

Codeknacker – Heft



Auf den Spuren verschlüsselter Informationen und geheimer Codes

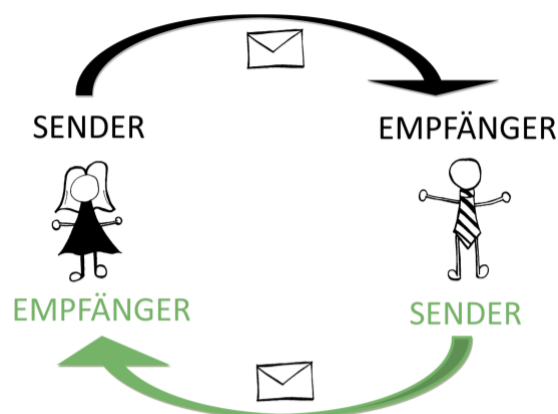
von _____

Herzlich willkommen zum digitalen Lernangebot der Prima Lernwerkstatt zum Thema „Top Secret“. Heute gehen wir gemeinsam auf die Spuren verschlüsselter Informationen und geheimer Codes.

Die Wissenschaft der Ver- und Entschlüsselung von Botschaften nennt man Kryptologie. Dieser Fachbegriff stammt von den griechischen Worten „kryptos“ und „logos“ ab. Das Wort „kryptos“ steht für das deutsche Wort „geheim“ und „logos“ bedeutet „Wort“. Umgangssprachlich sprechen wir auch von der „Kryptographie“. Genau genommen bezieht sich dieser Fachbegriff jedoch nur auf die Ver- und nicht die Entschlüsselung eines Textes.

Was bedeutet es jedoch genau einen Text zu ver- bzw. entschlüsseln?

Dazu müssen wir zunächst einmal wissen, dass es zur Übermittlung einer Nachricht, egal ob dies in Briefform oder elektronisch geschieht, einen Sender und einen Empfänger gibt.



Stell dir einmal vor, du möchtest einen Brief an einen Freund oder eine Freundin verschicken. Da du den Brief schreibst und losschickst, bist du der/die Sender/in und dein/e Freund/in der/die Empfänger/in des Briefs. Antwortet dein/e Freund/in dir ebenfalls mit einem Brief, dreht sich das Ganze um. Dann ist dein/e Freund/in der/die Sender/in und du der/die Empfänger/in des Briefs, da du den Brief nun zugeschickt bekommst.

Wenn du deinen Brief nun in geheimer Sprache schreiben möchtest, musst du zunächst den Klartext, also den Text, den alle Menschen lesen können, in einen Geheimtext übersetzen. Diesen Vorgang nennen wir „Verschlüsselung“. Wenn dein/e Freund/in den Brief mit dem Geheimtext dann erhält, muss die Botschaft decodiert werden, also zurück in eine uns verständliche Sprache übersetzt werden. Dieser Prozess ist notwendig, um den Inhalt der Nachricht zu verstehen und wird „Entschlüsselung“ genannt.

Insgesamt kannst du in diesem Codeknacker-Heft sechs unterschiedliche Geheimschriften kennenlernen: Die Gartenzaunmethode, das Winkeralphabet, die Skytale, den Cäsar-Code, den Polybios-Code und den Freimaurer-Code. Um alle diese Codes decodieren zu können, musst du manchmal noch etwas basteln. Das ist immer dann der Fall, wenn du neben einer Aufgabe diesen Klebstift abgebildet findest:

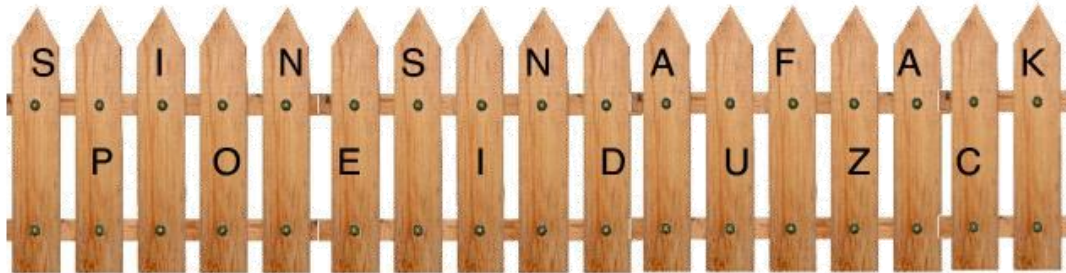


Gib aber nicht so schnell auf, wenn du eine Geheimschrift nicht sofort lesen kannst, es heißt ja nicht umsonst **G-E-H-E-I-M**-Schrift.

