BERGISCHE
UNIVERSITÄT
WUPPERTAL

SPIONCAMP

Kofferinhalt

Dieser Koffer enthält alle Materialien, die zur Durchführung des Stationenlernens »SpionCamp - Lernstationen zur Kryptographie« im Unterricht notwendig sind.

Allgemeines Material

- Metallkoffer mit Fächeraufteilung und Spion-Logo, 18 Fähnchenhalter und 20 Fähnchen zur Markierung des Schwierigkeitsgrads der aufgebauten Stationen (und für das Winker-Alphabet)

Stationsmaterial

Codierung

- Übersicht:
  1 Übersichtsblatt (laminiert)
- Station Morsealphabet:
  1 Stationsblatt (laminiert), Morsealphabet (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt, 1 Taschenlampe mit Blinkfunktion
- Station Braille-Schrift:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt, Steckvorlage (laminiert) auf Hartschaumplatte, Landkartennadel
- Station Winkeralphabet:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, mehrere Fähnchen

Steganographie

- Station Bild:
  1 Stationsblatt (laminiert), 1 Lösungsblatt
- Station Text:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt

Transposition

- Station Skytale:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt, 3 Skytale (Stöcke verschiedenen Durchmessers), 6 Nachrichten für die Skytale
- Station Schablonen:
  1 Stationsblatt (laminiert), 1 Blatt mit 3 verschlüsselten Nachrichten, 1 Nachrichtenvorlage, 1 Arbeitsblatt, 1 Lösungsblatt, 3 Schablonen
- Station Pflügen:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt

- Station Block-Chiffre:
  1 Stationsblatt (laminiert), 4 Permutationshilfen, 1 Folienstift, 1 Textvorlage, 1 Arbeitsblatt, 1 Lösungsblatt

Substitution

- Station Freimaurer-Chiffre:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt
- Station Caesar:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt, 1 Caesarscheibe in CD-Hülle
- Station Playfair:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt
- Station Rotoren:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt, 2 Rotoren in CD-Hüllen
- Station Vigenère:
  1 Stationsblatt (laminiert), Vigenère-Quadrat (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt
- Station Strom-Chiffre:
  1 Stationsblatt (laminiert), 1 Stromverschlüsseler, 1 Arbeitsblatt, 1 Lösungsblatt

Kryptoanalyse

- Station Buchstabenhäufigkeit:
  1 Stationsblatt (laminiert), 1 Geheimtext, 1 Arbeitsblatt, 1 Lösungsblatt,

Schlüsselaustausch

- Station Modulo-Rechnung:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt, 1 Lösungsblatt,
- Station Diffie-Hellman-Algorithmus:
  1 Stationsblatt (laminiert), 1 Arbeitsblatt

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen **Code**. Mit einem Code soll nichts geheim gehalten werden.

An der Station findet ihr verschiedene Codes:

- Morsealphabet: Damit kann man sich mit Lichtzeichen verständigen.
- Braille-Schrift: Damit können Blinde lesen.
- Winker-Alphabet: Damit kann man sich in Sicht, aber außer Hörweite verständigen.

Aufgabe 1 Suche dir einen dieser drei Codes aus. Zu jedem Code gibt es an der Station eine Karte, mit der du den Code näher kennenlernen kannst.

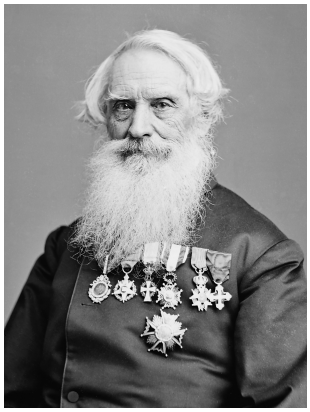
Aufgabe 2 Im täglichen Leben gibt es jede Menge Codes. Fallen dir Beispiele ein?

Version vom 2019-09-13

Morsealphabet

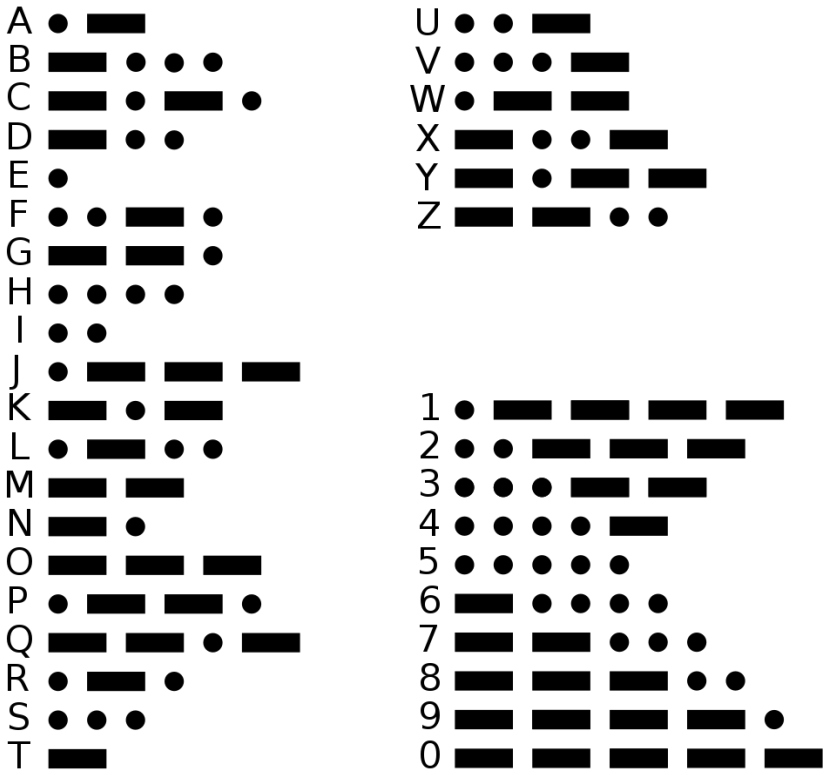
Codierung

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen **Code**. Mit einem Code soll nichts geheim gehalten werden.



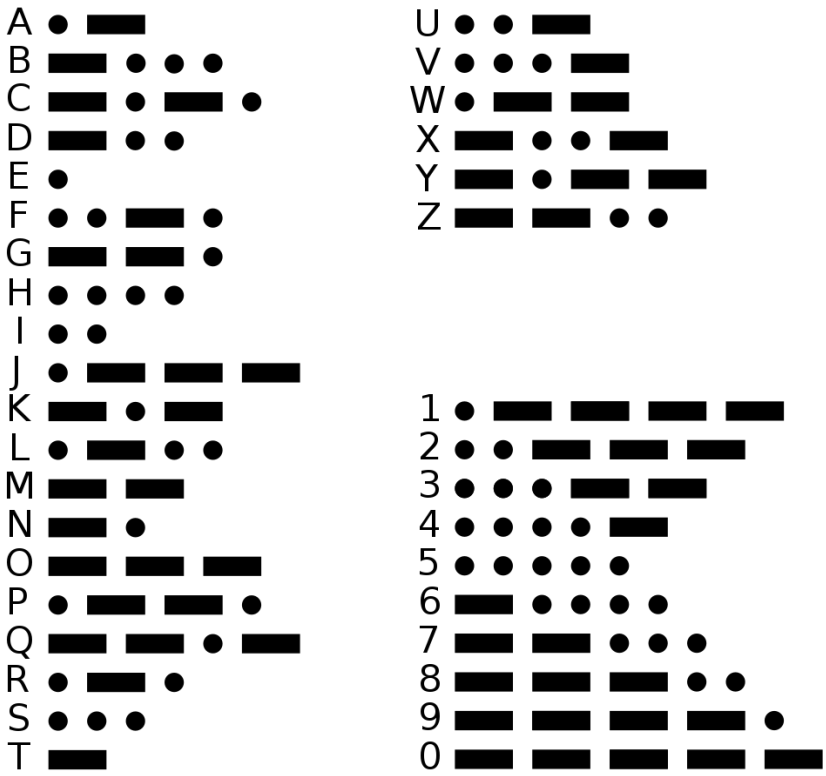
1832, noch vor der Erfindung des Telefons, erfand der Amerikaner Samuel Morse einen Apparat, den Morsetelegraphen. Mit dessen Hilfe konnten Nachrichten über große Entfernungen hinweg übermittelt werden. Dazu wurden so genannte Telegraphenmasten aufgestellt und Leitungen durch das ganze Land gespannt. Es konnten allerdings keine gesprochenen Worte übertragen werden, sondern lediglich kurze und lange elektrische Impulse.

Deshalb dachte sich Samuel Morse ein Alphabet aus, das nur aus kurzen und langen Signalen bestand:



Für die Übertragung von Morsezeichen kann man auch Lichtzeichen verwenden. Zwischen den Buchstaben wird eine kurze Pause gemacht. Zwischen den Wörtern eine etwas längere.

Morsealphabet-Tabelle



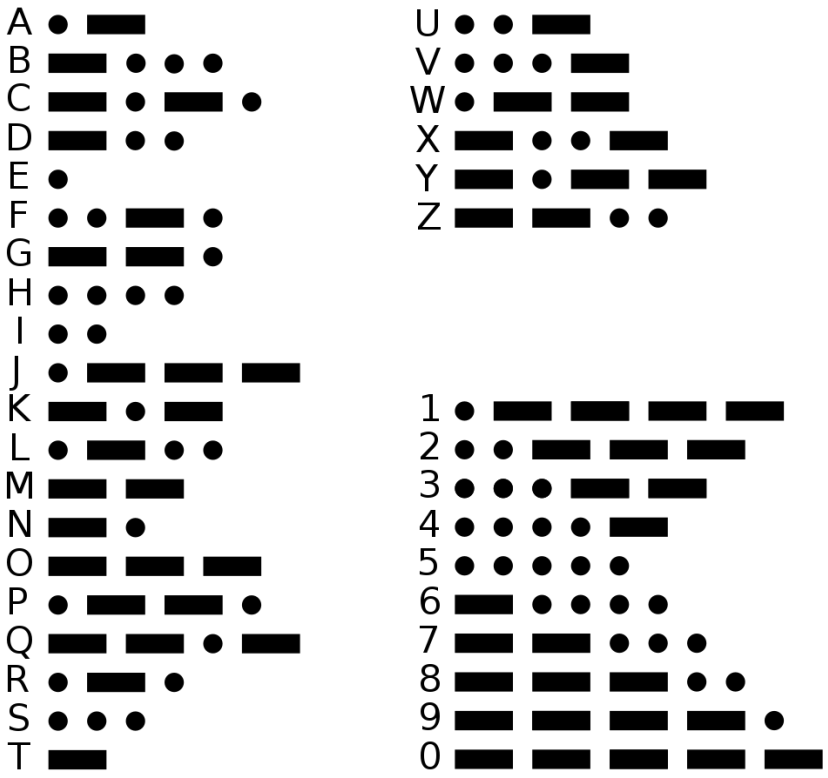
Aufgabe 1 Könnt ihr folgende Nachricht verstehen?

`--. ..- - . -. - .- --.`

Aufgabe 2 Wie lautet das Morse-Signal für SOS? (Das ist das internationale Hilfesignal.)

Aufgabe 3 Erkennst du das Muster, wie das Morsealphabet aufgestellt wurde? Überlege dir die Antwort anhand folgender Hilfsfragen: Welche Verbindung hat die Anzahl der Signale zu dem Buchstaben? Welche Buchstaben bestehen aus wenigen Signalen? Welche Buchstaben bestehen aus vielen Signalen?

Aufgabe 4 An der Station findet ihr eine Taschenlampe. Stellt euch zu zweit mit ein paar Metern Entfernung gegenüber auf, jeder mit einem Morsealphabet. Buchstabiert euch mit der Taschenlampe gegenseitig jeweils ein Wort.



Lösung 1 **Guten Tag**

Lösung 2 `...` `---` `...` ist das Zeichen für SOS.
In Not wird aber nicht »SOS SOS . . . « gefunkt, sondern immer »S« und »O« abwechselnd.

Lösung 3 Die Anzahl der Signale eines Buchstabens hängt mit der Buchstabenhäufigkeit in der englischen Sprache zusammen. Ein »E« kommt z. B. am häufigsten vor und hat deswegen nur ein Signal. Ein »Q« wird nur sehr selten benutzt und besteht deshalb aus vier Signalen.

Lösung 4 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen **Code**. Mit einem Code soll nichts geheim gehalten werden.

Louis Braille (geboren 1808 in Frankreich) wurde im Alter von 3 Jahren nach einem Unfall blind. Mit 14 Jahren entwickelte er eine Schrift, die auch Blinde lesen können. Sie besteht aus erhöhten Punkten, die mit den Fingern zu ertasten sind.
Es gibt für Blinde viele Bücher in Blindenschrift. Für den Computer gibt es spezielle Braille-Zeilen, mit denen auch Blinde z. B. im Web surfen können.
Obwohl es auch noch andere Schriftarten mit erhöhten Zeichen gibt, ist die Braille-Schrift heute am weitesten verbreitet.

Tafel mit Braille-Zeichen

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
1	2	3	4	5	6	7	8	9	0			

Dir ist vielleicht aufgefallen, dass z. B. »1« und »A« durch dasselbe Braille-Zeichen dargestellt werden. Damit man weiß, was gemeint ist, wird einer Zahl ein bestimmtes Zeichen vorangestellt. Geht es danach mit Buchstaben weiter, wird das Zeichen für »Buchstabe« geschrieben. Diese vorangestellten Zeichen heißen auch **Präfixe**. Du findest die Zeichen in der Abbildung rechts.

Zahl	Buchstabe

Beispiel

21 Äpfel

Es gibt auch Zeichen für Klammern, Umlaute, Groß- und Kleinschrift und andere spezielle Zeichen. Diese wurden hier weggelassen.

Version vom 2019-08-09

Stecke einen Text. Probiert zu zweit aus, ob die/der jeweils andere den Text mit dem Finger erfühlen kann. Nimm die Tabelle auf dem Stationsblatt für die Buchstabencodes hinzu.

Du brauchst Stecknadeln (nicht zu lang!) zum Stecken der Braille Schrift.

Version vom 2019-06-11

Aufgabe 1 Kannst du folgende Nachricht verstehen?

Aufgabe 2 Aufgabe 1 war ziemlich leicht. Kannst Du auch das hier »lesen«?

Aufgabe 3 An der Station findet ihr ein Blatt, auf dem ihr selbst Nachrichten »schreiben« könnt. Arbeitet im Team. Eine(r) schreibt ein Wort durch Stecken der Nadeln auf das Brett. Die/der andere liest dann wie ein Blinder — Augen schließen. Nicht schummeln! — und versucht, die Nachricht zu ertasten. Beschreibt eurem Partner Buchstabe für Buchstabe, welche Punkte erhöht sind. Zum Beispiel für ein **N**:

oben links, oben rechts, mitte rechts, unten links

Der Sehende kann dann nachschauen, welcher Buchstabe das ist. Wechselt nach dem Wort die Rollen.

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
1	2	3	4	5	6	7	8	9	0			

Version vom 2019-06-11

Lösung 1 **SPIONCAMP**

Lösung 2 **DIE ANTWORT IST 42**

Lösung 3 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

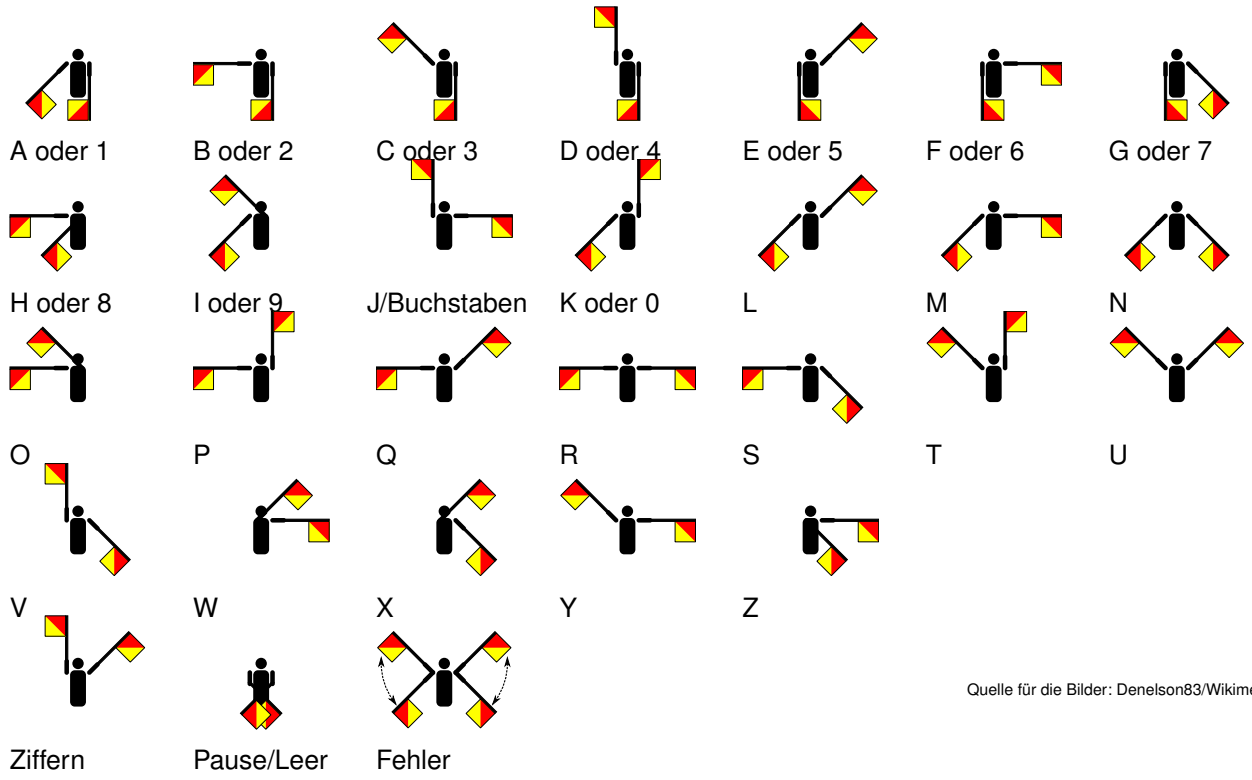
Version vom 2019-06-11

Winkeralphabet

Codierung

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. (Aber jeder kann nachschlagen, was sie bedeuten!) Man nennt so etwas einen **Code**. Mit einem Code soll nichts geheim gehalten werden.

