INFORMATIK AN GRUNDSCHULEN

– Handreichung –
Sachanalyse, Unterrichtsmaterial, Arbeitsblätter, Kopiervorlagen, Präsentationsmaterial

Projekt: Informatik an Grundschulen (IaG_Z)

Erweiterungsmodul Kryptologie

BERGISCHE UNIVERSITÄT WUPPERTAL

Bergische Universität Wuppertal

Ministerium für
Schule und Bildung
des Landes Nordrhein-Westfalen

INFORMATIK AN GRUNDSCHULEN

»Ich habe ein Geheimnis!«

Handreichung zum Erweiterungsmodul Kryptologie

Bergische Universität Wuppertal
Fachgebiet Didaktik der Informatik

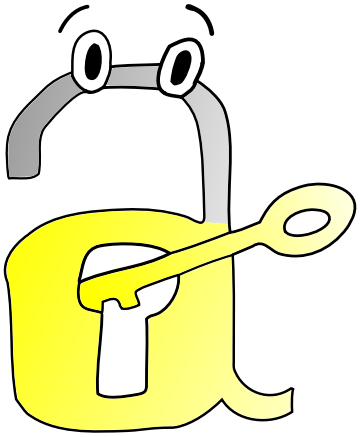
BERGISCHE UNIVERSITÄT WUPPERTAL

DDI Didaktik der Informatik

Ministerium für
Schule und Bildung
des Landes Nordrhein-Westfalen

Federführung
Dorothee Müller & Ludger Humbert

unter Mitarbeit von
Kathrin Haselmeier, Kerstin Grah,
Daniel Losch, Denise Schmitz,
Philipp Züsli, Nora Dürr
und den Lehrkräften unserer Korrespondenzschulen



Stand: 1. August 2019

Inhaltsverzeichnis

Lernausgangslage zur Arbeit mit dem Erweiterungsmodul

Das vorliegende Erweiterungsmodul setzt voraus, dass die Schülerinnen und Schüler sowohl das Grundlagenmodul zur Informatik als auch das Einstiegsmodul zur Kryptologie erfolgreich bewältigt haben. Die Lehrkraft kann damit die dort dokumentierten grundlegenden Kompetenzen der Schülerinnen und Schüler als Lernvoraussetzung ansehen, sollte sich allerdings im konkreten Unterricht vergewissern, dass die Lernausgangslage bezüglich der Kompetenzen auch als erreicht betrachtet werden kann.

1 Aufbau des Einstiegsmoduls Kryptologie

In der Handreichung zum Einstiegsmodul Kryptologie finden sich bereits die grundlegenden fachdidaktischen Hinweise zur Umsetzung sowohl von Informatikinhalten als auch von Methoden der Informatik. Dort werden die Phänomenbereiche der Informatik sowie der informatische Modellierungskreislauf als fachdidaktische Grundlagen ausführlich dargestellt.
Am Beispiel der Kryptologie wird ein inhaltliches Themenfeld aufgeschlossen. Hierbei wird zu jedem Teilbereich je ein kurzer Sachinput vorgestellt, der durch praktische Umsetzungsvorschläge und Kopiervorlagen für die Schüler- und Lehrerhand ergänzt wird. Dem Modul vorangestellt ist eine beispielhafte Einstiegsstunde zu Informatik in der Lebenswirklichkeit. Da die letzte Unterrichtseinheit »Caesar-Verschlüsselung« des Einstiegsmodul als Ausgangspunkt für das nun vorliegende Erweiterungsmodul dient, wird an dieser Stelle auf eine erneute Ausführung zu den Grundlagen verzichtet. Stattdessen wird die Struktur aufgegriffen und um die relevanten Aspekte aus der Erweiterung ergänzt.

2 Aufbau des Erweiterungsmoduls Kryptologie

Das Erweiterungsmodul zur Kryptologie umfasst drei Unterrichts-Teilmodule. Dabei knüpft die Erweiterung in jedem Teilmodul an die letzte Unterrichtseinheit »Caesar-Verschlüsselung« des Ursprungsmoduls Kryptologie an und führt dieses Verfahren weiter. Die im Ursprungsmodul eingesetzten Caesar-Scheiben kommen in den Teilmodulen 1 und 2 erneut zum Einsatz.
→ Die Caesar-Scheiben sind als Bastelvorlage unter *Weiteres_Material/Caesar-Scheibe* zu finden.

- Teilmodul 1 wird analog zum Einstiegsmodul ohne Informatiksystem umgesetzt, zwei weitere Teilmodule gestalten den Übergang von Informatik ohne Informatiksystem (Phänomenbereich 3) zu Informatik mit Informatiksystem (Phänomenbereich 1 oder 2).
- Für Teilmodul 2 werden neben den analogen Caesar-Scheiben des Ursprungsmoduls auch mehrere *Calliope mini* benötigt, auf welchen das entsprechende Programm bereits vorinstalliert werden muss.
  - → Das Programm ist zu finden unter *Calliope/Caesar-Programm*.
  - → Unter *Calliope/Calliope-Vorbereitung* findet sich eine Anleitung, wie das Programm auf den *Calliope mini* geladen wird.

