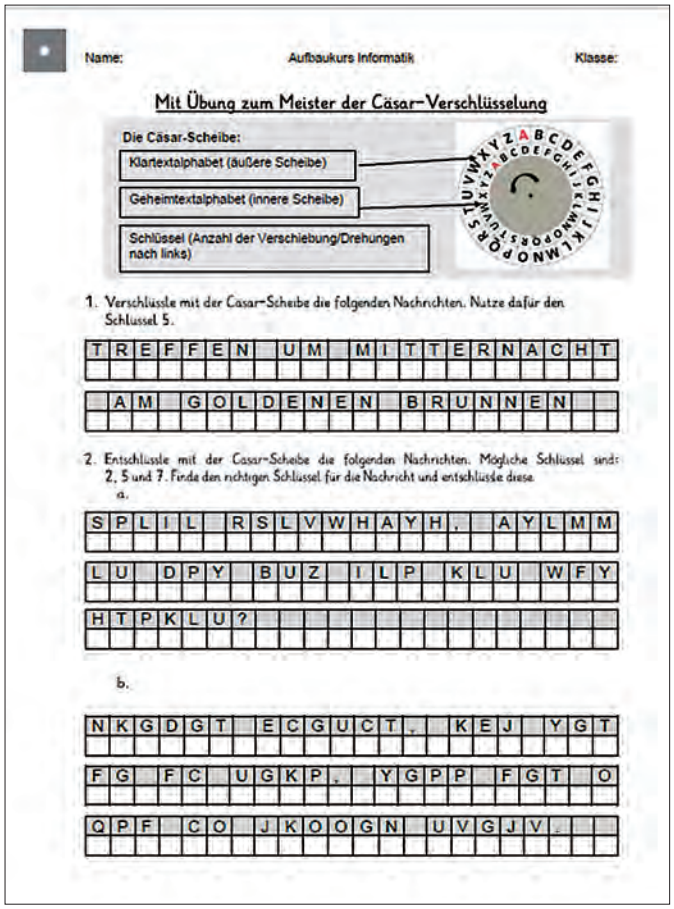




Anwenden und Üben

Übung macht den Meister der Cäsar-Verschlüsselung. In dieser Phase des individuellen Übens soll das neu erlernte Verfahren gefestigt werden. Besonders motivierend sind die Aufgabenstellungen, die als „Rätsel lösen" aufgefasst werden können und dadurch einen spielerischen Charakter erhalten. Während in der Erarbeitungsphase durch unterschiedliche Hilfestellungen differenziert wird, können die Schüler in dieser Phase Arbeitsblätter auswählen, die ihrem Niveau entsprechen. Durch Strukturierungshilfen wird das buchstabenweise Ver- und Entschlüsseln im G-Niveau erleichtert und es hilft dabei Übertragungsfehler zu vermeiden. Die erhöhte Schwierigkeit beim M- bzw. E-Niveau besteht darin, dass auf Umlaute sowie das Entschlüsseln einer Nachricht mithilfe unterschiedlicher Schlüssel geachtet werden muss. Lösungsblätter dienen der Selbstkontrolle. Allerdings können die Schüler die Angemessenheit ihrer Lösungen der Entschlüsselungsaufgaben bereits durch das erreichte Resultat bewerten. Im Fall einer richtigen Lösung entstehen nämlich deutsche Wörter bzw. deutsche Sätze. Zur zusätzlichen Differenzierung der unterschiedlichen Lerntempi ist eine Haltestationsaufgabe eingerichtet. Dort schreiben sich die Schüler im Tandem „geheime" Botschaften, die verschlüsselt sind und vom Tandempartner entschlüsselt werden.

Differenzierte Arbeitsblätter für die Anwendungs- und Übungsphase:



Name: Aufbaukurs Informatik Klasse:

Mit Übung zum Meister der Cäsar-Verschlüsselung

Die Cäsar-Scheibe:

Klartextalphabet (äußere Scheibe)

Geheimtextalphabet (innere Scheibe)

Schlüssel (Anzahl der Verschiebung/Drehungen nach links)

1. Verschlüssle mit der Cäsar-Scheibe die folgenden Nachrichten. Nutze dafür den Schlüssel 5.

TREFFEN UM MITTERNACHT

AM GOLDENEN BRUNNEN

2. Entschlüssle mit der Cäsar-Scheibe die folgenden Nachrichten. Mögliche Schlüssel sind: 2, 5 und 7. Finde den richtigen Schlüssel für die Nachricht und entschlüssle diese.

a.