Das Winkeralphabet stammt aus der Seefahrt. Man kann sich damit verständigen, wenn man sich in Sichtweite aber außer Hörweite voneinander befindet. Man nimmt zwei Flaggen in die Hände und zeigt durch Stellung der Arme bestimmte Zeichen an.



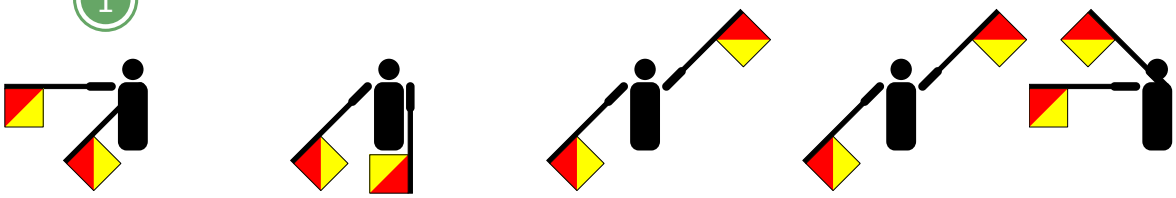
Quelle für die Bilder: Denelson83/Wikimedia

Einige Zeichen sind doppelt belegt: das erste Zeichen kann zum Beispiel »A« oder »1« bedeuten. Möchtest du eine Ziffern senden, winkst du einmal das Zeichen für »Ziffern«. Für Buchstaben nach Ziffern, das Zeichen »J«.

Kennt ihr dieses Zeichen?

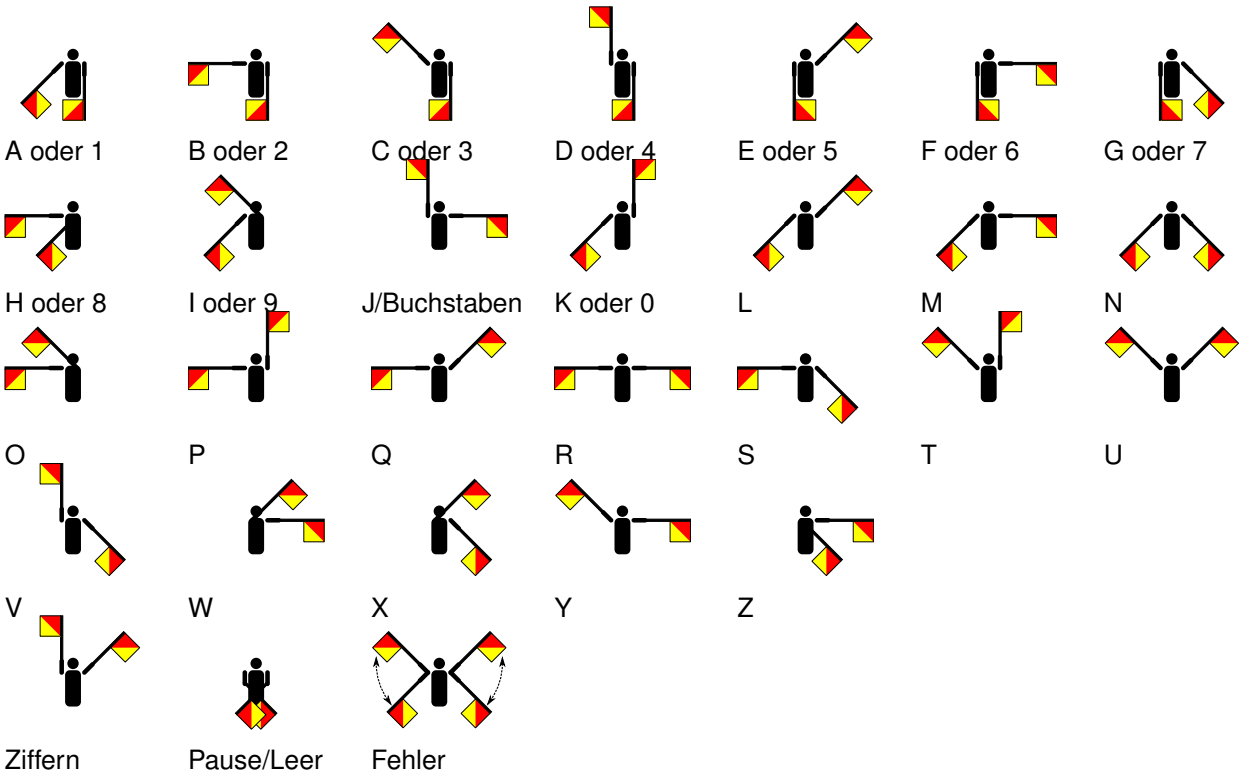
Es wurde 1958 erfunden und soll *atomare Abrüstung* symbolisieren. Atomare Abrüstung heißt auf Englisch *Nuclear Disarmament*. Die Zeichen für N und D aus dem Winkeralphabet wurden zu diesem Zeichen kombiniert. (Der senkrechte Strich ist das D, die beiden schrägen das N.)

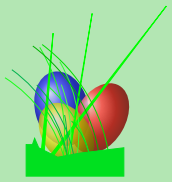
Aufgabe 1 Entschlüssele folgende Nachricht!



Aufgabe 2 An der Station findet ihr Flaggen. Nehmt jeder zwei und stellt euch mit ein paar Metern Entfernung gegenüber auf. Buchstabiert euch mit den Flaggen gegenseitig jeweils ein Wort.

Das Winkeralphabet





Die Buchstaben bleiben, **was** sie sind, aber man erkennt nicht, **wo** die Nachricht ist. Das ist eigentlich gar keine Verschlüsselung, man nennt das **Steganographie**. (Das Wort Steganographie ist abgeleitet von den griechischen Wörtern *steganos* = bedeckt und *graphein* = schreiben.)

Bei der Steganographie werden Nachrichten in Medien versteckt, z.B. in Bildern. Wenn du dir das Bild nur kurz ansiehst, fällt dir gar nicht auf, das hier eine Nachricht enthalten sein könnte.
Texte oder Bilder, in denen Nachrichten versteckt wurden, heißen *Semagramme*.

Aufgabe 1 Kannst du die Nachricht in dem folgenden Semagramm lesen?
Es ist nicht ganz einfach, da die Nachricht vor dem Verstecken codiert wurde.
Tipp: Sieh dir die Stationen zur Codierung nochmal an.

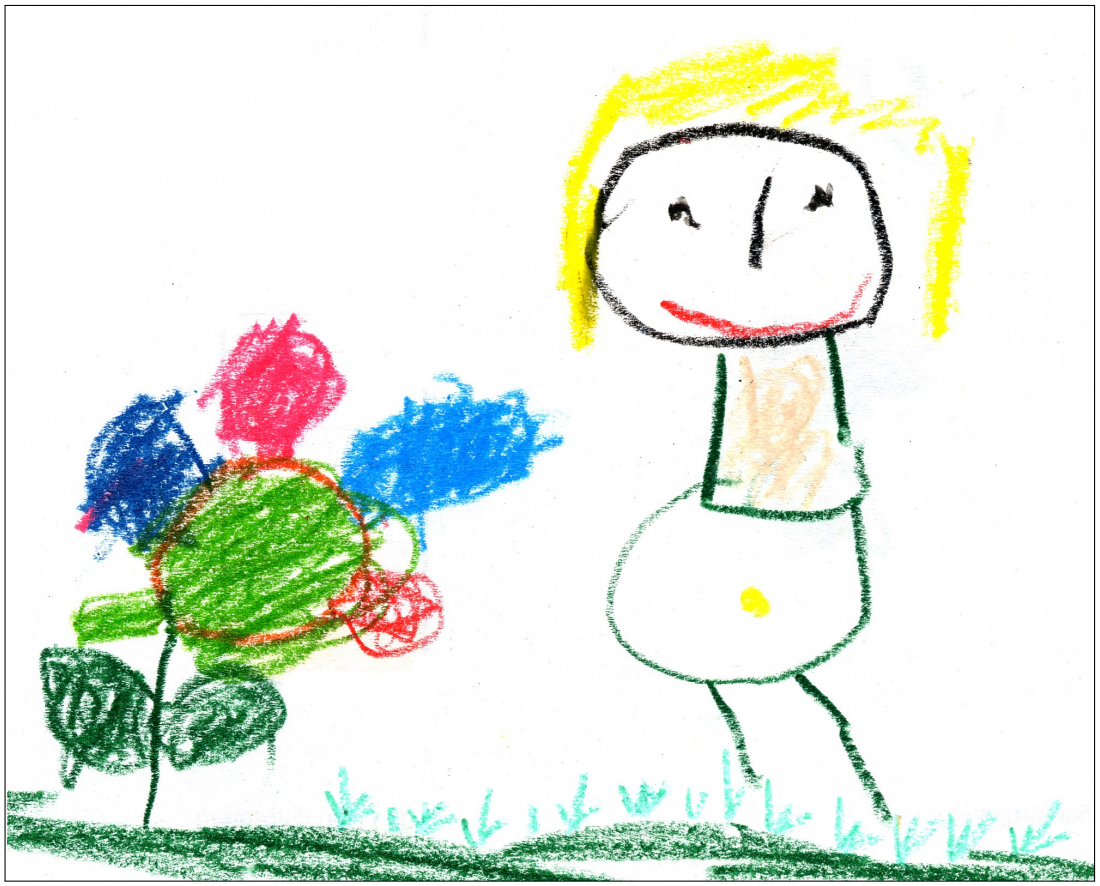


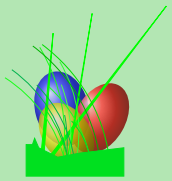
Bild: Emma, 3 Jahre (dem Bild wurde dann die (codierte) Nachricht hinzugefügt)

Lösung 1

Das Bild enthält eine Nachricht im Morsecode. Die Grashalme haben lange und kurze Stengel und sind zu Büscheln (= Buchstaben) zusammengefasst. Die Nachricht lautet also:

.-.. . .... .-. . .-. ... .. -. -.. -.. - - - - - - ..-.

(LEHRER SIND DOOF)



Die Buchstaben bleiben, **was** sie sind, aber man erkennt nicht, **wo** die Nachricht ist. Das ist eigentlich gar keine Verschlüsselung, man nennt das **Steganographie**. (Das Wort Steganographie ist abgeleitet von den griechischen Wörtern *steganos* = bedeckt und *graphein* = schreiben.)

Bei der Steganographie werden Nachrichten in Medien versteckt, z.B. in Texten. Wenn du dir den Text nur kurz durchliest, fällt dir gar nicht auf, das hier eine Nachricht enthalten sein könnte.
Die Steganographie in Texten wird in zwei unterschiedliche Arten unterteilt:

- Nachrichten werden durch kaum sichtbare graphische Details einer Schrift versteckt. Diese Nachrichten heißen *Semagramme*. Diese Art von Steganographie ist jedoch teilweise recht auffällig, wenn der Text genau betrachtet wird.

- Eine geheime Nachricht erscheint als unverfängliche und offen verständliche Nachricht, ist es jedoch gar nicht. Eine solche Nachricht heißt *Open Code*. Dieses Versteck ist deutlich unauffälliger als die Semagramme. Eine geübte Krypthographin oder ein geübter Kryptograph erkennt diese Tarnung jedoch an der gestellten Sprache, da die offene Nachricht so ausgewählt werden muss, dass die geheime Nachricht versteckt werden kann.

Kannst du die Nachrichten in diesen Semagrammen und Open Codes lesen?

Aufgabe 1 Diese **s**im**p**le Aufgabe müsstest du le**i**cht enträtseln können. Die Antw**o**rt ist zu deutlich erke**n**nbar.

Aufgabe 2 Einmal darfst du noch an einer leichten Aufgabe rätseln, danach kommen die etwas schwierigeren.

Aufgabe 3 Die Aufgabe ist schon etwas schwieriger. Wenn du genau hinsiehst, wirst du die Information aber erspähen.

Aufgabe 4 Jetzt wird es noch ein bisschen kniffliger. Aber eine gelernte Informatikerin oder ein gelernter Informatiker, erkennt den Trick direkt.

Aufgabe 5 Hast du es jetzt schon erraten? Es gibt nicht nur Auffälligkeiten rund um die Schriftart, sondern leider spielt manchmal die Gestalt des Textes eine lebenswichtige Rolle. Hier siehst du einen Trick, der ohne Hilfe von Codes die Nachricht kaschiert.

Aufgabe 6 Naja, auch tolle und richtig talentierte Agenten lernen einfach nicht tadellos.

Lösung 1 Die Nachricht **SPION** ist durch dick gedruckte Buchstaben versteckt.

Lösung 2 Einige Buchstaben sind größer als die anderen und verstecken die Nachricht **DATEN**.

Lösung 3 Die Buchstaben, die in einer anderen Schriftart geschrieben sind, ergeben das Wort **CAMP**.

Lösung 4 Die kursiven Buchstaben ergeben das Wort **CODE**.

Lösung 5 Liest man die Anfangsbuchstaben einer jeder Zeile, ergibt sich das Wort **HALLO**.

Lösung 6 Die Anfangsbuchstaben aller Wörter bilden die Nachricht **NATURTALENT**.

Version vom 2019-08-09

Skytale

Transposition

Die Buchstaben bleiben, **was** sie sind, aber nicht, **wo** sie sind.
Solche Verschlüsselungen heißen **Transposition**. (Das Wort *Transposition* ist abgeleitet vom lateinischen Wort *transponere* = verschieben.)

Eine der ältesten bekannten Verschlüsselungen ist eine Transposition. Die Regierung von Sparta benutzte vor über 2500 Jahren zur Verschlüsselung eine sogenannte **Skytale**. Das ist ein Zylinder, um den ein schmaler Streifen aus Pergament gewickelt wurde. Auf dieses Pergament wurde die Nachricht von links nach rechts geschrieben.

Wurde nun der Streifen abgewickelt, standen die Buchstaben untereinander aber nicht mehr in der richtigen Reihenfolge.
Zur Entschlüsselung musste der beschriebene Streifen wieder um eine Skytale mit gleichem Umfang gewickelt werden.

HOHNAEILGISLEM

HOHNAEILGISLEM

HOHNAEILGISLEM

WKTCEEHRNM?NI

WKTCEEHRNM?NI

WKTCEEHRNM?NI

FHTHUZEESELNCTC

FHTHUZEESELNCTC

FHTHUZEESELNCTC

SSRTOTIISCGIH

SSRTOTIISCGIH

SSRTOTIISCGIH

HGEDREREIRRN

HGEDREREIRRN

HGEDREREIRRN

IAJSNNODANIE

IAJSNNODANIE

IAJSNNODANIE

Aufgabe 1 An der Station findest du einige *Skytale-Nachrichten* und auch verschiedene *Skytalen*. Kannst du die Nachrichten entschlüsseln?

Aufgabe 2 Worauf müssen sich Sender und Empfänger geeinigt haben, bevor sie sich *Skytale-Nachrichten* schicken? Was darf niemand außer ihnen wissen?

Aufgabe 3 Kannst du folgende Nachricht ohne Skytale »knacken«?

K R C I O G H N M E B X M N E D M N R K O A L P

(Warum ist das »knacken« und nicht »entschlüsseln«?)

Aufgabe 4 Schreibt euch gegenseitig eine Skytale-Nachricht mit einer beliebigen Skytale.

Version vom 2019-06-11

Lösung 1

Es gibt folgende Nachrichten:

HALLO GEHEIMNIS
WER KENNT MICH?
FUSCHZETTELCHEN
SO ISTS RICHTIG
HERR DER RINGE
INDIANA JONES

Lösung 2

Beide müssen sich auf den Durchmesser der Skytale geeinigt haben.

Lösung 3

KOMM MORGEN NACH BERLIN (XDP)

Es ist »knacken«, weil der Schlüssel nicht zur Verfügung steht.

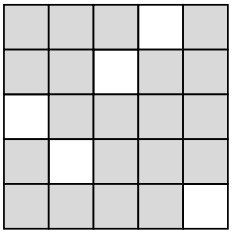
Lösung 4

Zu dieser Aufgabe gibt es keine allgemeine Lösung.

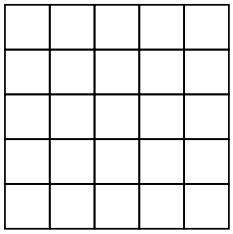
Version vom 2023-02-21

Die Buchstaben bleiben, **was** sie sind, aber nicht, **wo** sie sind.
So eine Verschlüsselung heißt **Transposition**. (Das Wort *Transposition* ist abgeleitet vom lateinischen Wort *transponere* = verschieben.)

Du brauchst für die Schablonen-Verschlüsselung eine Lochschablone. Das ist ein Papier, das an bestimmten Stellen Löcher hat. Beide Personen, der Sender und der Empfänger, benötigen die gleiche Schablone.