  Der Einsatz des Informatiksystems *Calliope mini* kann so auch in Klassenzimmern erfolgen, die nicht an das Internet angebunden sind.
- In Teilmodul 3 wird ausschließlich auf einer Website gearbeitet, das zu nutzende System muss daher mit dem Internet vernetzt sein. Analoge Materialien entfallen für das Teilmodul 3 vollständig.

3 Teilmodule

Die drei Teilmodule können einzeln, aber auch in den folgenden Kombinationen sinnvoll im Unterricht eingesetzt werden:

- Teilmodule 1,2
- Teilmodule 1,3
- Teilmodule 1,2,3

Durch diese Wahlmöglichkeit wird den Schulen unabhängig von ihren technischen Ausstattungen ermöglicht, das Erweiterungsmodul zur Kryptologie einzusetzen, die *Kryptoanalyse* als einen Teil der Kryptologie kennenzulernen und mit Informatiksystemen umzusetzen. Werden mehrere oder alle drei Teilmodule eingesetzt, können zudem die Beziehungen der drei Phänomenbereiche untereinander in besonderem Maße ins Bewusstsein der Schülerinnen und Schüler gehoben werden.

4 Szenario

Ein geheimer Treffpunkt soll mit Zeit und Ort den berechtigten Mitgliedern des Caesar-Clubs mitgeteilt werden. Nur bei Angabe des richtigen Schlüssels kann die Nachricht entschlüsselt gelesen werden.

4.1 Teilmodul 1 – ohne Informatiksystem, Phänomenbereich 3

Die Schülerinnen und Schüler bekommen erneut einen Brief von Bob (→ AB-V1a: Brief von Bob – Caesar ohne Informatiksystem), der ihnen den neuen Arbeitsauftrag ankündigt und die Verbindung schafft zur Unterrichtseinheit 4 des Einstiegsmoduls.
Auf einem Arbeitsblatt erhalten die Schülerinnen und Schüler eine verschlüsselte Nachricht: beispielsweise Zeit und Treffpunkt für ein Agententreffen, z. B. »Schulhof zehn Uhr Bob«. Jedes Kind ermittelt mit der Caesarscheibe (→ aus dem Ursprungsmodul, Vorlage unter *Weiteres_Material/Caesar-Scheibe*) den Schlüssel anhand der Information, dass die Nachricht mit Bob unterschrieben wurde. Es nennt den Schlüssel einer »Kontaktperson« (Lehrkraft, Zweitkraft oder Schülerin bzw. Schüler aus der Parallelklasse). Bei richtigem Schlüssel wird die entschlüsselte Nachricht mitgeteilt, ansonsten wird die Auskunft verweigert und ein neuer, verschlüsselter Text ausgegeben. Die Lösung der Aufgabe lässt pro Versuch nur eine Antwort zu, jedoch können insgesamt drei Versuche mit unterschiedlichen Texten nach demselben Prinzip unternommen werden.

4.2 Teilmodul 2 – Phänomenbereich 2

Auch in Teilmodul 2 bekommen die Schülerinnen und Schüler zu Beginn einen Brief von Bob (→ AB-V2a: Brief von Bob – Caesar mit dem Calliope mini). Der Bezug zum Informatiksystem wird im begleitenden Text hergestellt: Die Kontaktperson kann durch ein Informatiksystem, den *Calliope mini* ersetzt werden. Zur Vorbereitung auf die Stunde müssen die *Calliope Mini* mit dem entsprechenden Programm ausgestattet werden.

→ Das benötigte Programm finden Sie unter *Calliope/Caesar-Programm*
→ Installationsanleitung: *Calliope/Calliope-Vorbereitung*

Auf dem Arbeitsblatt zu Teilmodul 2 steht ebenfalls eine verschlüsselte Nachricht. Das Kind ermittelt aus dem Text anhand der Information, dass die Nachricht mit Bob unterschrieben wurde, und mit Hilfe der Caesarscheibe (aus dem Ursprungsmodul → Vorlage unter *Weiteres_Material/Caesar-Scheibe*) den Schlüssel. Zusätzlich sind auf dem Arbeitsblatt die nötigen Schritte vermerkt, wie der Einsatz des *Calliope mini* erfolgen soll. Das Kind gibt den

Schlüssel anhand der Anleitung in den *Calliope mini* ein. Bei richtigem Schlüssel wird ein lachender Smiley angezeigt und die entschlüsselte Nachricht wird mehrmals als durchlaufendes Textbanner ausgegeben. Handelt es sich um einen Fehlversuch, wird ein trauriger Smiley angezeigt und das Kind bekommt auf von dem *Calliope mini* ein neues Symbol mitgeteilt für eine neue, verschlüsselte Nachricht. Es gibt insgesamt nur drei Versuche.
Für die Einführung der Calliope und ihre Erprobung durch die Schülerinnen und Schüler sind zusätzliche Unterrichtsstunden empfehlenswert. Ideal ist der Einsatz von Teilmodul 2, wenn die Schülerinnen und Schüler bereits mit dem Calliope mini gearbeitet haben.