Und jetzt los: Viel Spaß auf den Spuren verschlüsselter Informationen und geheimer Codes!

Aufgabe 1: Die Gartenzaunmethode

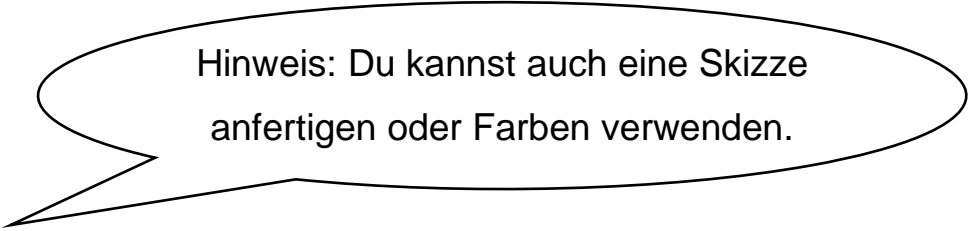
Bei der Gartenzaunmethode werden die Buchstaben des Klartextes nicht geändert. Sie werden lediglich mittels eines einfachen Verfahrens neu angeordnet. Der Gartenzaun zeigt dir das Muster der Anordnung.



- a) Versuche die Nachricht auf dem Gartenzaun zu entschlüsseln. Wie lautet die Botschaft?

- b) Um die Entschlüsselung der Botschaft schwieriger zu machen, kann man jede Zeile auf dem Gartenzaun für sich notieren und zwischen den Zeilen einen Punkt setzen. Wie sieht die Notation für den obigen Satz dann aus? Lies die Botschaft deinem Nachbarn vor.

- c) Verschlüssele die folgenden drei Sätze mit der Gartenzaunmethode.
Probiere verschiedene Möglichkeiten aus.



Hinweis: Du kannst auch eine Skizze
anfertigen oder Farben verwenden.

Spione haben keinen Zutritt.

Ich kann geheime Botschaften schreiben.

Am Wochenende gehe ich schwimmen.

d) Entschlüssele die drei geheimen Botschaften. Findest du auch eine Möglichkeit, die Nachrichten ohne Zaun oder Skizze zu entschlüsseln?