Lochschablone

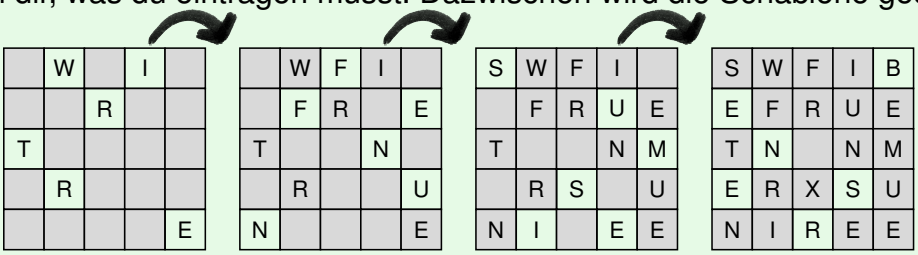


kariertes Papier

Mit dieser Art Schablone verschlüsselst du so:

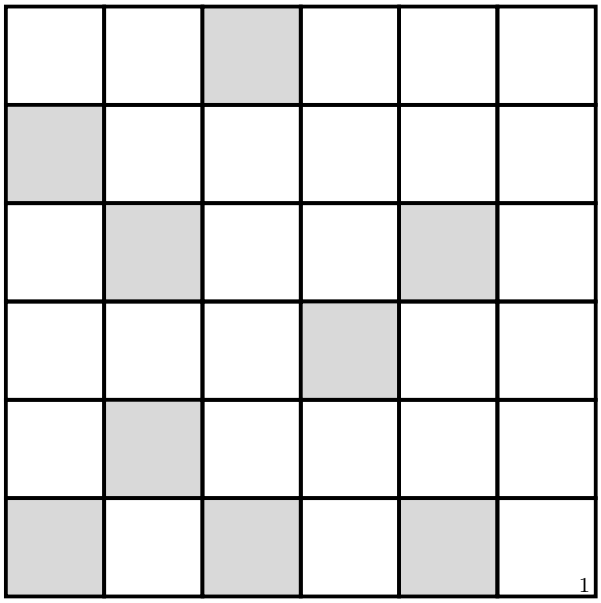
- Du legst die Schablone auf ein leeres Papier und trägst die ersten Buchstaben der Nachricht in die Löcher ein.
- Danach drehst du die Schablone im Uhrzeigersinn um 90 Grad und trägst die nächsten Buchstaben der Nachricht ein.
- So fährst du fort, bis du alle vier Stellungen der Schablone benutzt hast. Ist die Nachricht länger, beginnst du mit einem neuen Quadrat. Ist sie kürzer, werden übrige Felder mit irgendwelchen Buchstaben gefüllt.
- Bei Schablonen mit ungerader Zeilen- und Spaltenanzahl bleibt immer ein Buchstabe in der Mitte frei. Dieser muss anschließend frei gewählt werden.

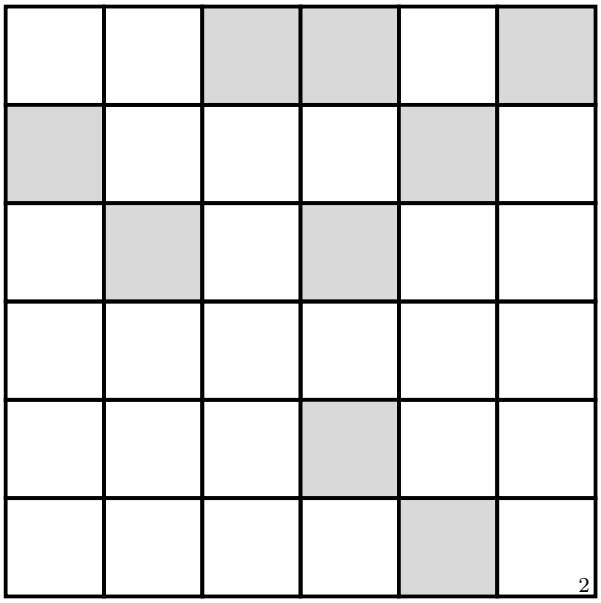
Beispiel Du möchtest z.B. den Text WIR TREFFEN UNS UM SIEBEN verschlüsseln (21 Buchstaben). Du brauchst eine Schablone, die alle Buchstaben aufnehmen kann, z.B. eine Schablone mit 5 Zeilen und 5 Spalten. Die folgenden Bilder zeigen dir, was du eintragen musst. Dazwischen wird die Schablone gedreht.

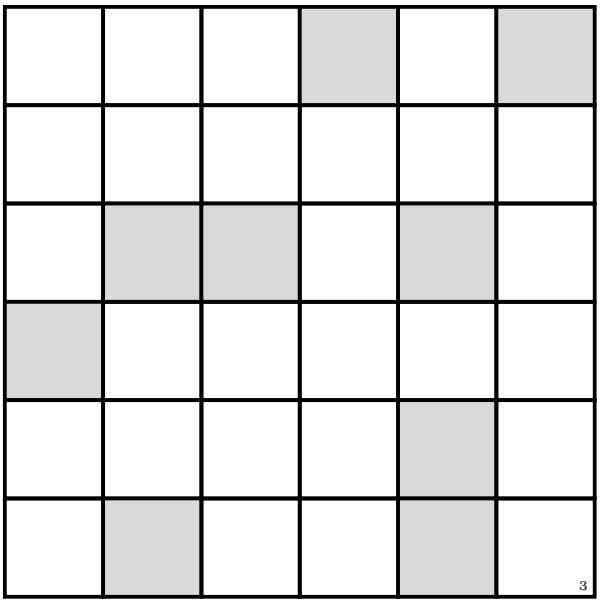


In der Mitte ist noch ein Buchstabe frei geblieben. Diesen kannst du beliebig setzen, z. B. »S«. Daraus ergibt sich dann der verschlüsselte Text SWFIBEFRUETNSNMERXSUNIREE.

Vorlagen für Schablonen







Die Schablonen ausschneiden und laminieren. Anschließend die Fenster (die dunkleren Felder) ausschneiden.

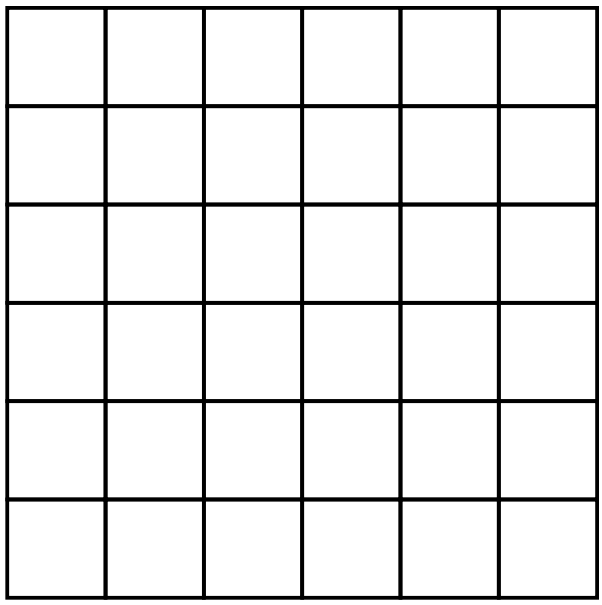
Texte zum Entschlüsseln

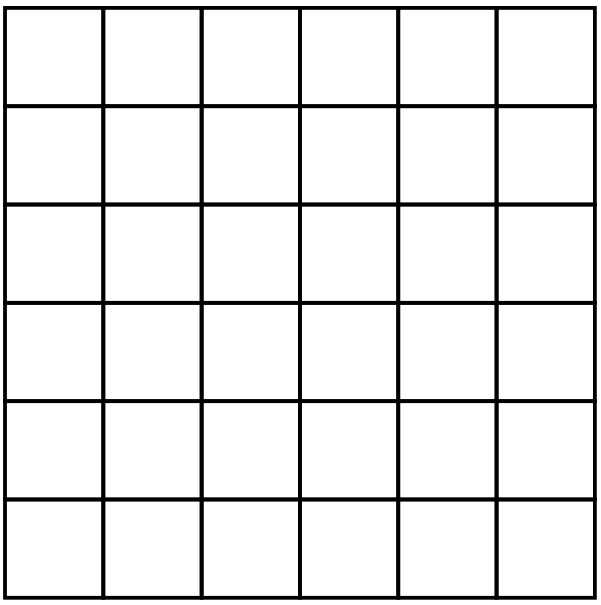
S	U	I	D	N	E	C	E	D	R	H	T
E	T	C	G	H	U	I	T	5	Z	S	S
B	R	B	T	R	E	E	E	I	E	N	R
I	R	L	S	T	I	K	C	S	A	H	U
N	D	A	E	E	D	T	C	N	O	D	I
E	F	N	E	L	R	H	E	R	N	I	N

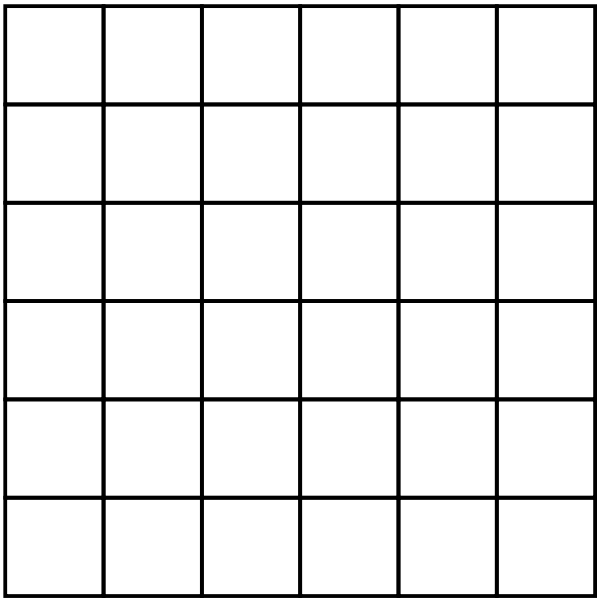
E	O	V	O	O	R
S	M	S	R	I	M
A	C	R	H	K	D
T	E	I	R	O	E
X	N	X	T	P	A
U	Y	F	D	V	L

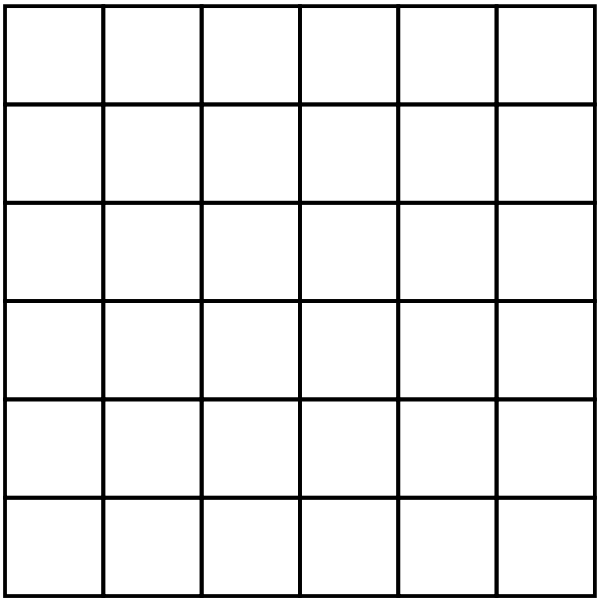
Version vom 2019-06-11

Vorlagen für Texte und Schablonen









Zum Basteln eigener Schablonen schneide bitte die Quadrate aus. Schneide dann noch einzelne kleine Kästchen aus.

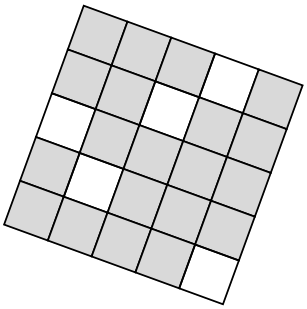
Version vom 2019-06-11

Aufgabe 1 Du findest an der Station einige verschlüsselte Nachrichten. Kannst du sie mit den Schablonen entschlüsseln?

Aufgabe 2 Schreibt euch gegenseitig eine Nachricht mit einer der Schablonen an der Station.

Aufgabe 3 Erkennst du das Muster, wie eine solche Schablone aufgebaut ist?
Überlege dir die Antwort anhand folgender Hilfsfragen: Wie dürfen die Löcher angeordnet sein? Wie viele Kästchen musst du ausschneiden, damit am Ende alle Kästchen komplett mit Buchstaben ausgefüllt sind? Wenn ein Kästchen ausgeschnitten ist, welche anderen Kästchen dürfen dann nicht ausgeschnitten werden?

Aufgabe 4 Entwirf selbst eine Schablone und verschlüssele mit deiner eigenen Schablone eine Nachricht.



Lösung 1

Text oben links:
DER BRIEF LIEGT IN DER UNTERSTEN SCHUBLADE (Schablone 3)
Text oben rechts:
DIE NACHRICHT ZERSTOERT SICH IN 5 SEKUNDEN (Schablone 1)
Text unten:
VORSICHT VOR DER EXPLOSION AUF DEM MARKT (Schablone 2)

Lösung 2

Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Lösung 3

Einen Vorschlag für die Lösung siehst du in der nachfolgenden Abbildung. Hier sind vier Ringe dargestellt. Du darfst bei der Schablonenproduktion aus jedem Ring jede Zahl nur einmal als Fenster verwenden.

1	2	3	4	5	1
5	1	2	3	1	2
4	3	1	1	2	3
3	2	1	1	3	4
2	1	3	2	1	5
1	5	4	3	2	1

Du drehst die Schablone nach jedem Schritt um 90 Grad. D.h. du füllst viermal Kästchen aus oder liest diese aus. Also kannst du insgesamt ein Viertel der Kästchen ausschneiden.

Lösung 4

Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Version vom 2019-06-11

Pflügen

Transposition

Die Buchstaben bleiben, **was** sie sind, aber nicht, **wo** sie sind.
Solche Verschlüsselungen heißen **Transposition**. (Das Wort *Transposition* ist abgeleitet vom lateinischen Wort *transponere* = verschieben.)

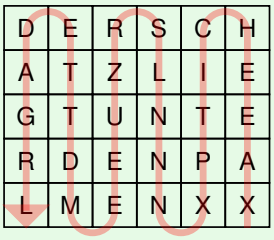
Das Pflügen zeigt dir, wie man durch Anordnen und Neuordnen von Buchstaben verschlüsseln kann. Pflügen geht so:

- Lege fest, wieviele Buchstaben in eine Zeile geschrieben werden sollen. Das ist der Schlüssel.
- Schreibe deinen Text auf, aber in jede Zeile nur so viele Buchstaben, wie vorher festgelegt. Die letzte Zeile wird mit beliebigen Buchstaben aufgefüllt.
- Der verschlüsselte Text entsteht, indem du nun die letzte Spalte von unten nach oben aufschreibst, danach die vorletzte Spalte von oben nach unten und so weiter.

Beispiel Der Text **DER SCHATZ LIEGT UNTER DEN PALMEN** soll verschlüsselt werden. Du wählst als Schlüssel zum Beispiel die **6** und schreibst die Buchstaben so auf:

D	E	R	S	C	H
A	T	Z	L	I	E
G	T	U	N	T	E
R	D	E	N	P	A
L	M	E	N	X	X

Ist die Nachricht zu kurz, dann wird einfach mit beliebigen Buchstaben aufgefüllt, bis der Kasten voll ist. Wie der Pfeil zeigt, schreibst du die Buchstaben nun ab. Die Reihenfolge ähnelt dem Pflügen eines Felds.



Du schickst die Nachricht **XAEEHCITPXNNNLSRZUEEMDTTEDAGRL** ab.

Version vom 2019-08-09

Aufgabe 1 Versuche, die folgende »gepflügte« Nachricht zu entschlüsseln. Der Schlüssel ist **6**.

X G C N E I T M I S R S E H I E H T C I D A H E

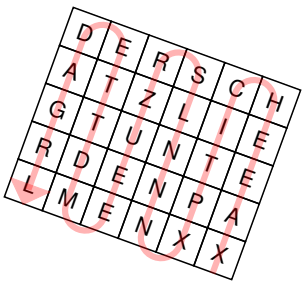
Aufgabe 2 Beschreibe, wie du eine empfangene Nachricht mit bekanntem Schlüssel (= Anzahl Buchstaben pro Zeile) entschlüsseln kannst.

Aufgabe 3 Schreibt euch gegenseitig eine Nachricht! Einigt euch auf den Schlüssel (= Anzahl Buchstaben pro Zeile)!

Aufgabe 4 Kannst du den folgenden Text ohne bekannten Schlüssel entschlüsseln? Du fängst eine Nachricht ab und möchtest herausbekommen, was darin steht. Du weißt, dass »Pflügen« als Verschlüsselungsverfahren benutzt wurde. Hier ist die Nachricht:

H I H A N N K E G C E C A O I T K S A C S N S F N T R I A D

Tipp: Die Anzahl der Buchstaben ist immer durch die zuvor festgelegte Anzahl von Buchstaben pro Zeile teilbar.



Version vom 2019-06-11

Lösung 1 Der Schlüssel ist 6. Da der Text 24 Zeichen hat, ergibt sich daraus ein 6x4 Rechteck. Also fange ich nach dem Pflügen-Schema rechts unten mit dem »X« an und gehe von dort aus vier Zeichen nach oben, dann in Schlangenlinien die nächste Spalte nach unten, usw. So ergibt sich das folgende Schema:

D I E S E N
A C H R I C
H T I S T G
E H E I M X

Die Nachricht lautet: Diese Nachricht ist geheim.

Lösung 2 Das Verfahren ist umgekehrt zum Verschlüsselungsvorgang. Anhand des bekannten Schlüssels und der Nachrichtenlänge kann man die Größe des Rechtecks ermitteln. Der Schlüssel entspricht der Spaltenanzahl. Die Nachrichtenlänge geteilt durch den Schlüssel ergibt die Zeilenanzahl. In dieses Rechteck wird die verschlüsselte Nachricht nach folgendem Verfahren eingetragen: Man fängt nach dem Pflügen-Schema rechts unten mit dem ersten Buchstaben an und geht von dort aus die errechnete Zeilenanzahl nach oben, dann in Schlangenlinien die nächste Spalte nach unten und so weiter. Die Nachricht kann dann von links nach rechts und Zeile für Zeile gelesen werden.