4.3 Teilmodul 3 – Phänomenbereich 1

Teilmodul 3 beginnt ebenfalls mit einem Brief von Bob. Dieser befindet sich als Eingangstext auf der Website → `https://ddi.uni-wuppertal.de/website/iagz/` (verkürzte Adresse → `http://uni-w.de/1qs`). Nach dem Lesen des Briefes gelangt die Schülerin / der Schüler auf die Seite mit der Entschlüsselungsaufgabe. Diese Seite enthält:

- die Entschlüsselungsanleitung (linke Spalte)
- den verschlüsselten Text (oberhalb der Caesar-Scheibe)
- die virtuelle, interaktive Caesar-Scheibe (Mitte)
- die Tipps zur Entschlüsselung (rechte Spalte)
- das Eingabefeld für den ermittelten Schlüssel (unterhalb der Caesar-Scheibe)

Nach einem falschen Lösungsversuch erscheint eine Meldung, dass dies der falsche Schlüssel war und die Möglichkeit, eine neue verschlüsselte Nachricht zu erhalten.
Als Reaktion des Informatiksystems auf die richtige Lösung werden die folgenden Ausgaben generiert:

- die Ausgabe der entschlüsselten Nachricht (unterhalb des Eingabefensters)
- ein abschließender Brief von Alice

5 Grundlegende Sachinformation zum Erweiterungsmodul Kryptologie

Der römische Feldherr Julius Caesar (100 bis 44 v. Chr.) verschlüsselte seine Nachrichten, indem er jeden Buchstaben durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzte. Diese Anzahl der Stellen heißt *Caesar-Schlüssel*, das Verfahren nennt sich *Caesar-Chiffre* bzw. *Caesar-Verschlüsselung*.
Man spricht bei dieser Art der Verschlüsselung von einer *mono-alphabetischen Substitution*. Mono-alphabetisch bedeutet hierbei, dass nur ein einziges, festgelegtes Alphabet zum Einsatz kommt. Als Substitution wird dieses Verfahren bezeichnet, da die einzelnen Zeichen durch andere Zeichen ausgetauscht bzw. ersetzt werden (lat.: »substituere«). Praktisch lässt sich das Verfahren, wie dargestellt, durch zwei sich teilweise überlagernde Scheiben realisieren, die gegeneinander gedreht werden können.
Während im Einstiegsmodul Kryptologie in der Unterrichteinheit zur Caesar-Verschlüsselung der verwendete Schlüssel zwischen zwei Schülerinnen und Schüler vereinbart wurde bzw. durch Ausprobieren herausgefunden werden konnte, sind im Erweiterungsmodul keine Vereinbarungen getroffen und der verwendete Schlüssel muss durch methodische Überlegungen zum eingesetzten Caesar-Verfahren im ersten Versuch richtig ermittelt werden. Dazu ist es nötig, dass die Schülerinnen und Schüler Rückschlüsse aus dem Klarnamen »Bob« des Absenders und die verschlüsselte Unterschrift unter dem verschlüsselten Aufgabentext auf den Schlüssel ziehen und so die richtige Verschiebung ermitteln.
Die methodische Untersuchung einer verschlüsselten Botschaft mit dem Ziel, die Nachricht zu entschlüsseln, nennt sich *Kryptoanalyse*.

6 Zu erwerbende Kompetenzen im Rahmen des Erweiterungsmoduls Kryptologie

Kompetenzen zu allen Teilmodulen

Die Schülerinnen und Schüler …

- gehen methodisch vor, um eine verschlüsselte Botschaft zu entschlüsseln (Kryptoanalyse).
- nutzen Vereinbarungen zur Übermittlung von Daten.
- realisieren und testen algorithmische Handlungsvorschriften.
- bewerten die für die Problemstellung gefundenen Lösungen bezüglich des angestrebten Zwecks.
- nennen und beschreiben Lösungsstrategien im Rahmen des gewählten kryptologischen Verfahrens.

Zusätzliche Kompetenzen zu Teilmodulen 2 und 3

Die Schülerinnen und Schüler …

1. interagieren zielgerichtet mit Informatiksystemen.
2. steuern ihre Dateneingabe gemäß des verwendeten Systems.
3. nutzen die Möglichkeiten des verwendeten Systems im dargestellten Kontext.

7 Allgemeine Hinweise zu Möglichkeiten der Differenzierung

Das vorliegende Modul versteht sich als *Planungshilfe* für Ihren Unterricht. Dies bedeutet, es steht Ihnen frei, qualitativ und quantitativ zu differenzieren, um die Lerninhalte und den Verlauf des Unterrichts den Bedürfnissen Ihrer Lerngruppe anzupassen. Nachfolgend skizzieren wir Ihnen daher mögliche Vorgehensweisen zur Differenzierung.