HSDGTUGPST.ATUUAFEAS

KIEAHIHITIHR.ENNCRCTSSCE

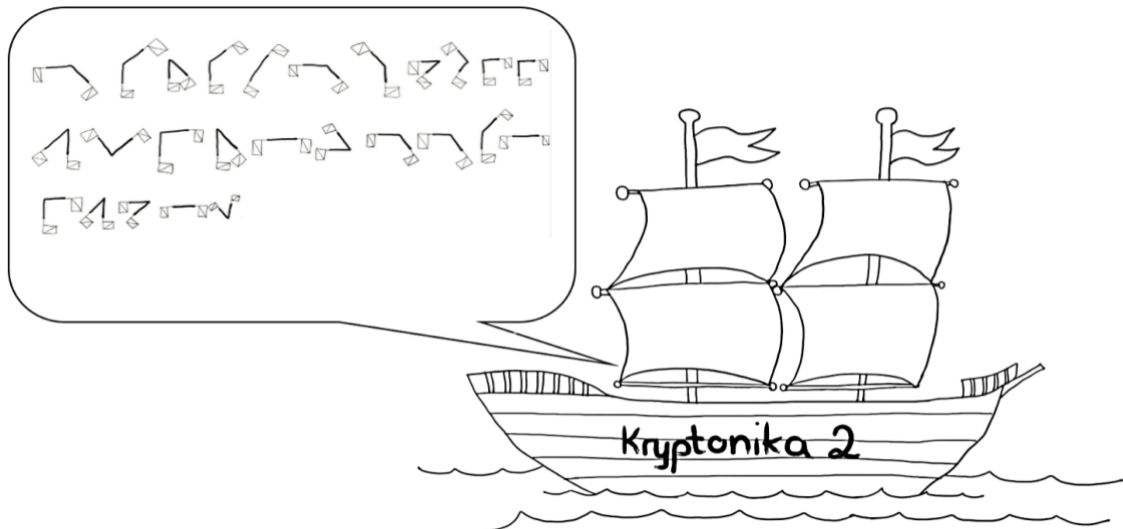
EBET.SITILUU.GVZN

e) Denke dir eigene Geheimbotschaften aus und verschlüssele sie mit der Gartenzaunmethode.

--

Aufgabe 2: Das Winkeralphabet

Vor der Erfindung des Radios verständigten sich Seeleute von Schiff zu Schiff mithilfe des Winkeralphabets. Ein Matrose, der für die Nachrichtenübermittlung zuständig war, hielt in jeder Hand eine Flagge, die er in bestimmten Positionen halten musste. Jede Position steht für einen bestimmten Buchstaben.



- a) Was möchte dir der Kapitän der „Kryptonika 2“ mitteilen?
Entschlüssele die Nachricht mithilfe des Winkeralphabets.



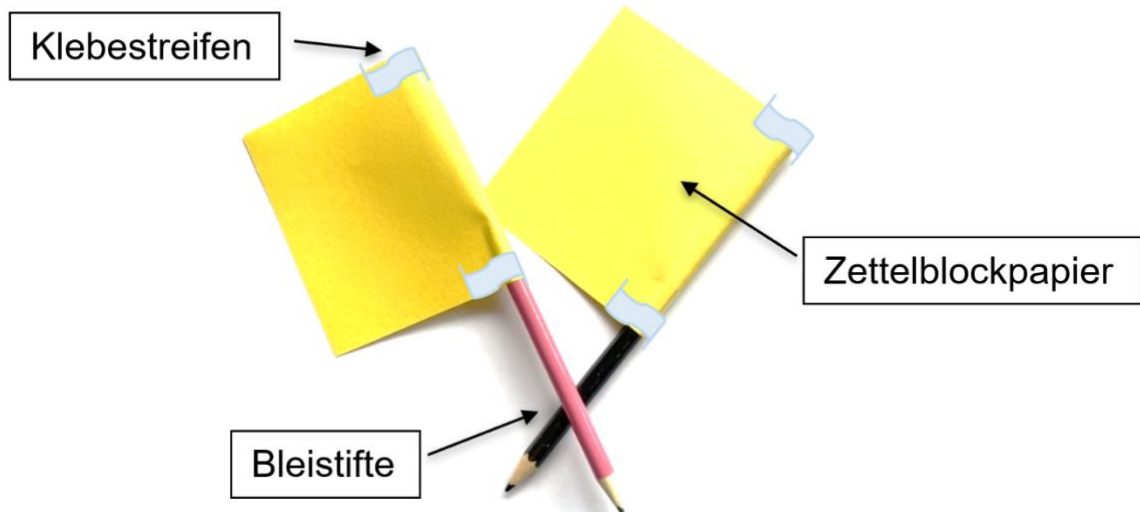
A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	Q	R	S	T
U	V	W	X	Y
Z	Irrtum	Anfang		

Nachricht des Kapitäns:

b) Antworte dem Kapitän mit „Schiff ahoi“, indem du die Nachricht mithilfe des Winkeralphabets verschlüsselst.

--	--	--	--	--	--	--	--	--	--

c) Stelle dir selbst zwei Fahnen aus zwei Stiften und Zettelblockpapier her. Suche dir dann einen Partner und stellt euch im Abstand von ein paar Metern gegenüber. Buchstabiert euch gegenseitig Wörter oder Sätze.



d) Ist diese Geheimsprache sicher vor Spionen? Was benötigt man, um sie zu entschlüsseln?