Lösung 3 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Lösung 4 Es sind 30 Buchstaben. 4 als Schlüssel scheidet damit aus. 5, 6 und 10 sind mögliche Schlüssel. Ausprobieren mit 5:

D A S K N
A C K E N
I S T G A
R N I C H
T S O E I
N F A C H

Schlüssel 5 klappt also direkt.

Lösung: **DAS KNACKEN IST GAR NICHT SO EINFACH**

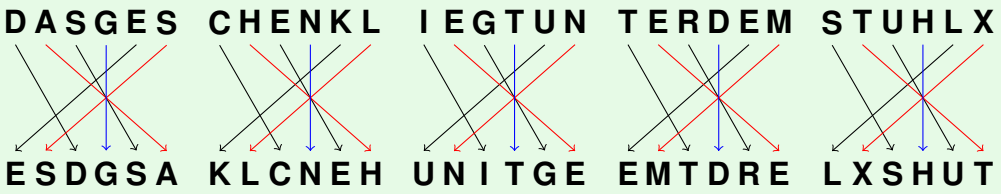
Die Buchstaben bleiben, **was** sie sind, aber nicht, **wo** sie sind.
Solche Verschlüsselungen heißen **Transposition**. (Das Wort *Transposition* ist abgeleitet vom lateinischen Wort *transponere* = verschieben.)

Bei einer Blockverschlüsselung wird eine Nachricht ohne Leerzeichen in Blöcke einer festen Länge unterteilt. Ist die Nachricht zu kurz, werden Füllbuchstaben ans Ende gesetzt. Es gibt verschiedene Möglichkeiten, die Blöcke zu verschlüsseln. Wir betrachten den Modus *Elektronic Code Book (ECB)*, bei dem jeder Block von den anderen unabhängig verschlüsselt wird. Dafür benutzen wir als Schlüssel Permutationen. Eine Permutation vertauscht die Buchstaben eines Textes auf eine vorgegebene Weise. Dabei schreiben wir die Permutation auf, indem wir die neuen Stellen der Buchstaben unter die alten Stellen schreiben.

Beispiel Für die Blocklänge 6 und die Permutation

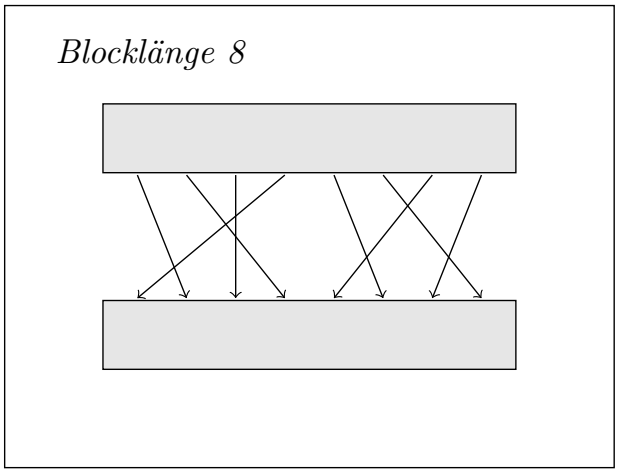
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix}$$

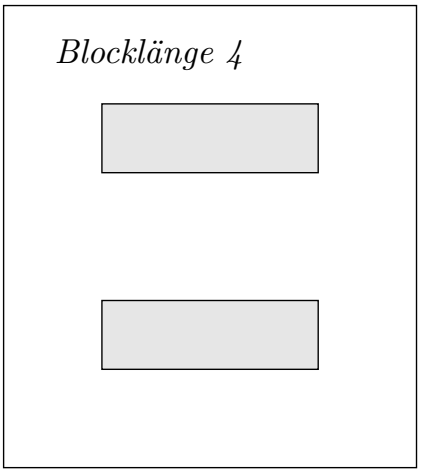
schreiben wir den ersten Buchstaben auf die dritte Stelle, den zweiten Buchstaben auf die sechste Stelle, den dritten Buchstaben auf die fünfte Stelle, den fünften Buchstaben auf die erste Stelle und den sechsten Buchstaben auf die zweite Stelle. Der vierte Buchstabe bleibt dabei einfach stehen.
Also wird die Nachricht **DAS GESCHENK LIEGT UNTER DEM STUHL** verschlüsselt zu **ESDGSAKLCNEHUNITGEEMTDRELXSHUT**. Dies sieht man besser, wenn man die Nachricht in Blöcke einteilt und mit Pfeilen zeigt, welche Buchstaben an welche Stellen geschoben werden:

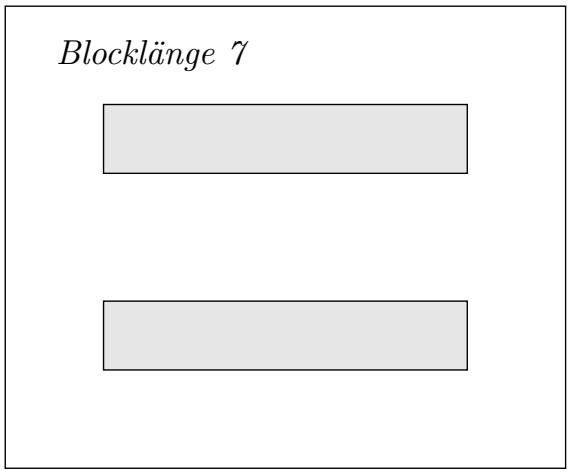


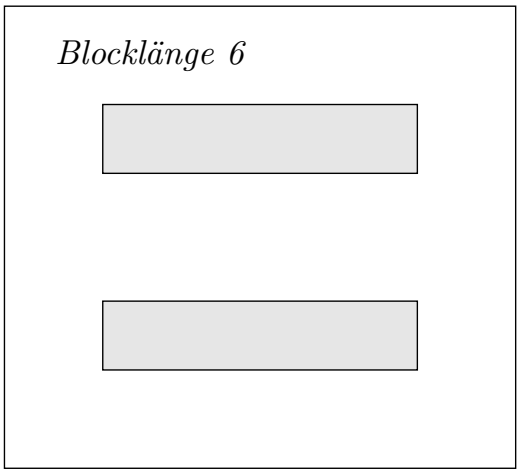
Die Anordnung der Pfeile einer Permutation bleibt bei jedem Block gleich. Deswegen können wir die Permutationshilfen nutzen, um Nachrichten schneller und korrekt zu verschlüsseln. Dabei ist es wichtig, dass du die Buchstaben nicht zu nah aneinander schreibst. Nutze dafür die Vorlage für Texte und schreibe in jedes Kästchen genau einen Buchstaben. Lege dann die Permutationshilfe der richtigen Blocklänge mit dem oberen Fenster auf den Block des Klartextes und schreibe die Buchstaben dann entsprechend der Pfeile in das untere Fenster.

Vorlage für Permutationshilfen





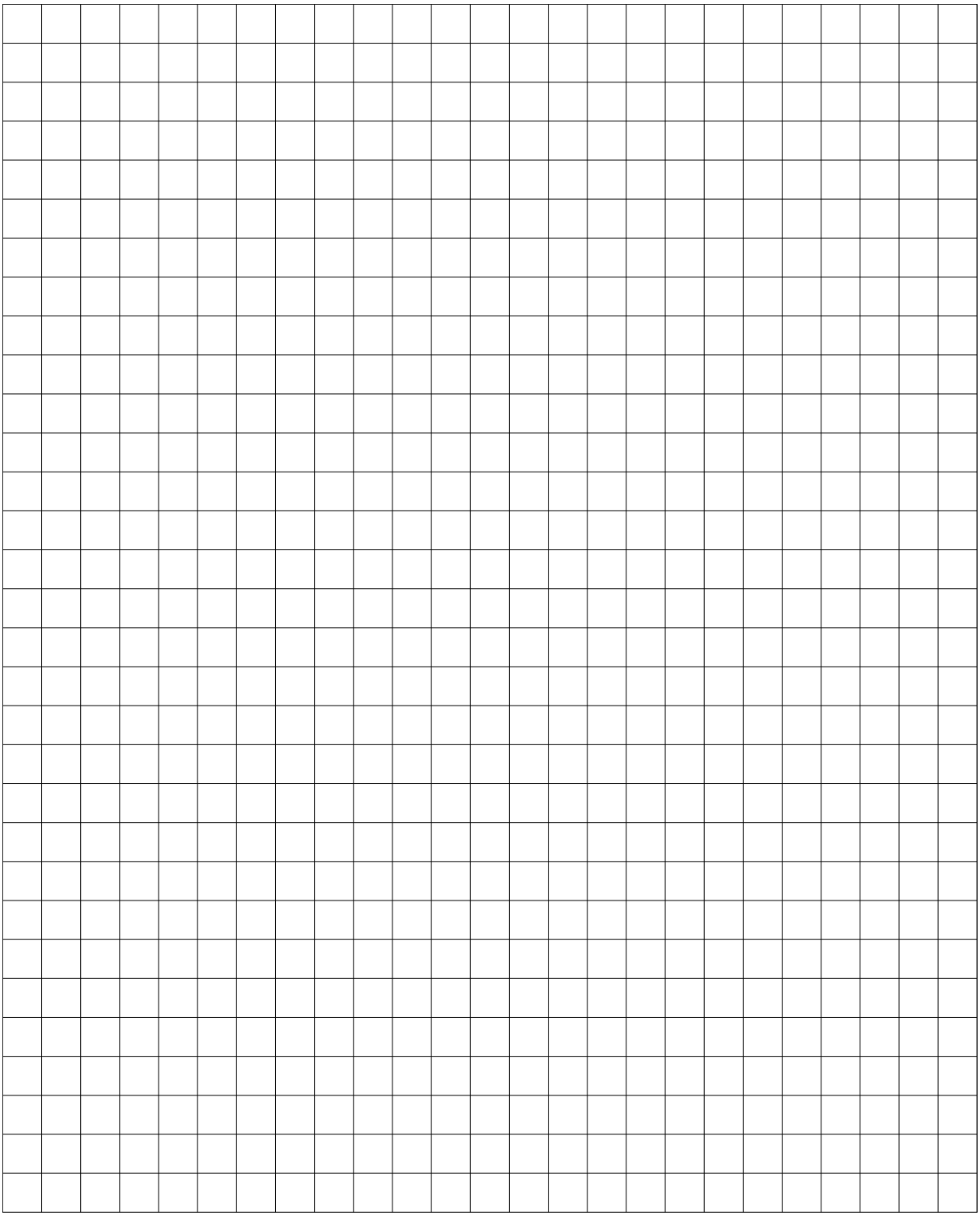




Die Permutationshilfen und die Fenster (die dunklen Felder) ausschneiden und laminieren. Anschließend die Fenster wieder ausschneiden, damit durch sie geschrieben werden kann. Auf die laminierten Oberflächen können dann die Permutationen geschrieben werden.

Version vom 2019-08-06

Vorlagen für Texte



Version vom 2019-08-03

Aufgabe 1 Nimm dir die Permutationshilfe mit Blocklänge 8 und der aufgezeichneten Permutation. Verschlüssele **WIR TREFFEN UNS UM DREI UHR**, indem du Leerzeichen auslässt und Füllbuchstaben am Ende der Nachricht einfügst.

Aufgabe 2 Beschreibe, wie du eine empfangene Nachricht mit bekanntem Schlüssel (Permutation) entschlüsseln kannst.

Aufgabe 3 Entschlüssele die Nachricht **TDREFRFEKPNUSTTIAAHMNFDE** mit dem vorgegebenen Schlüssel auf der Permutationshilfe mit Blocklänge 8.

Aufgabe 4 Zeichne die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix}$$

mit einem Folienstift auf die Permutationshilfe mit Blocklänge 6. Nutze dafür die Vorlage für Texte, um die Pfeile der Permutation richtig einzuzeichnen. Verschlüssele eine kurze Nachricht und lasse sie von jemandem entschlüsseln.

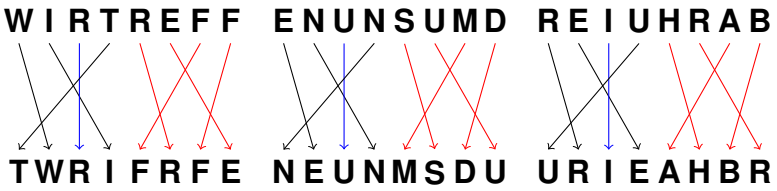
Aufgabe 5 Wählt eine Blocklänge (mit dazugehörige Permutationshilfe) und einen eigenen Schlüssel (Permutation) aus und schreibt euch gegenseitig eine Nachricht.

Aufgabe 6 Welche Schlüssel (Permutationen) sind mit Blocklänge 2 und 3 möglich?

Hinweis: Säubere die Permutationshilfen bitte nach Abschluss deiner Bearbeitung, damit die oder der Nächste von neu beginnen kann.

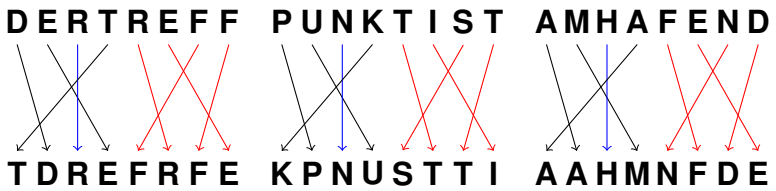
Version vom 2019-08-03

Lösung 1 Durch verschiedene Füllbuchstaben kann der letzte Block variieren. Die Lösung kann zum Beispiel so aussehen:



Lösung 2 Das Verfahren ist umgekehrt zum Verschlüsselungsvorgang. Man teilt die Nachricht in Blöcke der bekannten Länge und wendet den Schlüssel (= Permutation) umgekehrt an. Das bedeutet, die Permutation wird von unten nach oben gelesen. Bei der Permutationshilfe legt man das untere Fenster auf die Nachricht und schreibt die Buchstaben dann entsprechend gegen die Pfeilrichtung in das obere Fenster.

Lösung 3 Die entschlüsselte Nachricht lautet **DER TREFFPUNKT IST AM HAFEN**.



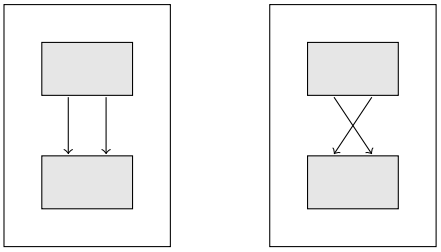
Lösung 4 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Lösung 5 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Version vom 2019-08-06

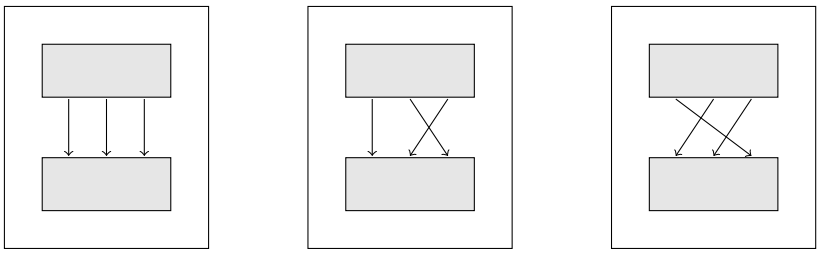
Lösung 6 Für die Blocklänge 2 gibt es zwei Schlüssel (Permutation), aber nur eine davon ist für eine Verschlüsslung sinnvoll. Die beiden Buchstaben werden dabei einfach vertauscht. Die Permutationen sehen so aus:

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

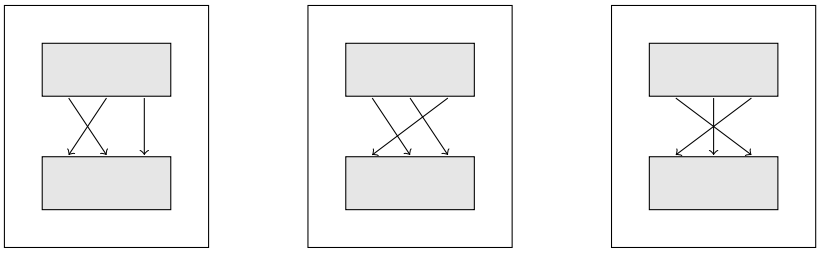


Für die Blocklänge 3 gibt es 6 mögliche Schlüssel (Permutationen). Dabei ist wieder eine nicht sinnvoll:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$



$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

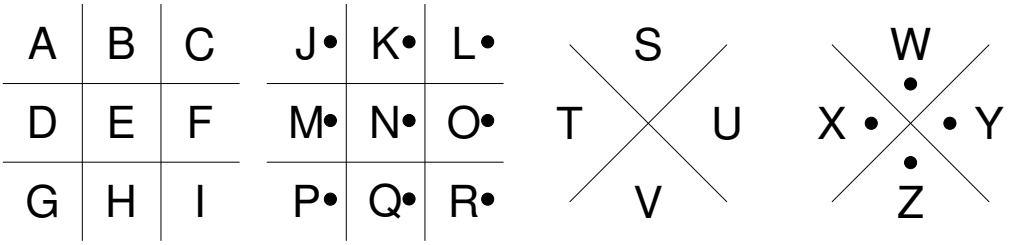


Freimaurer-Chiffre

Substitution (monoalphabetisch)

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind.
Solche Verschlüsselungen heißen **Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen.)

Diese Verschlüsselung, die im 18. Jahrhundert von den Freimaurern - einem Geheimbund - benutzt wurde, funktioniert so:
Zunächst schreibt man eine beliebige Reihenfolge aller Buchstaben des Alphabets in vier bestimmte Muster. Im folgenden Bild wurde die Reihenfolge von A bis Z genommen.