- Treffen Sie eine Auswahl der Teilmodule nicht nur hinsichtlich der technischen Möglichkeiten, sondern auch in Bezug auf Ihre Lerngruppe. Setzen Sie möglicherweise unterschiedliche Teilmodule in der gleichen Lerngruppe ein oder führen Sie die Teilmodule als Stationenarbeit durch.
- Passen Sie die Anzahl der Lösungsversuche an.
- Begrenzen Sie die Zeit, die für die Lösung zur Verfügung steht.
- Bieten Sie Ihren Schülerinnen und Schüler Hilfe mit den Tippkarten (bzw. Tippfenstern/Website) an.
- Bilden Sie Experten/Expertinnen für das eingesetzte System aus oder bestimmen im Unterrichtsverlauf Experten, die andere Kinder unterstützen können.

8 Materialübersicht:

8.1 Teilmodul 1

- Arbeitsblatt AB-V1a: Brief von Bob – Caesar ohne Informatiksystem
- Arbeitsblatt AB-V1b: Brief von Alice – Caesar ohne Informatiksystem
- Arbeitsblatt AB-V1c: Willkommen im Caesar-Club!
- Arbeitsblatt AB-V1d: Lösungsblatt für die verschlüsselten Nachrichten
- Arbeitsblatt AB-V1e: Caesar-Club – Der Text für den ersten Versuch
- Arbeitsblatt AB-V1f: Caesar-Club – Der Text für den zweiten Versuch
- Arbeitsblatt AB-V1g: Caesar-Club – Der Text für den dritten Versuch
- Arbeitsblatt AB-V1h: Caesar-Club – Zusatz (Brief von Alice)
- Arbeitsblätter AB-V1h-j: Tipp-Karten
- Caesar-Scheiben aus der Unterrichtseinheit 4 aus dem Einstiegsmodul zu Kryptologie (zu finden unter *Weiteres_Material/Caesar-Scheibe*)

8.2 Teilmodul 2

- Arbeitsblatt AB-V2a: Brief von Bob – Caesar mit dem *Calliope mini*
- Arbeitsblatt AB-V2b: Brief von Alice – Caesar mit dem *Calliope mini*
- Arbeitsblatt AB-V2c: Willkommen im Caesar-Club mit dem *Calliope mini*
- Caesar-Scheiben aus der Unterrichtseinheit 4 aus dem Einstiegsmodul zu Kryptologie (zu finden hier unter *Weiteres_Material/Caesar-Scheibe*)

- Arbeitsblätter AB-V2d-f: Tipp-Karten
- Klassensatz Calliope mit aufgespieltem Programm
- Anleitung und Programm zu finden unter *Calliope/Calliope-Vorbereitung* und *Calliope/Caesar-Programm*.

8.3 Teilmodul 3

- Zugang zu einem internetfähigen Informatiksystem,
  Website → `https://ddi.uni-wuppertal.de/website/iagz/`
  (verkürzte Adresse → `http://uni-w.de/1qs`) aufrufbar

9 Abbildungen Unterrichtsmaterial – Erweiterungsmodul Kryptologie

9.1 Teilmodul 1 – alphabetisch

AB-V1a: Brief von Bob – Caesar ohne Informatiksystem

Hallo Kinder,

hier schreibt euch noch einmal Bob.

Ihr wollt wissen, wie es mit Alice und mir weitergegangen ist?
Nun, das war so: Mit den Caesar-Scheiben konnten wir uns zu zweit schon ganz gut Botschaften schicken. Jetzt haben wir auch unsere Freunde eingeweiht, wir sind nun der »Caesar-Club«! Cool, oder?

Eve findet das jedenfalls so interessant, dass sie unsere Treffen belauschen möchte.

Wir haben uns also etwas ausgedacht, wie wir uns mit Caesars Hilfe verabreden können, ohne dass Eve den Treffpunkt herausfinden kann.

Weil nun der erste Entschlüsselungsversuch klappen muss, muss man schon ein ziemlicher Caesar-Experte sein, um die Botschaft zu entschlüsseln! Aber schaut selbst!

Ich bin gespannt, was ihr davon haltet!

Viel Spaß

euer Bob

AB-V1b: Brief von Alice – Caesar ohne Informatiksystem

Hallo Kinder,
ich bin's, Alice.

Cool, dass ihr unseren Treffpunkt herausgefunden habt!

Dafür musstet ihr die verschlüsselten Botschaften entschlüsseln – wie richtige Code-Knacker!
Euch macht so schnell keiner mehr etwas vor!

Es gibt übrigens einen Namen für das, was ihr geleistet habt: Ihr habt eine *Kryptoanalyse* durchgeführt. Klingt ganz schön kompliziert, oder?

Kryptoanalyse bedeutet, dass ihr euch genau überlegen musstet, wie ihr die Nachricht lesen könnt, ohne den Schlüssel zu kennen.