--

Aufgabe 3: Die Skytale

- a) Schneide den beschrifteten Textstreifen aus und klebe ihn an den entsprechenden Stellen zusammen (s. *Datei: A3_Bastelanleitung_Textstreifen*). Auf dem Textstreifen steht eine sehr alte Botschaft der Spartaner an die Athener. Finde eine Möglichkeit, die Nachricht zu knacken. Du benötigst dafür eine leere Küchenrolle als *Skytale*, das bedeutet auf altgriechisch *Stock* oder *Stab*. Wie lautet die Botschaft?



Botschaft:

- b) Die Athener möchten den Spartanern antworten. Benutze dazu den linierten Papierstreifen (s. *Datei: A3_Bastelanleitung_Textstreifen*) und verfasse folgende Botschaft mithilfe der Skytale: „Hilfe ist unterwegs!“



- c) Formuliere eine eigene geheime Botschaft an eine Freundin oder einen Freund. Verwende dazu den leeren Textstreifen (s. *Datei: A3_Bastelanleitung_Textstreifen*) und als Skytale einen anderen runden Stab, den du zu Hause findest.



d) Worauf müssen sich Sender und Empfänger geeinigt haben, bevor sie sich eine Skytale-Nachricht senden? Was darf niemand außer ihnen wissen?

e) Kannst du die folgende Nachricht auch ohne Skytale "knacken"?

KRCKOGHFMEFUMNRRMNATOAN!

f) Warum ist das "Knacken" und nicht "Entschlüsseln"? Was ist der Unterschied?

Aufgabe 4: Der Cäsar-Code

Der römische Feldherr und Schriftsteller Julius Caesar (100-44 v. Chr.) nutzte ein Verschlüsselungsverfahren, bei welchem jeder Buchstabe des Klartextes durch einen anderen Buchstaben des Alphabetes ersetzt wurde. Es gibt dabei immer eine bestimmte Zahl, mit deren Hilfe ihr erkennt, welcher Buchstabe des Klartextes durch welchen Buchstaben des Geheimtextes ersetzt wird. Diese Zahl nennt man auch den *Schlüssel*.

- a) Finde heraus, welchen Schlüssel Cäsar für diese Geheimnachricht an Kleopatra genutzt hat und entschlüssele die Nachricht. Schreibe den Klartext auf die gestrichelte Linie. Zur Unterstützung kannst du unser Decodier-Programm (s. *Datei Decodierprogramm*) und den untenstehenden Tipp nutzen.



G X E L V W I X H U P L F K G H U

 K H O O V W H V W H U Q L Q G H U

 Q D F K W

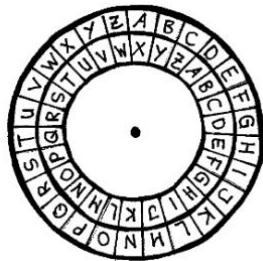
Tipp: Wie du der folgenden Tabelle entnehmen kannst, kommt in der deutschen Sprache der Buchstabe „E“ am häufigsten vor. 13% bedeutet beispielsweise, dass 13 von 100 Buchstaben in einem Text im Durchschnitt ein „E“ sind.

Häufigkeitsverteilung der Buchstaben unseres Alphabetes in Prozent

E	13%	H	6%	W	2%	K	<1%
T	9%	R	6%	F	2%	J	<1%
A	8%	D	4%	G	2%	X	<1%
O	8%	L	4%	Y	2%	Q	<1%
I	7%	C	3%	P	2%	Z	<1%
N	7%	U	3%	B	1%		
S	6%	M	2%	V	1%		

Welcher Buchstabe kommt in Cäsars Geheimnachricht am häufigsten vor? Mit diesem Tipp kannst du herausfinden, um wie viele Stellen Cäsar das Alphabet verschoben hat, um seine Botschaft zu verschlüsseln.

b) Der Mathematiker Leon Battista Alberti entwickelte im 15. Jahrhundert die Chiffrier-Scheibe. Die Chiffrier-Scheibe wird heute auch Cäsar-Scheibe genannt, weil sie auf sein Verschlüsselungsverfahren zurückgeht.