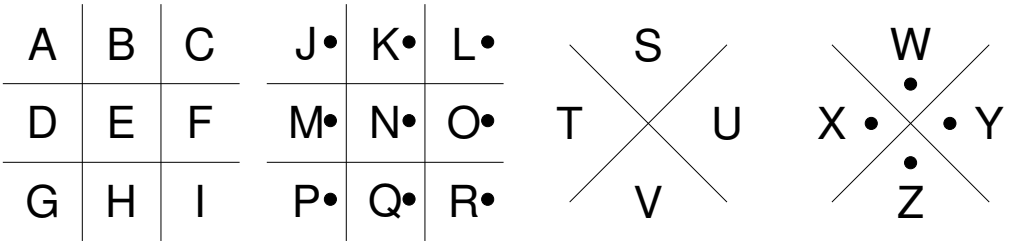
Zum Verschlüsseln wird jeder Buchstabe durch die Linien und Punkte ersetzt, die ihn umgeben.

Beispiel Schau dir das Bild oben an. Die Linien und Punkte, die beim **N** stehen, sehen in etwa so aus: ⊡. **N** wird immer durch dieses Zeichen ersetzt.

Aufgabe 1 Kannst du folgenden Text entschlüsseln?

Aufgabe 2 Schreibt euch eine Nachricht mit dem Freimaurer-Chiffre.

Aufgabe 3 Wie kann man ohne Schlüssel die Nachrichten entziffern?



Lösung 1 **VERSUCH DEIN GLUECK**

Lösung 2 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Lösung 3 Über eine Häufigkeitsanalyse. Man schaut nach, welches das häufigste Zeichen ist. Das könnte das »E« sein. Ebenso verfährt man mit dem zweithäufigsten Zeichen, und so weiter. Du brauchst dazu eine Tabelle, wie häufig jeder Buchstabe in einer bestimmten Sprache vorkommt. Ein Ausprobieren aller Kombinationen wäre viel zu aufwändig.

Version vom 2019-06-14

Caesar

Substitution (monoalphabetisch)

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind.
Solche Verschlüsselungen heißen **Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen.)

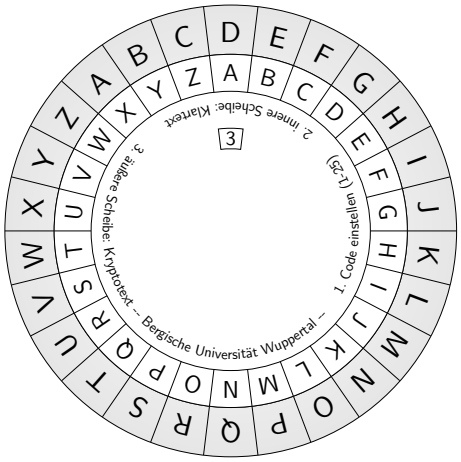
Der römische Feldherr Julius Caesar (100 bis 44 v. Chr.) verschlüsselte seine geheimen Nachrichten, indem er jeden Buchstaben durch einen anderen ersetzte. Dabei wurde der Buchstabe immer durch den um eine bestimmte Anzahl von Stellen im Alphabet verschobenen Buchstaben ersetzt. Diese Anzahl der Stellen heißt **Caesar-Schlüssel**.

Beispiel Beim Schlüssel **3** nahm Caesar immer den Buchstaben, der im Alphabet drei Stellen weiter rechts steht.
Dazu schrieb er das Alphabet zweimal untereinander. Das untere Alphabet schrieb er allerdings um drei Stellen verschoben.

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

Caesar ersetzte also in seinem Text jedes **A** durch ein **D**, jedes **B** durch ein **E** usw. Beachte, dass **X** durch **A** ersetzt wird, also das Alphabet nach dem Z einfach mit A weitergeschrieben wird.

Damit nicht jedesmal die beiden gegeneinander verschobenen Alphabete aufgeschrieben werden müssen, kann auch eine sogenannte Chiffrierscheibe benutzt werden. In der Abbildung ist wie im Beispiel der Schlüssel 3 eingestellt.
Mit der Scheibe kannst du nun sowohl Texte verschlüsseln als auch entschlüsseln. Möchtest du verschlüsseln, dann suchst du den Buchstaben auf der inneren Scheibe und schreibst den entsprechenden Buchstaben auf der äußeren Scheibe auf. Entschlüsseln geht entsprechend umgekehrt: Hier suchst du den Buchstaben außen und schreibst den entsprechenden Buchstaben auf der inneren Scheibe auf.



Caesar

Substitution (monoalphabetisch)

Die »normale« Caesar-Verschlüsselung ist ziemlich leicht zu »knacken«. Etwas schwieriger wird es, wenn das Verfahren mit einem Schlüsselwort kombiniert wird.
Diese Verschlüsselung funktioniert so:

- Sender und Empfänger einigen sich auf ein Schlüsselwort.
- Dieses Wort schreibst du unter ein normales Alphabet. Buchstaben, die doppelt vorkommen, lässt du dabei weg.
- Anschließend wird das Alphabet mit den noch nicht benutzten Buchstaben, in alphabetischer Reihenfolge beim letzten Buchstaben des Schlüsselworts beginnend, aufgefüllt. Kein Buchstabe darf doppelt vorkommen.

Beispiel Schlüsselwort: GEHEIMSCHRIFT. Dieses Schlüsselwort wird unter das Alphabet geschrieben, doppelte Buchstaben werden dabei weggelassen.

	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
wird ersetzt durch	G	E	H	I	M	S	C	R	F	T																

Nun wird mit den restlichen Buchstaben aufgefüllt.

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

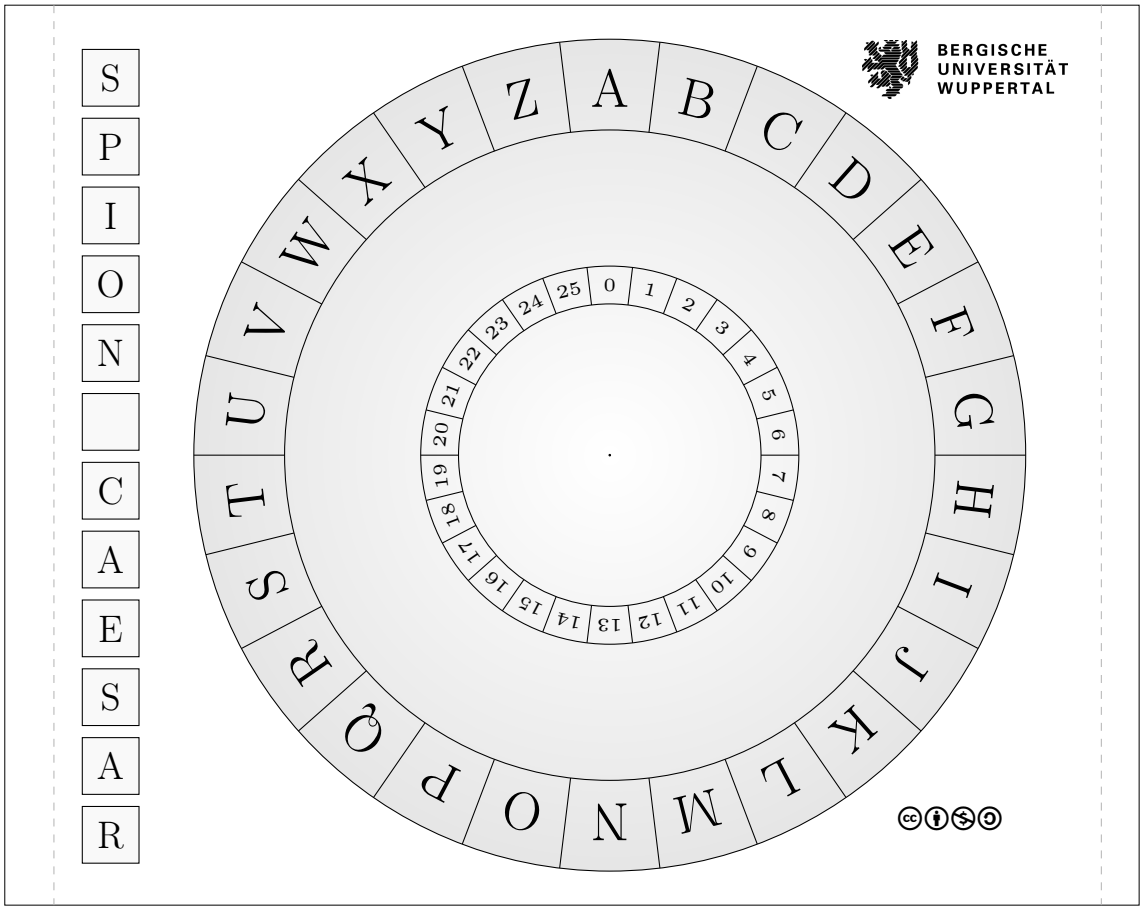
Mit dieser Tabelle wird dann ver- und entschlüsselt.

Version vom 2019-08-09

BERGISCHE UNIVERSITÄT WUPPERTAL

Caesar

Substitution (monoalphabetisch)



Caesar

Substitution (monoalphabetisch)

Bergische Universität Wuppertal - SpionCamp - Caesar

S P I O N _ C A E S A R

Verschlüsseln

Stelle den Caesarcode (1-25) mit der inneren Scheibe ein. Nimm den Klartext und schaue jeden Buchstaben auf der inneren Scheibe nach. Auf der äußeren Scheibe steht der entsprechende Geheimtext.

Entschlüsseln

Stelle den Caesarcode (1-25) mit der inneren Scheibe ein. Nimm den Geheimtext und schaue jeden Buchstaben auf der äußeren Scheibe nach. Auf der inneren Scheibe steht der entsprechende Klartext.

BERGISCHE UNIVERSITÄT WUPPERTAL

Bergische Universität Wuppertal - SpionCamp - Caesar

S P I O N _ C A E S A R

- Beim Ausdruck darauf achten, dass das Dokument nicht skaliert gedruckt wird (CD-Hüllenbreite: 15cm)
- Durchmesser großes Rad: 11cm, klein: 8,6cm
- Laminieren der kleinen Scheibe empfohlen!
- Kleines Rad ausschneiden und graues Code-Fenster (X) ausschneiden
- Falls eine CD-Hülle verwendet wird: Den inneren Ring aus dem kleinen Rad herausschneiden
- Großes Rad mit dem CD-Hüllen-Rand oder ohne diesen ausschneiden
- Falls keine CD-Hülle verwendet wird: die Scheiben mit einer Musterbeutelklammer  verbinden

Aufgabe 1 Entschlüsselt mit der Chiffrierscheibe die folgenden Nachrichten. Mögliche Schlüssel sind: **2**, **7**, **10**, **13**. Einer ist jeweils der richtige Schlüssel. Das heißt, dass man bei Verschiebung um diese Zahl die Nachricht erhält.

a) **SPLIL RSLVWHAYH, AYLMMLU DPY BUZ ILP KLU WFYHTPKLU?**

b) **YVRORE PNRFNE, VPU JREQR QN FRVA.**

Aufgabe 2 Könnt ihr die Nachricht ohne bekannten Schlüssel entschlüsseln?
YHQL YLGL YLFL

Aufgabe 3 Warum ist dieses Verschlüsselungsverfahren leicht zu »knacken«?

Aufgabe 4 Verschlüsselt und entschlüsselt gegenseitig den Titel eures Lieblingsbuches mit dem Schlüsselwort **LESERATTE**.

Aufgabe 5 Entschlüssele die folgende Nachricht. Das Schüsselwort ist **SCHATZSUCHE** oder **MEISTERDETEKTIV**.

STG HIKMJU YVTDJ KVAJTG STG CMGXEMAX

Aufgabe 6 Was ist der Vorteil bei dem Schlüsselwort-Caesar-Verfahren?

Aufgabe 7 Fällt dir eine Möglichkeit ein, wie du einen Text entschlüsseln kannst, ohne alle Schlüssel durchzuprobieren? *Tipp:* Nutze dabei eine bestimmte Eigenschaft einer Sprache (z. B. Deutsch) aus.

Version vom 2019-06-11

Lösung 1

a) Schlüssel 7:
LIEBE KLEOPATRA, TREFFEN WIR UNS BEI DEN PYRAMIDEN?

b) Schlüssel 13:
LIEBER CAESAR, ICH WERDE DA SEIN.

Lösung 2

VENI VIDI VICI (Lateinisch: Ich kam, ich sah, ich siegte. Dies schrieb Julius Caesar in einem Brief an Gaius Matius, nachdem er die Truppen Pharnakes II. von Pontus in nur vier Stunden besiegte.)

Lösung 3

Man muss höchstens 25 Schlüssel durchprobieren, um die Lösung zu erhalten.

Lösung 4

Die Ersetzungstabelle sieht so aus:

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

So wird zum Beispiel aus CRYPTONOMICON:
SHPFJDCDBWSDC.

Lösung 5

Schlüssel ist **MEISTERDETEKTIV**:

DER SCHATZ LIEGT HINTER DER PARKBANK

Die Ersetzungstabelle sieht so aus:

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

Lösung 6

Allein durch Ausprobieren von 25 Schlüsseln ist das Verfahren nicht zu knacken.

Lösung 7

Häufigkeitsanalyse: In der Deutschen Sprache ist der häufigste Buchstabe das »E«. Der häufigste Buchstabe im Geheimtext könnte also dem E entsprechen.

Version vom 2019-06-11

Playfair

Substitution (bigraphisch)

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. Es werden nicht einzelne Buchstaben, sondern Buchstaben**paare** verschlüsselt. Solche Verschlüsselungen heißen **bigraphische Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen. *Bi* heißt *zwei* und *graphisch* kommt vom griechischen *graphein* = schreiben.)

Der englische Physiker Charles Wheatstone (s. Bild) erfand 1854 eine Verschlüsselung, bei der immer zwei Buchstaben auf einmal verschlüsselt werden. Sein Freund, der Politiker Lord Lyon Playfair Baron von St. Andrews, führte diese Verschlüsselung in die militärischen und diplomatischen Kreise Englands ein. Das Verschlüsselungsverfahren wurde schließlich nach jenem Politiker benannt.

Erklärung am Beispiel:

1. Sender und Empfänger einigen sich auf ein Schlüsselwort. Dieses wird in ein 5×5-Quadrat (mehrfache Buchstaben weglassen!) geschrieben. **I** und **J** werden dabei nur als ein Buchstabe gezählt. Der Rest des Alphabets wird fortlaufend dahintergeschrieben.

Beispiel Für das Schlüsselwort **PLAYFAIR** sieht die Verschlüsselungsmatrix wie folgt aus:

p	l	a	y	f
i/j	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

2. Die Nachricht wird in Zweiergruppen aufgeschrieben. Dabei darf nie zweimal der gleiche Buchstabe in einer Gruppe stehen. Passiert das, wird ein **X** eingefügt. Steht am Ende ein Buchstabe allein, wird ein **X** angehängt.

Beispiel Nachricht: **HALLO CHARLES** wird zu **HA LX LO CH AR LE SX**

3. Nun werden diese Buchstabenpaare ersetzt. Wodurch sie ersetzt werden, hängt davon ab, wo sie im Quadrat stehen:
   - Stehen beide Buchstaben in derselben Zeile, werden sie jeweils durch ihren Nachfolger in der Zeile ersetzt. (Nachfolger des letzten ist der erste Buchstabe.)
   - Stehen beide Buchstaben in derselben Spalte, werden sie jeweils durch ihren Nachfolger in der Spalte ersetzt. (Nachfolger des letzten ist der erste Buchstabe.)
   - Stehen die Buchstaben in verschiedenen Zeilen und Spalten, wird der obere der beiden durch den Buchstaben ersetzt, der in derselben Zeile wie der obere und in derselben Spalte wie der untere Buchstabe steht. Der untere wird durch den Buchstaben ersetzt, der in derselben Zeile wie der untere und in derselben Spalte wie der obere Buchstabe steht.

Beispiel

HA wird zu **QB** (gleiche Spalte)
LX wird zu **YV**:

p	l	a	y	f
i/j	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

LO wird zu **RV** (gleiche Spalte)
CH wird zu **BK**
AR wird zu **LB**
LE wird zu **PG**
SX wird zu **XY** (gleiche Spalte)

Verschlüsselte Nachricht: **QBYVRVBKLBPGXY**

BERGISCHE UNIVERSITÄT WUPPERTAL

Aufgabe 1 Verschlüsselt euren Namen mit dem Schlüsselwort **FUCHS**.

Aufgabe 2 Entschlüsselt folgenden Text. Das Schlüsselwort ist **WOLKENBRUCH**:

YF DF BD WT ZG DI BD WY MI NG

Aufgabe 3 Beschreibe das Verfahren für das Entschlüsseln der Nachricht? Was ist hier anders?

Aufgabe 4 Verschlüsselt euch gegenseitig mit einem ausgehandelten Schlüsselwort einen Text. Entschlüsselt die Nachricht!

Version vom 2019-06-11

Lösung 1

Playfair-Matrix für FUCHS:

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

Z. B. ist **ANNA** verschlüsselt **GIIG**.

Lösung 2

Playfair-Matrix für WOLKENBRUCH:

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

Lösung: **QUADRATISCH PRAKTISCH**

Lösung 3 Diese Entschlüsselung geht so:

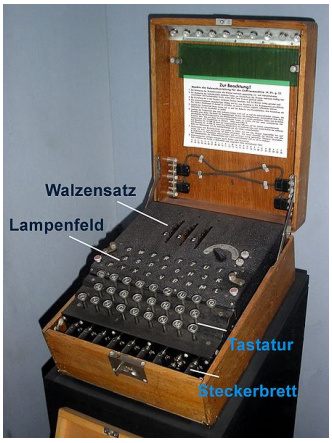
- Der Empfänger muss das Schlüsselwort kennen. Dieses wird in ein 5×5-Quadrat (mehrfache Buchstaben weglassen!) geschrieben. **I** und **J** werden dabei nur als ein Buchstabe gezählt. Der Rest des Alphabets wird fortlaufend dahintergeschrieben.
- Die verschlüsselte Nachricht wird in Zweiergruppen aufgeschrieben.
- Nun werden diese Buchstabenpaare ersetzt. Wodurch sie ersetzt werden, hängt davon ab, wo sie im Quadrat stehen:
  - Stehen beide Buchstaben in derselben Zeile, werden sie jeweils durch ihren Vorgänger in der Zeile ersetzt. (Vorgänger des ersten ist der letzte Buchstabe.)
  - Stehen beide Buchstaben in derselben Spalte, werden sie jeweils durch ihren Vorgänger in der Spalte ersetzt. (Vorgänger des ersten ist der letzte Buchstabe.)
  - Stehen die Buchstaben in verschiedenen Zeilen und Spalten, wird der obere der beiden durch den Buchstaben ersetzt, der in derselben Zeile wie der obere und in derselben Spalte wie der untere Buchstabe steht. Der untere wird durch den Buchstaben ersetzt, der in derselben Zeile wie der untere und in derselben Spalte wie der obere Buchstabe steht.