Da kann doch eigentlich gar nichts mehr schief gehen…

Viele Grüße an euch, die neuen Experten,

eure Alice

AB-V1c: Willkommen im Caesar-Club!

Den Schlüssel kennst du nicht. Aber wenn du es schaffst, im ersten Versuch den richtigen Caesar-Code einzustellen, kannst du die Nachricht trotzdem entschlüsseln! Versuche, in der Botschaft einen Hinweis zu bekommen, welche Zahl der Schlüssel ist.

Wenn du die Zahl kennst, zeigst du sie vor.

Ist die Zahl richtig, versuchst du, den Text zu übersetzen.

Ist sie falsch, musst du es mit einem anderen Text noch einmal versuchen!

AB-V1d: Caesar-Club – Lösungen für die Texte:

Text zum ersten Versuch:
ZWQ CAFVWJ,
OAJ LJWXXWF MFK FSUZ VWJ KWUZKLWF KLMFVW ZAFLWJ VWE KUZMDZGX!
WMWJ TGT

Lösung zum ersten Versuch, Schlüssel 18:
Hey Kinder,
wir treffen uns nach der sechsten Stunde hinten auf dem Schulhof!
Euer Bob

Text zum zweiten Versuch:
YZNS PTYXLW: SLWWZ,
YLNS OPX FYEPCCTNSE RPSED STYEPC OPY DNSFWSZQ!
OPTY QCPFYO MZM

Lösung zum zweiten Versuch, Schlüssel 11:
Noch einmal: Hallo,
nach dem Unterricht gehts hinter den Schulhof!
Dein Freund Bob

Text zum dritten Versuch:
RMBHB STIXXB MA JMABQUUB:
CVAMZ BZMNNMV QAB VIKP AKPCTAKPTCAA PQVBMZU AKPCTPWN!
DQMTM OZCMAAM JWJ

Lösung zum dritten Versuch, Schlüssel 8:
Jetzt klappt es bestimmt:
Unser Treffpunkt ist nach Schulschluss hinterm Schulhof!
Viele Gruesse Bob

Text zum Zusatz:
WPAAD OJHPBBTC!
XRW LTGST PJRW SP HTXC! XRW UGTJT BXRW PJU TJRW!
TJGT PAXRT

Lösung zum Zusatz, Schlüssel 15:
Hallo Zusammen!
Ich werde auch da sein! Ich freue mich auf euch! Eure Alice

AB-V1e: Caesar-Club – Der Text für den ersten Versuch:

ZWQ CAFVWJ,

OAJ LJWXXWF MFK FSUZ VWJ KWUZKLWF KLMFVW ZAFLWJ VWE KUZMDZGX!

WMWJ TGT

AB-V1f: Caesar-Club – Der Text für den zweiten Versuch:

YZNS PTYXLW: SLWWZ,

YLNS OPX FYEPCCTNSE RPSED STYEPC OPY DNSFWSZQ!

OPTY QCPFYO MZM

AB-V1g: Caesar-Club – Der Text für den dritten Versuch:

RMBHB STIXXB MA JMABQUUB:

CVAMZ BZMNNMV QAB VIKP AKPCTAKPTCAA PQVBMZU AKPCTPWN!

DQMTM OZCMAAM JWJ

AB-V1h: Caesar-Club – Zusatz:

WPAAD OJHPBBTC!

XRW LTGST PJRW SP HTXC! XRW UGTJT BXRW PJU TJRW!

TJGT PAXRT

AB-V1i: Erster Tipp – Caesar-Club

Du hast Post von Bob bekommen!

AB-V1j: Zweiter Tipp – Caesar-Club

Schaue dir die Unterschrift an!

AB-V1k: Dritter Tipp – Caesar-Club

Die Geheimbuchstaben findest du
auf der roten Scheibe.
Gesucht sind die grünen Buchstaben.

9.2 Teilmodul 2 – alphabetisch

AB-V2a: Brief von Bob – Caesar mit dem *Calliope mini*

Hallo Kinder,

hier schreibt euch noch einmal Bob.

Ihr wollt wissen, wie es mit Alice und mir weitergegangen ist?
Nun, das war so: Mit den Caesar-Scheiben konnten wir uns zu zweit schon ganz gut Botschaften schicken. Jetzt haben wir auch unsere Freunde eingeweiht, wir sind nun der »Caesar-Club«! Cool, oder?

Eve findet das jedenfalls so interessant, dass sie unsere Treffen belauschen möchte.

Wir haben uns also etwas ausgedacht, wie wir uns mit Caesars Hilfe verabreden können, ohne dass Eve den Treffpunkt herausfinden kann.
Wir benutzen den *Calliope mini*, einen Minicontroller, für unsere Verabredungen! Auf dem Arbeitsblatt bekommst du dazu eine Erklärung.

Weil nun der erste Entschlüsselungsversuch klappen muss, muss man schon ein ziemlicher Caesar-Experte sein, um die Botschaft zu entschlüsseln! Aber schaut selbst!