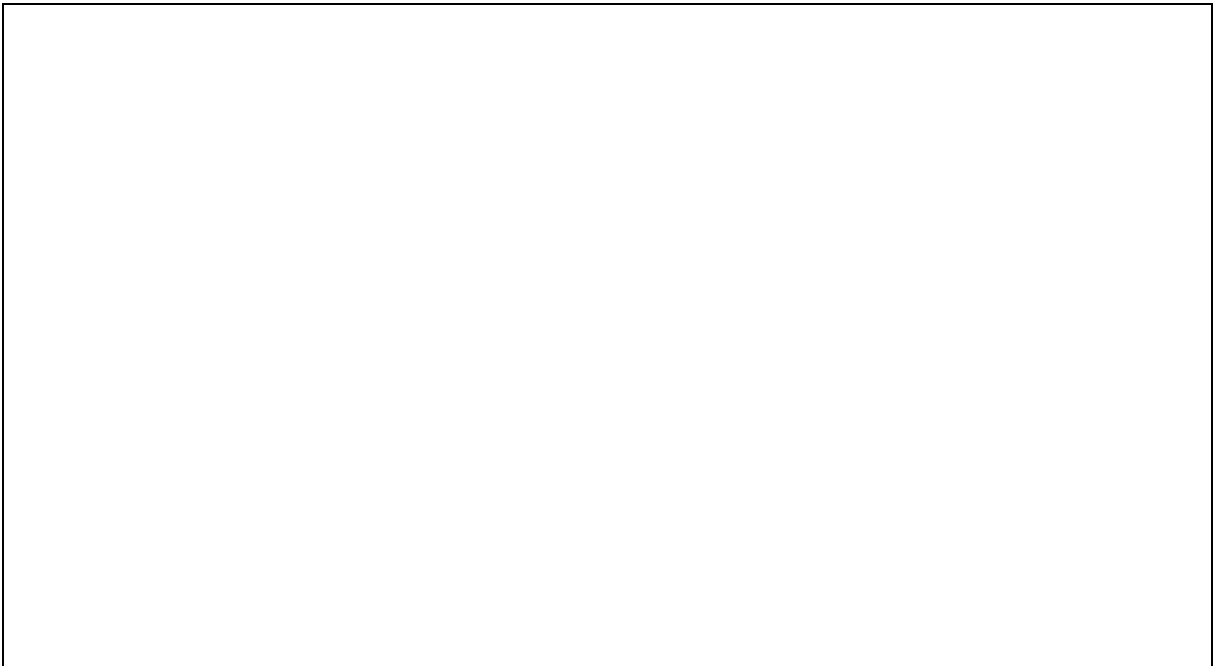


Bastele dir eine eigene Chiffrier-Scheibe und schaue dir genau an, wie die Verschlüsselung mit der Scheibe funktioniert (s. *Datei: A4_Bastelanleitung_Caesarscheibe*).