Lösung 4 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Rotoren

Substitution (polyalphabetisch)

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. **Was** sie sind, ist immer wieder verschieden.
Solche Verschlüsselungen heißen **polyalphabetische Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen. *Poly* heißt *viel*.)



Die berühmteste Rotor-Maschine zur Verschlüsselung ist die **ENIGMA**, die vom deutschen Militär im zweiten Weltkrieg eingesetzt wurde. Das Wort »Enigma« kommt aus dem Griechischen und bedeutet »Rätsel«. Das Prinzip beruht auf einer drehbaren Scheibe, die jeden Buchstaben durch einen anderen ersetzt, dann gedreht wird und nun jeden Buchstaben durch einen anderen als zuvor ersetzt. Die Enigma hatte mehrere Scheiben. Sie wurde erst nach einigen Jahren durch intensive mathematische Forschung geknackt.

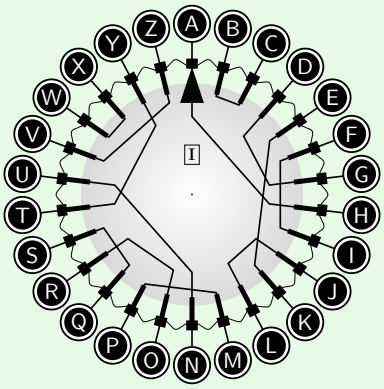
So wird mit Rotoren verschlüsselt:

- Sender und Empfänger einigen sich auf einen Schlüsselbuchstaben.
- Der Rotor wird so eingestellt, dass der Pfeil auf den Schlüsselbuchstaben zeigt.
- Jeder Buchstabe der Nachricht wird durch den Buchstaben ersetzt, der sich am anderen Ende der auf dem Rotor eingezeichneten Verbindung befindet.
- Immer, wenn du einen Buchstaben verschlüsselt hast, wird der Rotor im Uhrzeigersinn eine Position weiter gedreht.

Zum Entschlüsseln muss erneut der Schlüsselbuchstabe eingestellt werden, dann wird von vorn bis hinten entschlüsselt.

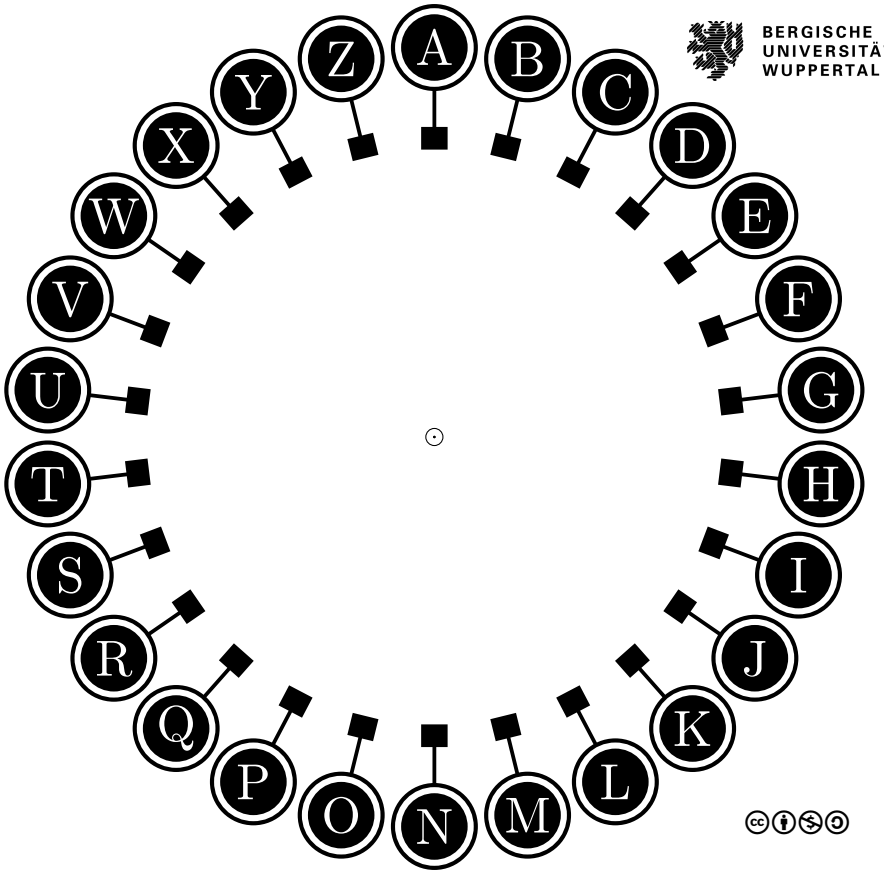
Beispiel

Der Schlüsselbuchstabe ist hier »A«. Möchtest du nun den Buchstaben »S« verschlüsseln, so folgst du der Linie bei »S« und landest bei »Q«. Dann wird der Rotor um eine Position nach rechts gedreht, der Pfeil steht nun auf dem B. Dann verschlüsselst du den nächsten Buchstaben. Die Verbindungen der Buchstaben haben sich nun auch verschoben, so dass z. B. als zweiter Buchstabe ein »C« durch ein »D« verschlüsselt wird.



S P I O N

E N I G M A



BERGISCHE UNIVERSITÄT WUPPERTAL

S P I O N

E N I G M A

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

BERGISCHE UNIVERSITÄT WUPPERTAL

Bergische Universität Wuppertal - SpionCamp - Rotor I

S
P
I
O
N

E
N
I
G
M
A

Verschlüsseln

Nimm den Klartext und drehe den Rotor mit dem Pfeil auf den Schlüsselbuchstaben. Auf diesen müssen sich Sender und Empfänger vorher einigen. Suche den zu verschlüsselnden Buchstaben und folge der Linie. Am Ende der Linie steht der Geheimtext. Nach jedem Buchstaben drehst du die Scheibe um eine Position im Uhrzeigersinn.

Entschlüsseln

Nimm den Geheimtext und drehe den Rotor mit dem Pfeil auf den Schlüsselbuchstaben. Auf diesen müssen sich Sender und Empfänger vorher einigen. Suche den zu entschlüsselnden Buchstaben und folge der Linie. Am Ende der Linie steht der Klartext. Nach jedem Buchstaben drehst du die Scheibe um eine Position im Uhrzeigersinn.

Bergische Universität Wuppertal - SpionCamp - Rotor I

S
P
I
O
N

E
N
I
G
M
A

Bergische Universität Wuppertal - SpionCamp - Rotor II

S
P
I
O
N

E
N
I
G
M
A

Verschlüsseln

Nimm den Klartext und drehe den Rotor mit dem Pfeil auf den Schlüsselbuchstaben. Auf diesen müssen sich Sender und Empfänger vorher einigen. Suche den zu verschlüsselnden Buchstaben und folge der Linie. Am Ende der Linie steht der Geheimtext. Nach jedem Buchstaben drehst du die Scheibe um eine Position im Uhrzeigersinn.

Entschlüsseln

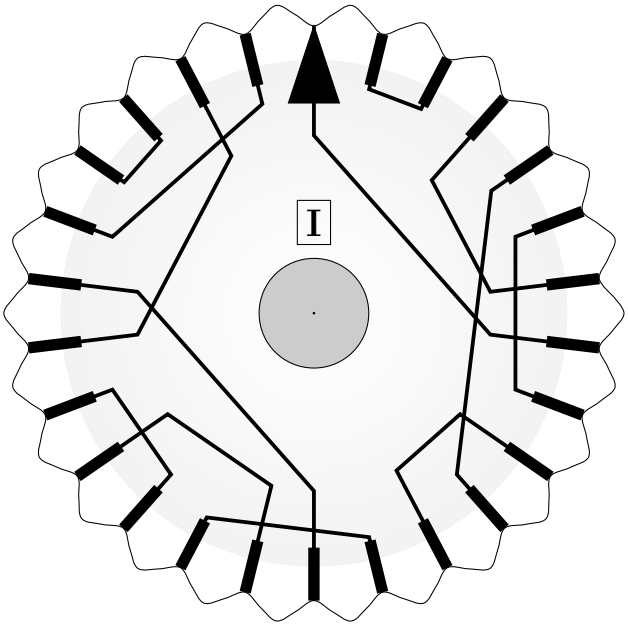
Nimm den Geheimtext und drehe den Rotor mit dem Pfeil auf den Schlüsselbuchstaben. Auf diesen müssen sich Sender und Empfänger vorher einigen. Suche den zu entschlüsselnden Buchstaben und folge der Linie. Am Ende der Linie steht der Klartext. Nach jedem Buchstaben drehst du die Scheibe um eine Position im Uhrzeigersinn.

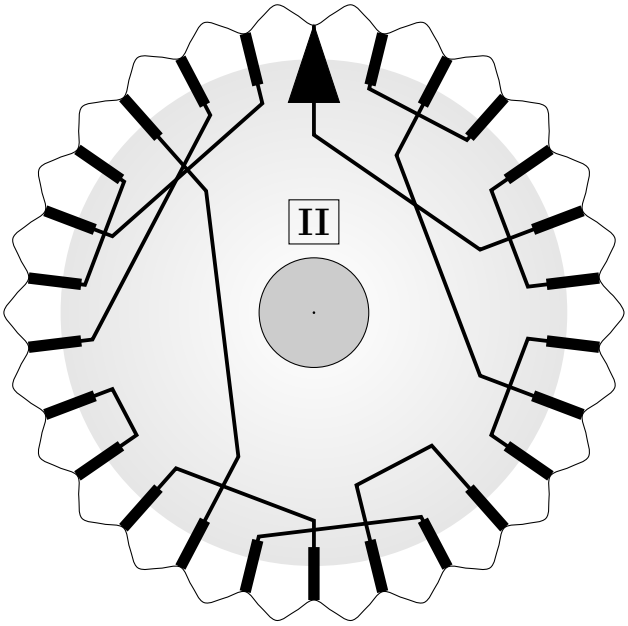
CC BY NC SA

Bergische Universität Wuppertal - SpionCamp - Rotor II

S
P
I
O
N

E
N
I
G
M
A





Falls eine CD-Hülle verwendet werden soll: den inneren Ring aus dem kleinen Rad herausschneiden. Falls keine CD-Hülle vorhanden ist, können Musterbeutelklammern  verwendet werden.

Aufgabe 1 Arbeitet zu zweit: Verschlüsselt jeweils ein Wort mit dem Schlüsselbuchstaben **G**. Tauscht die Nachrichten aus und versucht, den Text wieder zu entschlüsseln.

Aufgabe 2 Entschlüssele folgende Texte:

a) **SOVLZUFTCNKGRVR** (Verwende Rotor I mit dem Schlüsselbuchstaben **C**.)

b) **IJMJQEHVY** (Verwende Rotor II und stelle den Schlüsselbuchstaben **L** ein.)

Aufgabe 3 Warum ist das Drehen so wichtig? Welche Art der Verschlüsselung entsteht, wenn der Rotor zwischen den Buchstaben nicht gedreht wird?

Aufgabe 4

a) Was passiert, wenn man z. B. die Nachricht **AAAA** verschlüsselt?

b) Schaffst du es, eine Nachricht zu schreiben, die verschlüsselt **XXXX** ergibt?

Aufgabe 5 (Schwierig) Was glaubst du, wie man eine Nachricht ohne Rotor knacken könnte? Könntest du folgenden Text entziffern: **DHKCGUVGR** ?

Version vom 2019-06-11

Lösung 1 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Lösung 2
a) **UM SIEBEN AM FLUSS**
b) **AB INS BETT**

Lösung 3 Dann kommen nur die fest verdrahteten Buchstaben zum Einsatz, also eine Tabelle mit Vertauschungen von Buchstaben. Das wäre sehr leicht mit einer einfachen Häufigkeitsanalyse zu knacken.

Lösung 4
a) Es wird jedes Mal ein anderer Buchstabe ausgegeben. Zum Beispiel wird mit dem Schlüsselbuchstaben A aus **AAAA** mit Rotor I **HWVZ** und mit Rotor II **FWVS**.
b) Rotor I, Schlüsselbuchstabe A: Klartext **WYBQ** ergibt **XXXX**. Rotor II, Schlüsselbuchstabe A: Klartext **PVBZ** ergibt **XXXX**.

Lösung 5 Man benötigt zunächst einen langen Geheimtext. Bei bekanntem Rotoraufbau kann man jeden 26. Buchstaben zu einem Text zusammenfassen und darüber eine Häufigkeitsanalyse durchführen. Ein Rotor ist also eine Ansammlung von Caesar-Verschlüsselungen.
Der Text war also viel zu kurz, um ihn zu entschlüsseln. Er wurde mit dem Rotor II und dem Schlüsselbuchstaben **S** verschlüsselt. Der Klartext lautet **GEHEIMNIS**.

Version vom 2019-06-11

Vigenère

Substitution (polyalphabetisch)

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind. **Was** sie sind, ist immer wieder verschieden.
Solche Verschlüsselungen heißen **polyalphabetische Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen. *Poly* heißt *viel*.)

Der Franzose Blaise de Vigenère (1523 bis 1596, s. Bild) entwickelte ein Verschlüsselungsverfahren, das viele verschobene Alphabete verwendet. Dazu werden alle möglichen Alphabetverschiebungen untereinander geschrieben — das sind 26 Alphabete. Das Ganze heißt dann **Vigenère-Quadrat** (s. Material).

Verschlüsseln geht damit so:

- Sender und Empfänger einigen sich auf ein Schlüsselwort. Dieses wird unter die Nachricht geschrieben. Unter jeden Buchstaben der Nachricht wird ein Buchstaben des Schlüsselwortes geschrieben. Das Schlüsselwort wird dabei ständig wiederholt.
- Nun nimmt man sich jeweils einen Buchstaben der Nachricht und den zugehörigen Buchstaben des Schlüsselwortes.
- Der Buchstabe im Vigenère-Quadrat, der in der Spalte des Klartextbuchstabens und der Zeile des Schlüsselbuchstabens liegt, ist der verschlüsselte Buchstabe.

Beispiel

Nachricht: `MORGEN ABEND UM NEUN GEHTS LOS`
Schlüsselwort: `EINFAC HEINF AC HEIN FACHE INF`
Geheimtext: `QWELEP HFMAI UO UICA LEJAW TBX`

(Bild: das erste **M** wird mit dem Schlüsselbuchstaben **E** verschlüsselt.)

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

Vigenère-Quadrat

Nimm dir für die Ver- und Entschlüsselung ein Lineal oder Ähnliches zur Hilfe, damit du nicht in den Spalten und Zeilen verrutschst.

Klartext

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

Aufgabe 1 Verschlüsselt euren Namen mit dem Schlüsselwort **HUT**.

Aufgabe 2 Entschlüsselt folgenden Text. Das Schlüsselwort ist **ROT**:
XIM XSFRQAK

Aufgabe 3 Beschreibe ähnlich zum Verschlüsseln, wie das Entschlüsseln funktioniert.

Aufgabe 4 Wählt ein beliebiges Schlüsselwort und schreibt euch gegenseitig eine Nachricht.

Version vom 2019-06-11

Lösung 1

Z. B. **MARIE**:

```
MARIE
HUTHU
TUKPY
```

Lösung 2

GUT GEMACHT

Lösung 3

Das Entschlüsseln geht genau umgekehrt: Das Schlüsselwort wird wieder unter die Nachricht geschrieben. Nun sucht man in der Zeile des Schlüsselwort-Buchstabens den verschlüsselten Buchstaben. Diese Spalte gehört zu dem entschlüsselten Buchstaben der Nachricht, der in der ersten Zeile steht.

Lösung 4

Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Strom-Chiffre

Substitution (polyalphabetisch)

Die Buchstaben bleiben, **wo** sie sind, aber nicht, **was** sie sind.
Solche Verschlüsselungen heißen **Substitution**. (Das Wort *Substitution* ist abgeleitet vom lateinischen Wort *substituere* = ersetzen.)

Bei einer Stromverschlüsselung benötigt man einen Startschlüssel. Aus dem Startschlüssel entsteht zusammen mit dem Klartext ein Schlüsselstrom. Das heißt eine Reihe von Schlüsseln, wovon wir uns aber nur den Startschlüssel merken müssen.
Wir betrachten den speziellen Fall der Autokey-Verschlüsselung. Diese wurde, wie die Vigenère-Verschlüsselung, vom Franzosen Blaise de Vigenère (1523 bis 1596, s. Bild) entwickelt. Bei der Autokey-Verschlüsselung wird an den Startschlüssel der Klartext gehangen. Also werden die einzelnen Buchstaben zum Schlüssel für folgende Buchstaben.

Hinweis: Solltest du die Vigenère-Station noch nicht bearbeitet haben, macht es Sinn, dies zuerst zu tun, damit du Verbindungen ziehen kannst. Ansonsten wirst du das erste Beispiel nicht verstehen, kannst diese Station aber trotzdem weiter bearbeiten.

Beispiel Mit dem Schlüssel **GEHEIM** können wir die Nachricht mit dem Vigenère-Quadrat verschlüsseln. Dafür verschlüsseln wir die ersten Buchstaben mit dem Schlüsselwort und die folgenden Buchstaben mit dem Klartext von Anfang an.