Ich bin gespannt, was ihr davon haltet!

Viel Spaß

euer Bob

AB-V2b: Brief von Alice – Caesar mit dem *Calliope mini*

Hallo Kinder,
ich bin's, Alice.

Cool, dass ihr unseren Treffpunkt herausgefunden habt!

Dafür musstet ihr die verschlüsselten Botschaften entschlüsseln – wie richtige Code-Knacker!
Euch macht so schnell keiner mehr etwas vor!

Es gibt übrigens einen Namen für das, was ihr geleistet habt: Ihr habt eine *Kryptoanalyse* durchgeführt. Klingt ganz schön kompliziert, oder?

Kryptoanalyse bedeutet, dass ihr euch genau überlegen musstet, wie ihr die Nachricht lesen könnt, ohne den Schlüssel zu kennen.

Außerdem habt ihr den *Calliope mini* kennengelernt – der ist ganz schön cool, oder? Mit dem *Calliope mini* kann man noch viel mehr spannende Projekte machen! Vielleicht könnt ihr ja noch ein wenig damit ausprobieren!?

Krypto-Experten seid ihr nun auf jeden Fall!
Viele Grüße

eure Alice

AB-V2c: Willkommen im Caesar-Club mit dem *Calliope Mini*!

Deine Aufgabe ist es, den richtigen Caesar-Code *durch Überlegen* herauszufinden. Dafür bekommst du von dem *Calliope mini* gleich ein Symbol zugeteilt. Dieses Symbol findest du unten wieder. Daneben steht als verschlüsselter Text eine Nachricht von **Bob** mit dem richtigen Treffpunkt.

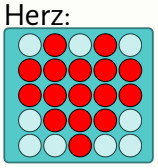
Versuche, in der Botschaft einen Hinweis zu bekommen, welche Zahl der Schlüssel ist.

Diesen Schlüssel musst du dir merken und in den *Calliope mini* eingeben. Wenn du richtig überlegt hast, siehst du die richtige Botschaft. Diese kannst du dir in dem weißen Kasten, unten auf dieser Seite, aufschreiben.
Wenn du den Schlüssel falsch eingibst, bekommst du ein neues Symbol für den nächsten Versuch.

Wenn du dreimal daneben gelegen hast, kannst du dir einen Tip abholen und noch einmal starten!

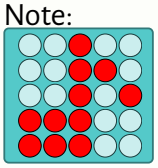
Eine Anleitung für den *Calliope mini* findest du auf dem zweiten Arbeitsblatt.
Alles klar?

Herz:



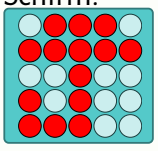
IMRKERK WGLYPLSJ ZMIVDILR YLV FSF

Note:



ERNAINQW DQA BLQDUQXO NRWPJWP KXK

Schirm:



EOTGXTAR QUZSMZS HUQDLQTZ GTD NAN

Willkommen im Caesar-Club! (AB2)

Du weißt, was deine Aufgabe ist? Wenn nicht, dann lies zuerst das andere Arbeitsblatt.
Dann wird es jetzt ernst: Nimm dir nun den *Calliope mini*.

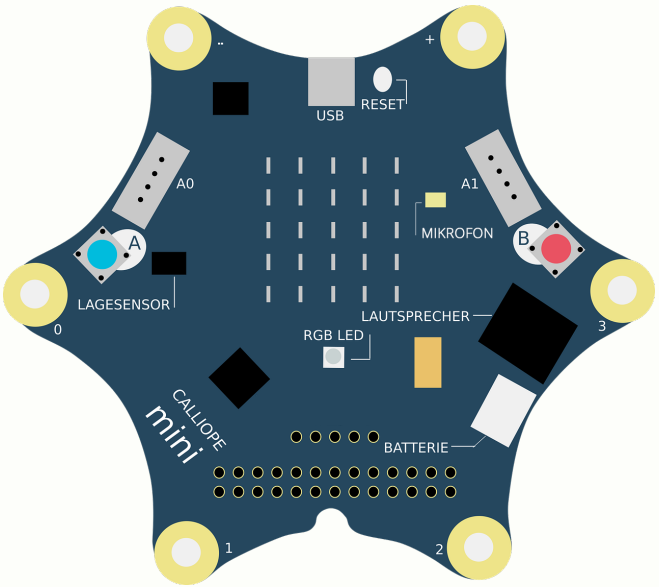
1. Nimm den *Calliope mini* in eine Hand und drehe ihn einige Male um. Auf dem LED-Feld in der Mitte erscheint nun ein Symbol.
2. Suche das Symbol auf dem anderen Arbeitsblatt und versuche, den geheimen Schlüssel herauszufinden. Dabei hilft dir die Caesar-Scheibe.
3. Mit den Tasten A und B auf dem *Calliope mini* kannst du den Schlüssel eingeben, den du herausgefunden hast. Der Schlüssel wird dir angezeigt, sobald du anfängst, ihn einzugeben.