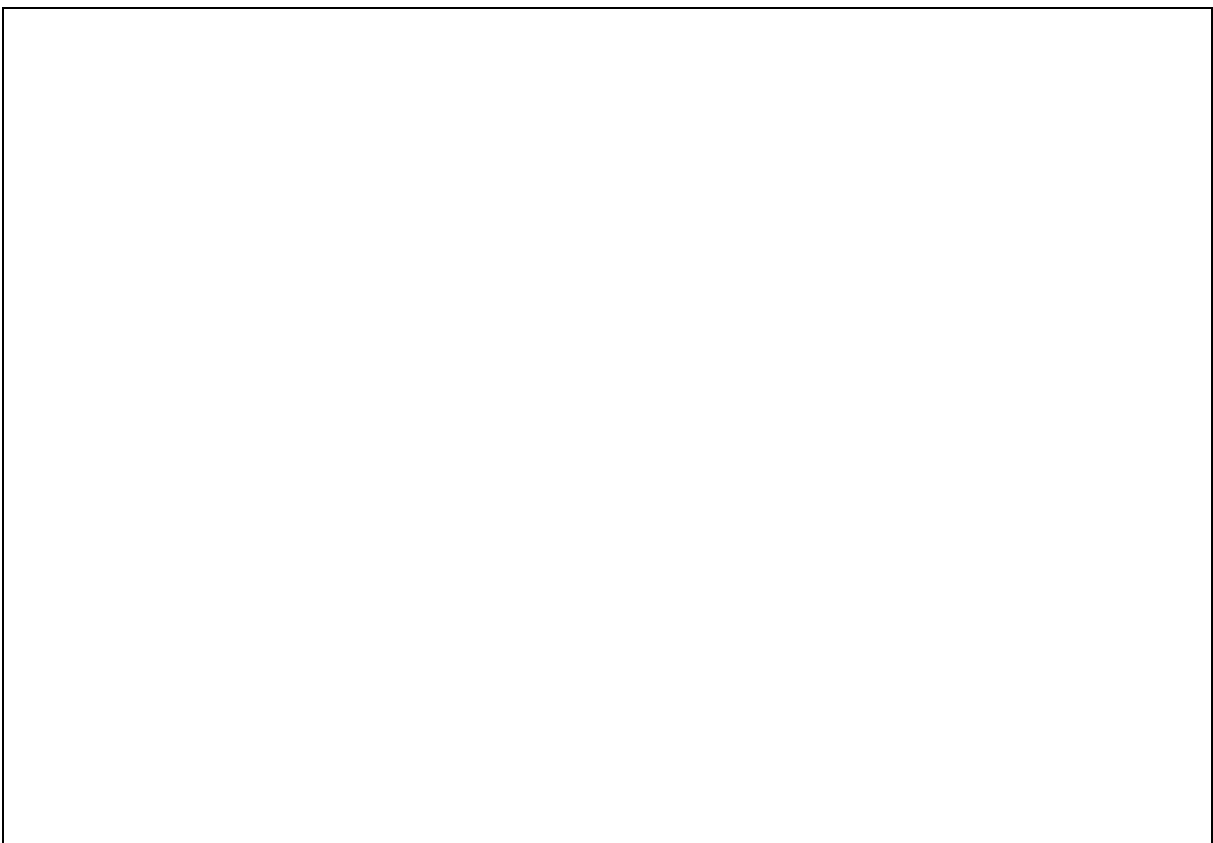
Überlege dir nun eine kurze Antwort auf den Brief von Julius Caesar an Kleopatra und verschlüssele sie mithilfe der Chiffrierscheibe. Den Schlüssel darfst du selbst festlegen.

Deine geheime Antwort:

c) Die Erfindung von Leon Battista Alberti ist eine Weiterentwicklung der Cäsar-Methode. Worin liegt der Vorteil der Scheibe?



d) Wie viele Möglichkeiten gibt es, einen Text mit der Chiffrierscheibe zu verschlüsseln?