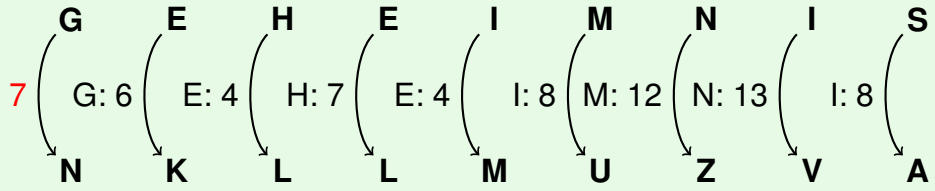
Nachricht:	DAS TREFFEN IST UM ACHT UHR
Schlüsselwort:	GEH EIMDAST REF FE NIST UMA
Geheimtext:	JEZ XZQIFWG ZWY ZQ NKZM OTR

Da wir das Arbeiten mit dem Vigenère-Quadrat jedoch bereits bei der Vigenère-Station gelernt haben, schauen wir uns eine weitere Möglichkeit für die Ver- und Entschlüsselung an. In der Wissenschaft wird häufig mit Zahlen anstatt mit Buchstaben gearbeitet. Dies vereinfacht vor allem die Arbeit mit Informatiksystemen. Außerdem veranschaulicht es besser, wieso die Autokey-Verschlüsselung als Stromverschlüsselung bezeichnet wird. Als Hilfsmittel verwenden wir den Stromverschlüsseler. Dieser zeigt dir die Stellen der einzelnen Buchstaben im Alphabet. Dabei fangen wir immer bei 0 an zu zählen. Deswegen wird der Buchstabe **A** mit der Stelle **0** gleichgesetzt.

Strom-Chiffre

Substitution (polyalphabetisch)

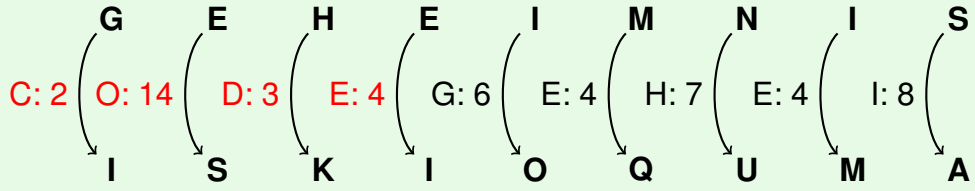
Beispiel Als Startschlüssel ist die Zahl **7** gewählt und unsere Nachricht lautet **GEHEIMNIS**. Nun stellen wir die Nachricht in den Stromverschlüsseler ein, indem wir die Buchstabenbänder so drehen, dass die Buchstaben in den ausgeschnittenen Fenstern unserer Nachricht entsprechen. Wir fangen von vorne an, die Buchstabenbänder jeweils um den passenden Schlüssel weiter zu drehen. Wir schieben also den ersten Buchstaben **G** 7 Stellen weiter und erhalten ein **N**. Dann schieben wir den zweiten Buchstaben **E** um die Stelle vom ersten Klartext weiter, also 6 Stellen, da G an der sechsten Stelle im Alphabet liegt, und landen bei **K**. Nun nehmen wir uns den dritten Buchstaben und schieben ihn um die Stelle vom zweiten Klarbuchstaben weiter. Dies machen wir so lange, bis wir alle Buchstaben verschlüsselt haben.



Unser Geheimtext lautet somit **NKLLMUZVA**.

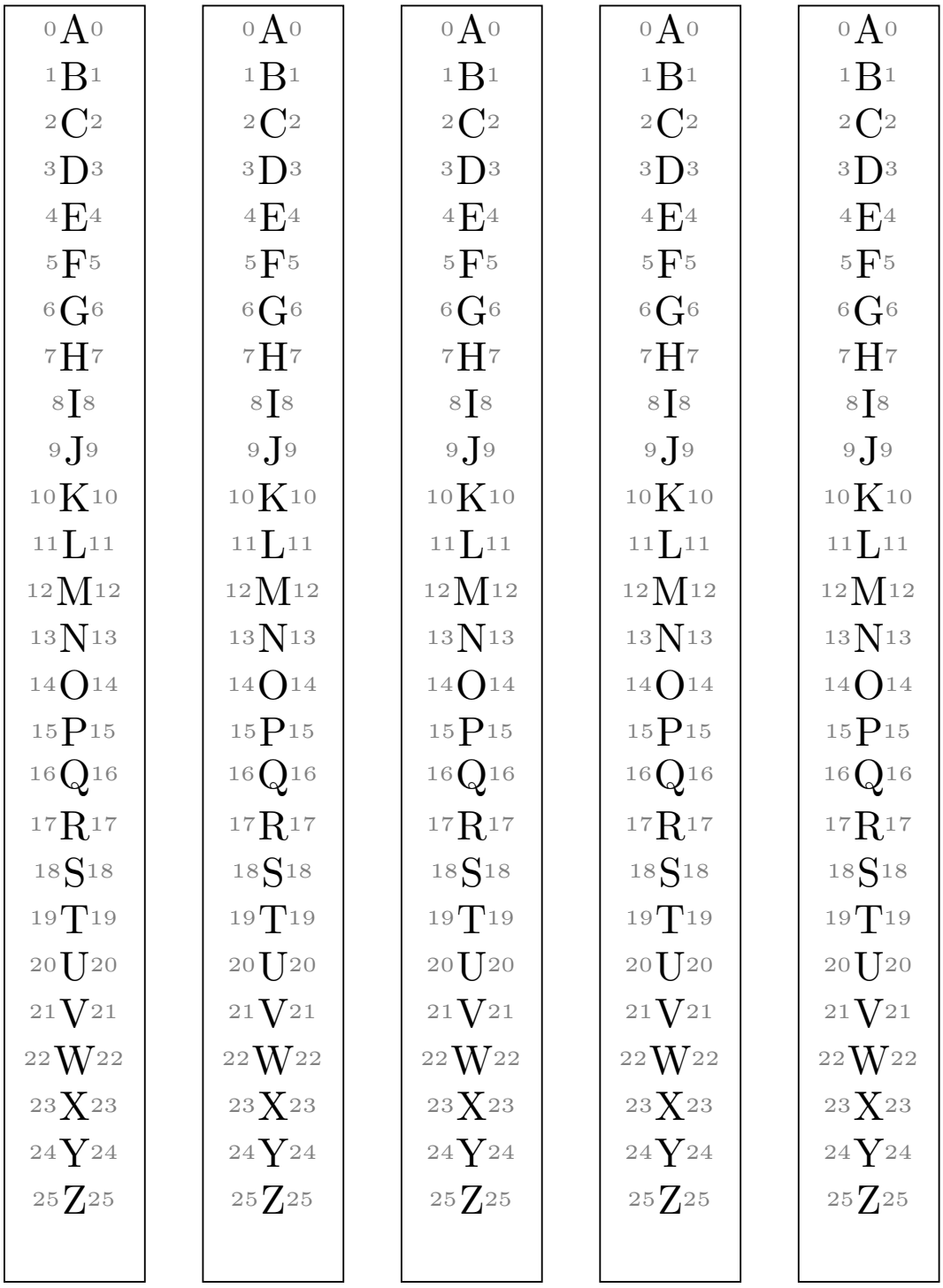
Die »normale« Autokey-Verschlüsselung ist ziemlich leicht zu »knacken«. Etwas schwieriger wird es, wenn das Verfahren mit einem Startschlüssel aus mehren Zahlen kombiniert wird. Um sich den Startschlüssel einfacher merken zu können, kann man auch ein Schlüsselwort wählen. Die Buchstaben des Schlüsselwortes werden wieder in Zahlen umgewandelt.

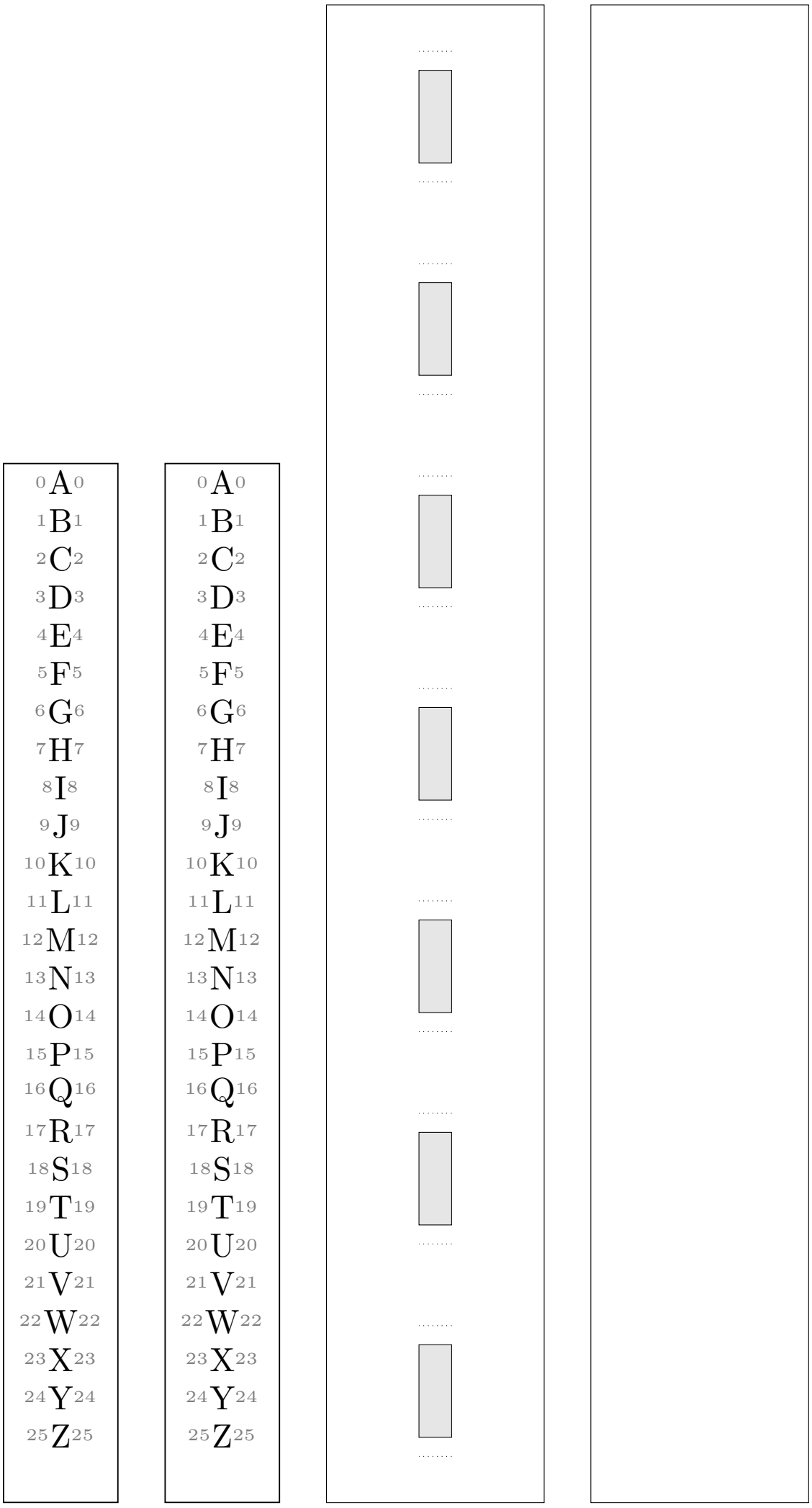
Beispiel Unser Startschlüssel ist jetzt **CODE**, was den Zahlen **2 14 3 4** entspricht, und unsere Nachricht lautet wieder **GEHEIMNIS**. Dann stellen wir die Nachricht in den Stromverschlüsseler ein und verschlüsseln zuerst die ersten vier Buchstaben mit unserem Schlüsselwort und die folgenden wie eben mit den Klartextbuchstaben der Nachricht von Anfang an.



Unser Geheimtext lautet also **ISKIOQUMA**.

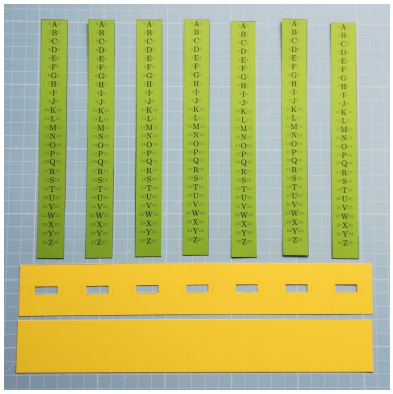
Version vom 2019-08-06


0A0
1B1
2C2
3D3
4E4
5F5
6G6
7H7
8I8
9J9
10K10
11L11
12M12
13N13
14O14
15P15
16Q16
17R17
18S18
19T19
20U20
21V21
22W22
23X23
24Y24
25Z25

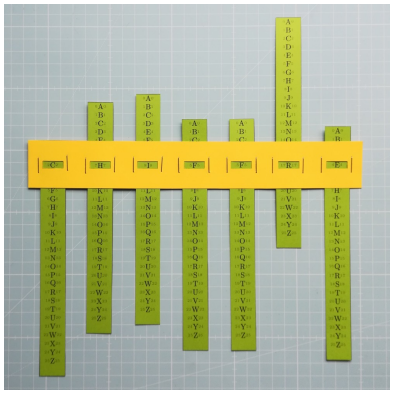

0A0
1B1
2C2
3D3
4E4
5F5
6G6
7H7
8I8
9J9
10K10
11L11
12M12
13N13
14O14
15P15
16Q16
17R17
18S18
19T19
20U20
21V21
22W22
23X23
24Y24
25Z25
0A0
1B1
2C2
3D3
4E4
5F5
6G6
7H7
8I8
9J9
10K10
11L11
12M12
13N13
14O14
15P15
16Q16
17R17
18S18
19T19
20U20
21V21
22W22
23X23
24Y24
25Z25

Bastelanleitung

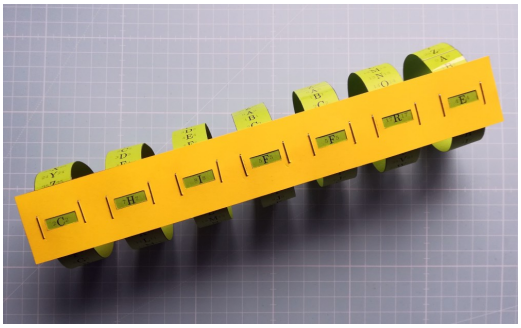
Du benötigst zusätzlich zum ausgedruckten Material einen Tacker und Klebeband.



- Schneide die Buchstabenbänder aus. Bei Papier sollte der schwarze Rand noch zu sehen sein, bei Pappe nicht mehr. Dann passen die Bänder gut in die dafür vorgesehenen Plätze.
- Schneide die beiden Rechtecke aus und trenne die Fenster (die dunklen Felder) heraus.
- Lege die beiden Rechtecke übereinander und tackere sie an den gepunkteten Linien zusammen.



- Schiebe die Buchstabenbänder zwischen die Tackernadeln und prüfe, ob man die Bänder gut durchziehen kann. Schneide sie, wenn benötigt, etwas dünner aus.
  Der Stromverschlüsseler kann bereits jetzt verwendet werden, wenn er platzsparender aufbewahrt werden muss, da die Verschiebung trotzdem durchgeführt werden kann.



- Klebe die Bänder mit Klebeband an den Enden so zusammen, dass **A** direkt **Z** folgt. Nutze die freie Fläche dabei als Klebefläche. Prüfe wieder, ob man die Bänder auch bei den Klebeflächen gut durchziehen kann.

Version vom 2019-09-21

Aufgabe 1 Verschlüssele **FOLGE DEM PFEIL** mit dem Startschlüssel **16**.
Stelle dazu zuerst die ersten sieben Buchstaben im Stromverschlüsseler ein, sodass du sie in den Fenstern sehen kannst. Verschlüssele den ersten Buchstaben mit dem Startschlüssel **16** und die darauf folgenden mit dem jeweiligen vorherigen Klartextbuchstaben.

Aufgabe 2 Beschreibe, wie du eine empfangene Nachricht mit bekanntem Startschlüssel entschlüsseln kannst.

Aufgabe 3 Entschlüssele die Nachricht **JHVJUJHTSHALBUEUJYRNX** mit dem Startschlüssel **6**.

Aufgabe 4 Warum ist dieses Verschlüsselungsverfahren leicht zu »knacken«?

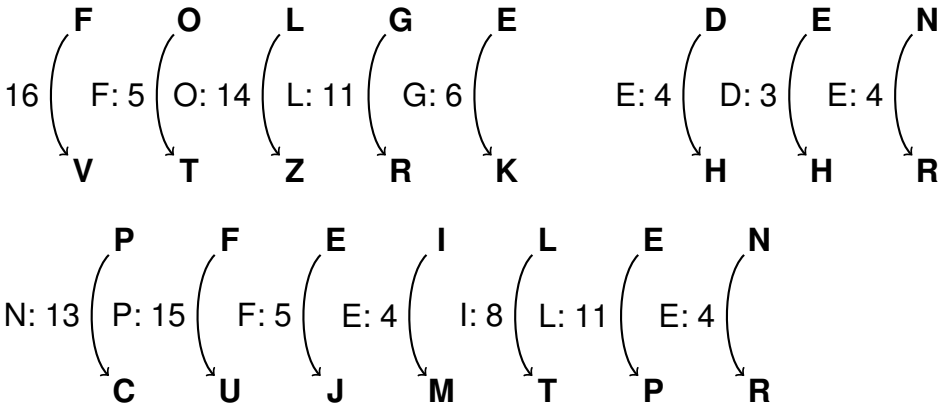
Aufgabe 5 Wählt einen Startschlüssel aus mehreren Zahlen und schreibt euch gegenseitig eine Nachricht.

Aufgabe 6 Was passiert beim Ver- und was beim Entschlüsseln, wenn du einen Buchstaben um ein Stelle zu weit schiebst?