   Drückst du die blaue Taste **A**, zählst du hoch.

   Drückst du die rote Taste **B**, zählst du runter.
4. Wenn du die richtige Zahl eingestellt hast, drückst du gleichzeitig **A und B**.
   Der *Calliope mini* nimmt deine Antwort nun an.

Ist die Zahl richtig, siehst du den fröhlichen Smiley und bekommst den Treffpunkt genannt. Pass gut auf, damit du keinen Buchstaben verpasst und halte den Treffpunkt geheim! Eve hat ihre Ohren überall …
Ist die Zahl falsch, schüttelst du den *Calliope mini* wieder und hast ein anderes Symbol für den nächsten Versuch.
Wenn du dreimal daneben liegst, fängt der *Calliope mini* an zu blinken und du kannst dir einen Tipp abholen, um wieder ganz am Anfang zu starten.
(Deine Lehrerin oder dein Lehrer stellen den *Calliope mini* dann so ein, dass du wieder neu starten kannst.)

Hast du alles verstanden? Dann kann es ja losgehen!



AB-V2d: Erster Tip für den *Calliope Mini*

Du hast Post von Bob bekommen!

AB-V2e: Zweiter Tip für den *Calliope mini*

Schaue dir die Unterschrift an!

AB-V2e: Dritter Tip für den *Calliope Mini*

Der Schlüssel war falsch?
Dann kontrolliere, ob der grüne Anfangsbuchstabe »B« von »Bob« neben dem ersten roten Buchstaben von Bobs geheimer Unterschrift auf der Nachricht steht.
Im gelben Feld erscheint nun der richtige Schlüssel!

9.3 Teilmodul 3

Brief von Bob

Hallo Kinder,
hier schreibt euch noch einmal Bob.

Ihr wollt wissen, wie es mit Alice und mir weitergegangen ist?
Nun, das war so: Mit den Caesar-Scheiben konnten wir uns zu zweit schon ganz gut Botschaften schicken. Jetzt haben wir auch unsere Freunde eingeweiht, wir sind nun der »Caesar-Club«! Cool, oder?

Eve findet das jedenfalls so interessant, dass sie unsere Treffen belauschen möchte.
Wir haben uns also etwas ausgedacht, wie wir uns mit Caesars Hilfe verabreden können, ohne dass Alice den Treffpunkt herausfinden kann.
Wir benutzen das Internet!

Hier auf dieser Website findet ihr eine virtuelle Caesar-Scheibe. Darüber steht eine verschlüsselte Botschaft von mir. Wenn ihr die Caesar-Scheibe richtig einstellt, wird die Botschaft entschlüsselt.
Rechts neben der Scheibe findet ihr einige Tips, wenn ihr nicht weiterkommt!

Weil nun der erste Entschlüsselungsversuch klappen muss, muss man schon ein ziemlicher Caesar-Experte sein, um die Botschaft zu entschlüsseln! Aber schaut selbst!

Ich bin gespannt, was ihr davon haltet!

Viel Spaß,

euer Bob

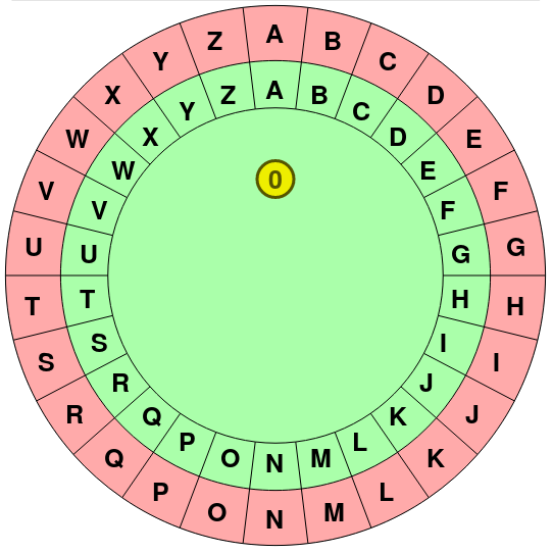
So kannst du mit dieser Internetseite arbeiten:

Du kannst die Scheibe drehen, indem du auf die blauen Felder mit der Hand klickst. Nun erscheint in dem gelben Kreis eine Zahl. Das ist der Schlüssel, den du eingeben musst!
Um den Schlüssel eingeben zu können, musst du das Eingabefeld erst anklicken. Die Zahl gibst du dann über die Tastatur ein und klickst danach auf *Entschlüsseln*.

Achtung: Auf der roten Scheibe findest du die Buchstaben der geheimen Nachricht von Bob. Auf der grünen Scheibe sind die Buchstaben der entschlüsselten Nachricht.

Bobs geheime Nachricht an dich:

UNYYB XVAQRE! JVE GERSSRA HAF HZ ARHA HUE NA QRE RVFQVRYR. OBO



👈 Linksrum drehen | Rechtsrum drehen 👉

Gib hier den Schlüssel ein!

Entschlüsseln🔓

Klicke hier für einen ersten Tipp!