SPLIL RSLVWHAYH. AYLMM

LU DPY BUZ ILP KLU WFY

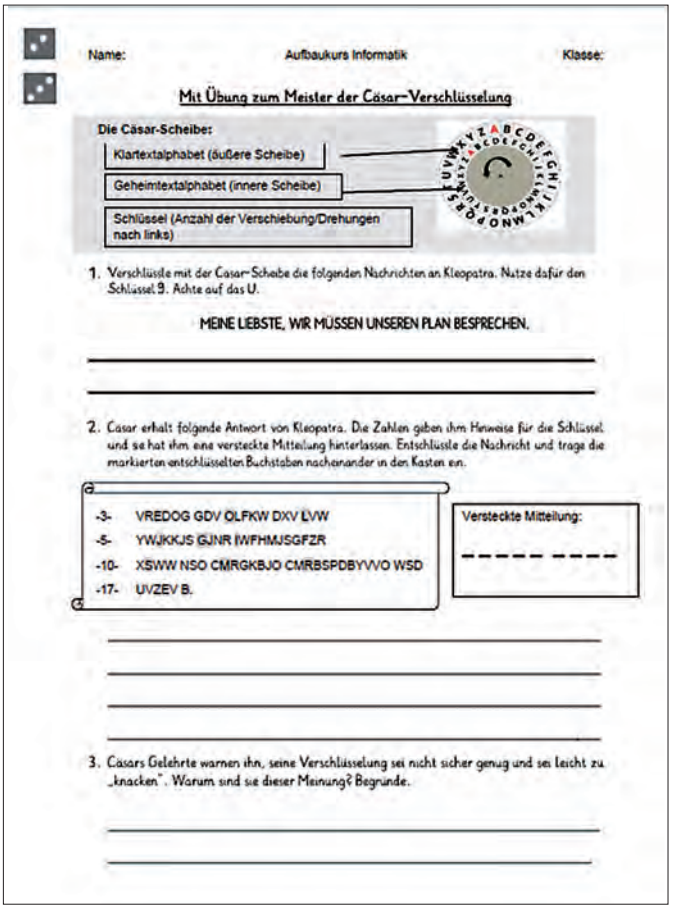
HTPKLU?

b.

NKGDGT ECGUCT. KEJ YGT

FG FC UGKP. YGPP FGT O

QPF CO JKOOGN UVGJV.



Name: Aufbaukurs Informatik Klasse:

Mit Übung zum Meister der Cäsar-Verschlüsselung

Die Cäsar-Scheibe:

Klartextalphabet (äußere Scheibe)

Geheimtextalphabet (innere Scheibe)

Schlüssel (Anzahl der Verschiebung/Drehungen nach links)

1. Verschlüssle mit der Cäsar-Scheibe die folgenden Nachrichten an Kleopatra. Nutze dafür den Schlüssel 9. Achte auf das U.

MEINE LIEBSTE, WIR MÜSSEN UNSEREN PLAN BESPRECHEN.

2. Cäsar erhält folgende Antwort von Kleopatra. Die Zahlen geben ihm Hinweise für die Schlüssel und sie hat ihm eine versteckte Mitteilung hinterlassen. Entschlüssle die Nachricht und trage die markierten entschlüsselten Buchstaben nacheinander in den Kasten ein.

-3- VREDOG GDV OLFKW DXV LVW

-5- YWJKKJS GJNR IWFHMJSGFZR

-10- XSWW NSO CMRGKBJO CMRBSPDBYVVO WSD

-17- UVZEV B.

Versteckte Mitteilung:

3. Cäsars Gelehrte warnen ihn, seine Verschlüsselung sei nicht sicher genug und sei leicht zu „knacken". Warum sind sie dieser Meinung? Begründe.

Konsolidierungsphase

In der letzten Unterrichtsphase soll mithilfe eines Eintrages in das Lerntagebuch zur Einheit „Informationsgesellschaft und Datensicherheit“ der eigene Lernprozess reflektiert werden. Mithilfe vorgegebener Leitfragen wie beispielsweise „Was hast du gelernt?“, „Womit hattest du Schwierigkeiten?“ oder „Was ist für dich besonders wichtig gewesen?“ erstellen die Schüler einen individuellen Eintrag, der ihre Kenntnisse, Wissenslücken und das Thema in ihren Worten zusammenfasst. Für die Lehrkraft sind diese Lerntagebücher ebenfalls sehr aufschlussreich, da die Schülerformulierungen helfen Fehler, Unklarheiten und Wissenslücken zu diagnostizieren, um diese in der nächsten Stunde gegebenenfalls aufzugreifen. Im differenzierten und individualisierten Unterricht hilft es außerdem Verständnisprobleme und Unklarheiten zu erkennen und zu nutzen. Die Stunde wird mit dem Verteilen des „Souvenirs“ beendet. Auf diesem Fächerstreifen sind nochmals die wichtigsten Inhalte der Stunde zusammengefasst. ■

Lerntagebuch in Form eines Logbuchs