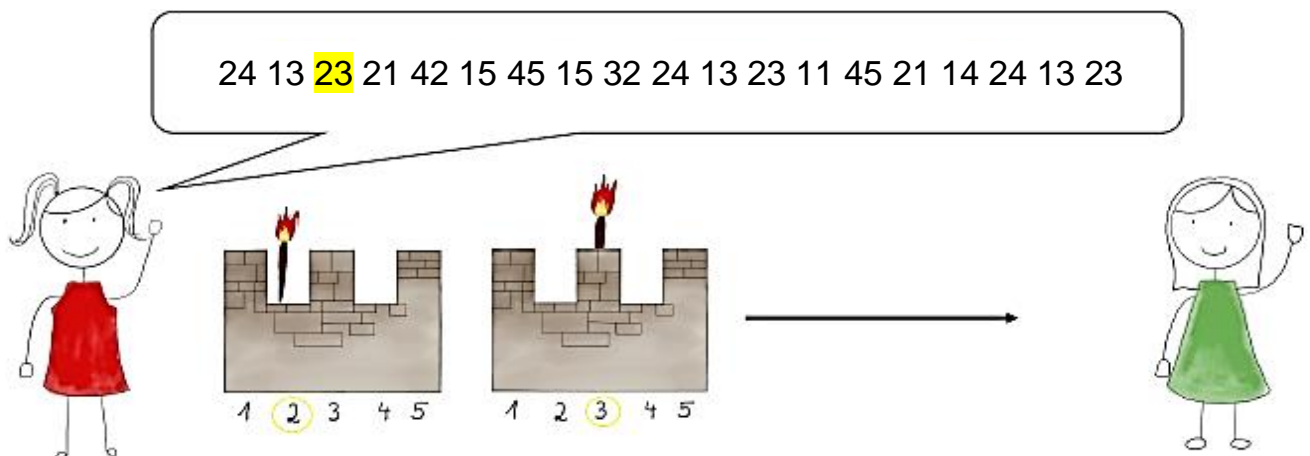


Aufgabe 5: Der Polybios-Code

Der griechische Schreiber Polybios (ca. 200-120 v. Chr.) beschrieb ein Verfahren zur optischen Übermittlung von Nachrichten. Der Polybios-Code diente dabei nicht dem Geheimhalten der Nachricht. Es ging vielmehr darum, sich über weite Entfernungen zu unterhalten.

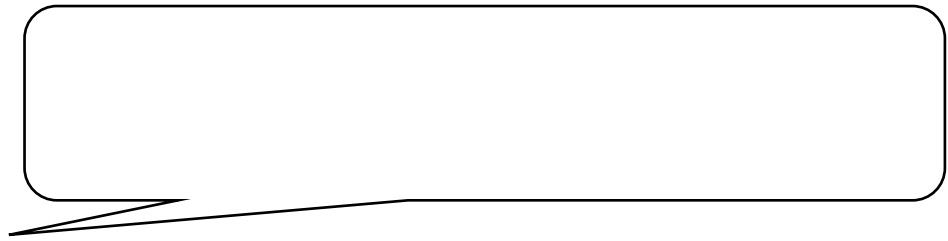
Wollte man beispielsweise eine Nachricht an eine Person übermitteln, die ein gutes Stück entfernt war, nutzte man leuchtende Fackeln, die an unterschiedlichen Stellen der Burgzinnen positioniert wurden. Mithilfe des Polybios-Quadrates konnten die optischen Signale entschlüsselt werden.

- a) Finde heraus, was das Mädchen im roten Kleid zu dem Mädchen in dem grünen Kleid sagt und notiere es in der leeren Sprechblase auf der nächsten Seite.



Die folgende Tabelle hilft dir den Code zu entschlüsseln:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z



b) Überlege dir, was das Mädchen in dem grünen Kleid antworten könnte.
Verschlüssele deine Botschaft mittels des Polybios-Codes.



c) Funktioniert eine Verschlüsselung mithilfe des Polybios-Codes auch, wenn du die Buchstaben nicht nach dem Alphabet, sondern wild durcheinander anordnest?

Probiere verschiedene Möglichkeiten aus und begründe auf der nächsten Seite.

	1	2	3	4	5
1					
2					
3					
4					
5					


	1	2	3	4	5
1					
2					
3					
4					
5					

	1	2	3	4	5
1					
2					
3					
4					
5					

Begründung:

d) Was ist die Voraussetzung dafür, dass Sender und Empfänger sich richtig verstehen können?

- b) Schreibe eine geheime Botschaft an deine Freundin oder deinen Freund und überprüfe, ob sie den Freimaurer-Code ebenfalls entschlüsseln können.



- c) Mittlerweile wird diese Art von Verschlüsselung, wie auch etliche der anderen Verschlüsselungsmethoden in diesem Heft, nicht mehr angewendet. Überlege, woran das liegen könnte?





Didaktik der Mathematik (Primarstufe)

Institut für Mathematik
Universität Koblenz-Landau
Westring 2

76829 Landau

<https://www.uni-landau.de/primalernwerkstatt>

Zusammengestellt von:

Katharina Bitzer, Michelle Hebel, Elena Müller, Thuy-Vy Nguyen, Joana
Thul

Betreut von:

Prof. Dr. Stephanie Schuler

Veröffentlicht am:

12.10.2020