Klicke hier für einen zweiten Tipp!

Klicke hier für einen dritten Tipp!

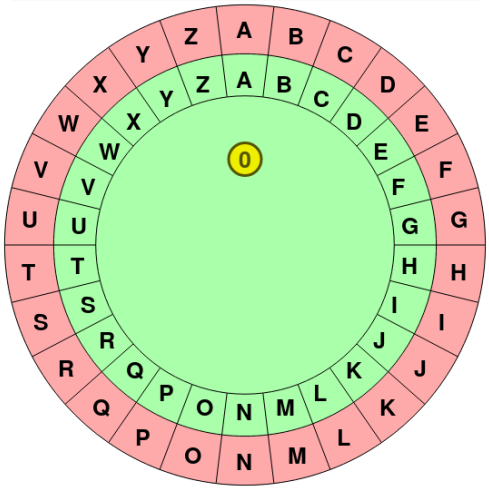
So kannst du mit dieser Internetseite arbeiten:

Du kannst die Scheibe drehen, indem du auf die blauen Felder mit der Hand klickst. Nun erscheint in dem gelben Kreis eine Zahl. Das ist der Schlüssel, den du eingeben musst!
Um den Schlüssel eingeben zu können, musst du das Eingabefeld erst anklicken. Die Zahl gibst du dann über die Tastatur ein und klickst danach auf *Entschlüsseln*.

Achtung: Auf der roten Scheibe findest du die Buchstaben der geheimen Nachricht von Bob. Auf der grünen Scheibe sind die Buchstaben der entschlüsselten Nachricht.

Bobs geheime Nachricht an dich:

FYJJM IGLBCP! UGP RPCDDCL SLQ KMPECL KGRRYE YSD BCK QAFSJFMD. ZMZ



👈 Linksrum drehen | Rechtsrum drehen 👉

Gib hier den Schlüssel ein!

Entschlüsseln🔓

Bob hat dir geschrieben!

Schau dir die Unterschrift an!

Die Geheimbuchstaben findest du auf der roten Scheibe. Gesucht sind die Buchstaben auf der grünen Scheibe.

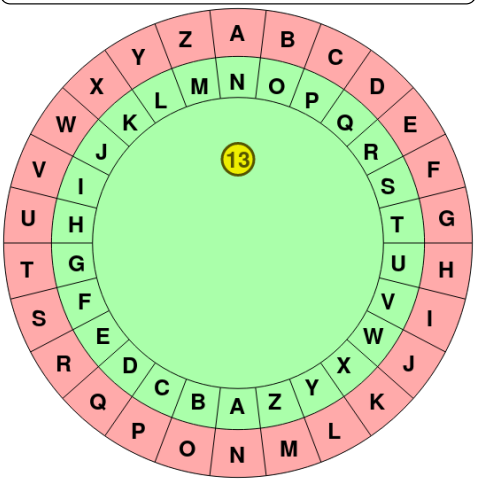
So kannst du mit dieser Internetseite arbeiten:

Du kannst die Scheibe drehen, indem du auf die blauen Felder mit der Hand klickst. Nun erscheint in dem gelben Kreis eine Zahl. Das ist der Schlüssel, den du eingeben musst!
Um den Schlüssel eingeben zu können, musst du das Eingabefeld erst anklicken. Die Zahl gibst du dann über die Tastatur ein und klickst danach auf *Entschlüsseln*.

Achtung: Auf der roten Scheibe findest du die Buchstaben der geheimen Nachricht von Bob. Auf der grünen Scheibe sind die Buchstaben der entschlüsselten Nachricht.

Bobs geheime Nachricht an dich:

UNYYB XVAQRE! JVE GERSSRA HAF HZ ARHA HUE NA QRE RVFQVRYR. OBO



Klicke hier für einen ersten Tipp!

Klicke hier für einen zweiten Tipp!

Klicke hier für einen dritten Tipp!

Linksrum drehen | **Rechtsrum drehen**

13

Entschlüsseln

HALLO KINDER! WIR TREFFEN UNS UM NEUN UHR AN DER EISDIELE. BOB

Brief von Alice

Hallo Kinder,
ich bin's, Alice.

Cool, dass ihr unseren Treffpunkt herausgefunden habt!

Dafür musstet ihr die verschlüsselten Botschaften entschlüsseln und eine virtuelle Caesar-Scheibe benutzen – wie richtige Code-Knacker! Euch macht so schnell keiner mehr etwas vor!

Es gibt übrigens einen Namen für das, was ihr geleistet habt: Ihr habt eine *Kryptoanalyse* durchgeführt. Klingt ganz schön kompliziert, oder?

Kryptoanalyse bedeutet, dass ihr euch genau überlegen musstet, wie ihr die Nachricht lesen könnt, ohne den Schlüssel zu kennen.

So wie es aussieht, habt ihr es auch geschafft, eure Lösung auf der Website richtig einzugeben, cool!

Viele Grüße an euch, die neuen Experten,

eure Alice