Buchstabe	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
Stelle	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

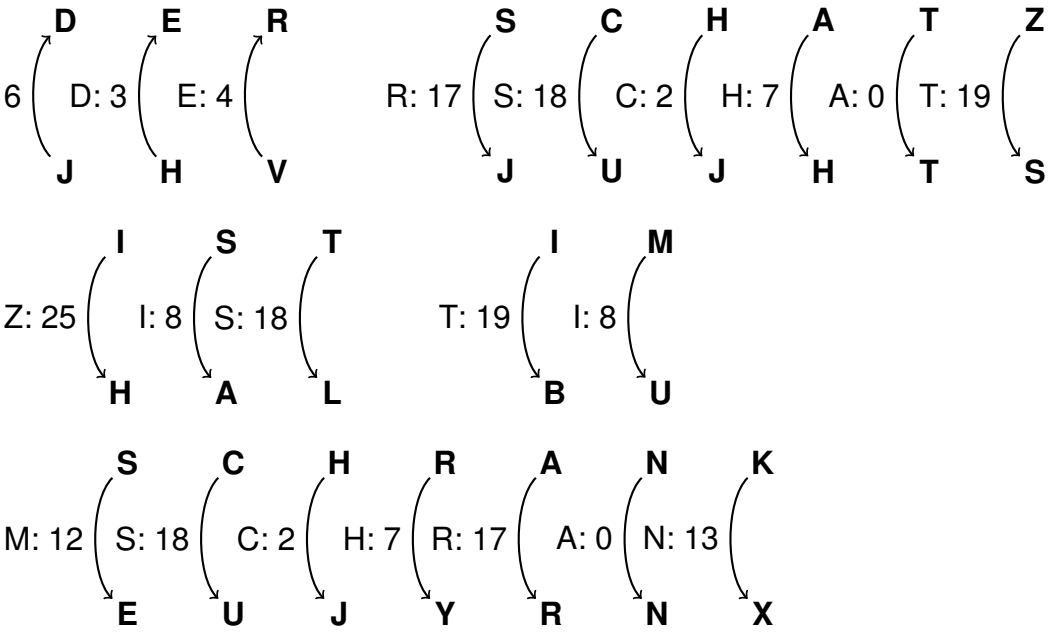
Version vom 2019-08-06

Lösung 1 Die Geheimnachricht lautet **VTZRK HHR CUJMTPR**. Die Verschlüsselung sieht so aus:



Lösung 2 Das Verfahren ist umgekehrt zum Verschlüsselungsvorgang. Man fängt ebenfalls vorne mit dem Startschlüssel an und schiebt die Buchstaben einzeln mit dem passenden Schlüssel zurück. Dabei verwendet man jeweils den entschlüsselten Klarbuchstaben als nächsten Schlüssel. Die Stromverschlüsselungshilfe zeigt dir direkt den nächsten Schlüssel neben dem Buchstaben an.

Lösung 3 Der Klartext lautet **DER SCHATZ IST IM SCHRANK**. Die Entschlüsselung sieht so aus:



Version vom 2019-08-06

Lösung 4 Das Verfahren ist leicht zu »knacken«, da man höchstens 26 Startschlüssel durchprobieren muss, um die Lösung zu erhalten.

Lösung 5 Zu dieser Aufgabe gibt es keine allgemeine Lösung.

Lösung 6 Beim Verschlüsseln merkt man nicht, wenn man einen Buchstaben zu weit verschoben hat, da nur der dazugehörige Buchstabe des Geheimtextes fehlerhaft wird. Allerdings führt dieser Fehler bei der Entschlüsselung dazu, dass der komplette darauf folgende Klartext falsch entschlüsselt wird. Dies liegt daran, dass der Schlüsselstrom an einer Stelle einen zu hohen Schlüssel aufweist und sich das auf alle weiteren Schlüssel auswirkt.

Buchstabenhäufigkeit

Kryptoanalyse

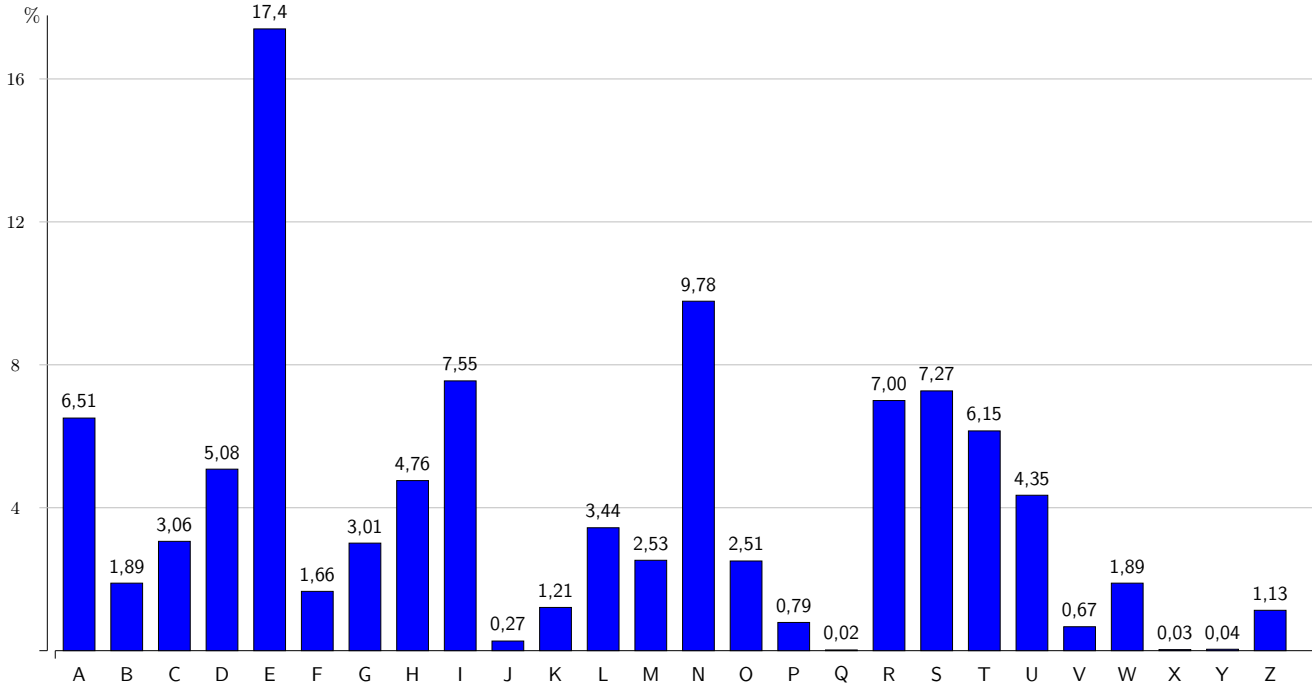
Bei der **Kryptoanalyse** wird versucht, durch Eigenschaften des Geheimtextes den Schlüssel oder den Klartext herauszufinden.
Um einen Geheimtext, der durch eine monoalphabetische Substitution entstanden ist, ohne bekannten Schlüssel zu entschlüsseln, verwendet man die **Häufigkeitsanalyse**.

Verschiedene Buchstaben werden in der deutschen Sprache unterschiedlich häufig verwendet. Dies kann bei einer Substitution dazu führen, dass einige Buchstaben auffällig häufig vorkommen. Das beste Beispiel dafür ist das **E**, da statistisch gesehen jeder sechste Buchstabe in einem deutschen Text ein **E** ist, muss auch in einem verschlüsselten Text ein Buchstabe besonders häufig vorkommen, der höchstwahrscheinlich dem **E** entspricht. Die Häufigkeiten der Buchstaben sind in der folgenden Tabelle und in der Grafik dargestellt. Dabei werden Umlaute ausgeschrieben (z.B. AE statt Ä).

A	B	C	D	E	F	G	H	I
6,51 %	1,89 %	3,06 %	5,08 %	17,4 %	1,66 %	3,01 %	4,76 %	7,55 %

J	K	L	M	N	O	P	Q	R
0,27 %	1,21 %	3,44 %	2,53 %	9,78 %	2,51 %	0,79 %	0,02 %	7,00 %

S	T	U	V	W	X	Y	Z
7,27 %	6,15 %	4,35 %	0,67 %	1,89 %	0,03 %	0,04 %	1,13 %



Buchstabenhäufigkeit

Kryptoanalyse

Neben den Wahrscheinlichkeiten der einzelnen Buchstaben werden noch andere statistische Daten bei der Kryptoanalyse verwendet. In deutschen Texten kommen einige Buchstabenkombinationen häufiger vor. Die Buchstabenkombination zweier aufeinander folgender Buchstaben nennt man *Bigramm*. Insgesamt gibt es 676 ($=26^2$) verschiedene Bigramme. Die zehn häufigsten Bigramme der deutschen Sprache sind in der folgenden Tabelle aufgelistet. Dabei fällt auf, dass die beiden eher seltenen Buchstaben **C** und **H** gemeinsam relativ häufig auftreten.

ER	EN	CH	DE	EI	ND	TE	IN	IE	GE
4,09 %	4,00 %	2,42 %	2,27 %	1,93 %	1,87 %	1,85 %	1,68 %	1,63 %	1,47 %

Bei der Analyse von Geheimtexten fallen Bigramme, die aus Doppelbuchstaben bestehen, besonders auf. Die zehn häufigsten Doppelbuchstaben sind:

SS	NN	LL	EE	MM	TT	RR	DD	FF	AA
0,76 %	0,43 %	0,42 %	0,23 %	0,23 %	0,23 %	0,15 %	0,13 %	0,12 %	0,08 %

Im Deutschen werden auch sehr viele kurze Wörter benutzt. Dies hilft bei der Entschlüsselung ebenfalls weiter. Die zehn häufigsten Wörter sind mit absteigender Häufigkeit:

die der und den am in zu ist dass es

Version vom 2019-08-06

BERGISCHE UNIVERSITÄT WUPPERTAL

Geheimtext

```
W                                        k
Dbqq zs zcbabq Kbhk bqkanrwsbaabwq xiqqkbak, ubrbllanrak zs zcb
K                    g g        w         k     m
Xlfokimqmwfab lcnrkcv vsk. Qsq dclz zcnr xbcqb yiqimwormubkcanrb
               g m               k
Jblanrwsbaabwsqv ybrl mstrmwkbq xibqqbq.
        k                                          gk
Zbl Klcnx zmubc cak, qcnrk qsl mst zcb Rmbstcvxbckbq zbl
           z                              W
Usnrakmubq gs mnrkbq, aiqzblq msnr zma Dcaabq sbubl zcb Aolmnrb,
            g           K       g                          z     z
zcb Bltmrlsqvbq msa zbl Xlfokiwivcb sqz zbcqb Cqksckciq gs qskgbq.
   k         z m            g  mm      k  z  W          w
Ai xmqqak zs gsy Ubcaocbw Ucvlmyyb sqz xslgb Diblkbl jbldbqzbq,
 m                 z   g
sy Usnrakmubq tbakgswbvbq. Zbcqb Cqksckciq rcwtk zcl Usnrakmubq,
W            g  z      z  z              m    G    m
Diblkbl izbl vmqgb Ambkgb gs bllmkbq. Eb ybrl Vbrbcykbhkb zs
        g k   k                          k mm             Z
ublbcka vbxqmnxk rmak, zbaki anrqbwwbl xiyyak zs mq zma Gcbw.
```

Geheimtext	A	B	C	D	E	F	G	H	I	J	K	L	M
Anzahl	33	83	35	6	1	3	10	2	16	2	39	32	27
Klartext				W			Z						

Geheimtext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Anzahl	16	5	0	49	24	33	6	13	11	14	12	10	27
Klartext									G		K	M	

Version vom 2019-08-06

Aufgabe 1 Du findest an der Station einen Geheimtext. Kannst du ihn durch die Kryptoanalyse lesen?
Um dir die Arbeit zu vereinfachen, sind die Buchstaben bereits gezählt und fünf Einträge der Ersetzungstabelle vorgegeben. Außerdem sind Großbuchstaben und Leerzeichen beibehalten.
Markiere Doppelbuchstaben und versuche Auffälligkeiten zu finden.
Vergleiche die Häufigkeiten mit den realen Häufigkeiten der deutschen Sprache. Bei welchen Buchstaben kannst du dir sicher sein, wie sie verschlüsselt wurden? Nutze dafür die unten stehende Tabelle, um die entschlüsselten Buchstaben einzutragen.

Aufgabe 2 Schreibe nun deine bereits entschlüsselten Buchstaben über den Text und versuche ihn mithilfe der Angaben auf dem Stationsblatt und deinem Wissen über die deutsche Sprache zu entschlüsseln.

Klartext	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
Geheimtext							V				X		Y										D			G

Version vom 2019-08-06

Aufgabe 1 In der folgenden Tabelle sind die Häufigkeiten angegeben.

A	B	C	D	E	F	G	H	I
6,48 %	16,3 %	6,88 %	1,18 %	0,20 %	0,59 %	1,96 %	0,39 %	3,14 %

J	K	L	M	N	O	P	Q	R
0,39 %	7,66 %	6,29 %	5,30 %	3,14 %	0,98 %	0,00 %	9,62 %	4,72 %

S	T	U	V	W	X	Y	Z
6,48 %	1,18 %	2,55 %	2,16 %	2,75 %	2,36 %	1,96 %	5,30 %

Der Buchstabe mit dem höchsten Anteil kann leicht zugeordnet werden. So entspricht das **B** dem Klartext **E**. Besonders häufig treten auch, mit absteigender Häufigkeit, **Q**, **K**, **C**, **A**, **S** und **L** auf. Sie können einem der Buchstaben **N**, **I**, **S**, **R**, **T** oder **A** zugeordnet werden. Es lässt sich erschließen, dass **Q** dem Klarbuchstaben **N** entspricht, weil die Häufigkeit einen großen Abstand zu den anderen Häufigkeiten besitzt. Wie die Zuordnung für die anderen Buchstaben genau aussieht, wissen wir jedoch noch nicht.

Im Text kommen fünf verschiedene Doppelbuchstaben vor. Dies sind **QQ**, **AA**, **LL**, **YY** und **WW**. Da **Q** bereits **N** zugeordnet wurde, muss es sich bei **AA** um **S** handeln, weil **SS** eigentlich am häufigsten vorkommen sollte.

Wir wissen also, dass es sich bei **A** um **S** handelt und können uns deswegen anschauen, welche Bigramme dem **A** häufig folgen. Dabei muss es sich dann um das **SCH** handeln. Dabei können wir Bigramme auslassen, bei denen ein Buchstabe bereits entziffert ist. **ANR** taucht im gesamten Text fünfmal auf. Außerdem treten **NR** insgesamt vierzehnmal gemeinsam im Text auf. Die zweithäufigste Kombination **AKM** finden wir dreimal im Text, allerdings **KM** nur zusammen mit **A**. Dabei kann es sich also nicht um **SCH** handeln. Also muss **ANR** die Klarbuchstaben **SCH** verschlüsseln.

Von den häufigsten Buchstaben bleiben noch **K**, **C**, **S** und **L** bzw. **I**, **R**, **T** oder **A**. Dies können wir uns für die weitere Kryptoanalyse merken.

Klartext	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
Geheimtext			N		B		V	R			X		Y	Q					A				D			G

Aufgabe 2

Durch das sorgfältige Durchgehen des Textes fallen z.B. diese Dinge auf:

- Insgesamt viele kurze Wörter beginnen mit **Z** und stehen häufig vor großgeschriebenen Wörtern. Also kann es sich dabei nur um Artikel handeln, die eigentlich mit **D** beginnen.
- In Zeile sieben steht ein Wort aus zwei Buchstaben **Ai**. Da wir bereits wissen, was **A** verschlüsselt, kann es sich dabei nur um das Wort **So** handeln. Die Zuordnung von **I** zu **O** passt auch, da **IB** häufiger vorkommt, dabei handelt es sich um **OE**, also den Umlaut **Ö**, der in der Kryptologie häufig nicht vorkommt.
- In der ersten Zeile steht **zcbabq**, was aufgrund der bisherigen Ergebnisse zu **d_esen** entschlüsselt wird, also muss es sich dabei um **diesen** handeln. Dies passt auch gut in den häufig vorkommenden Artikel **zcb**, also **die**.
- Im Text findet sich zweimal das Wort **sqz**, das bereits als **_nd** entschlüsselt werden kann. Deswegen muss **S** zum Klarbuchstaben **U** gehören. Dadurch wird aus **zs** auch **du** und aus **Qsq Nun**.

Natürlich können auf diese Weise auch noch viel mehr Buchstaben aufgedeckt werden. Dadurch sieht die Ersetzungstabelle insgesamt so aus:

Klartext	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
Geheimtext	M	U	N	Z	B	T	V	R	C	?	X	W	Y	Q	P	O	?	L	A	K	B	J	D	H	F	G

Daraus ergibt sich der Text:

```
Wenn du diesen Text entschluesseln konntest, beherrschst du die
Kryptoanalyse richtig gut. Nun wird dich keine monoalphabetische
Verschluesselung mehr aufhalten koennen.
Der Trick dabei ist, nicht nur auf die Haeufigkeiten der
Buchstaben zu achten, sondern auch das Wissen ueber die Sprache,
die Erfahrungen aus der Kryptologie und deine Intuition zu nutzen.
So kannst du zum Beispiel Bigramme und kurze Woerter verwenden, um
Buchstaben festzulegen. Deine Intuition hilft dir Buchstaben,
Woerter oder ganze Saetze zu erraten. Je mehr Geheimtexte du
bereits geknackt hast, desto schneller kommst du an das Ziel.
```

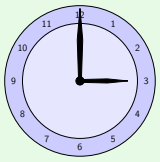
Modulo-Rechnung

Schlüsselaustausch

Um einen Klartext zu verschlüsseln und auch anschließend zu entschlüsseln, brauchen Sender und Empfänger denselben Schlüssel. Dieser ist meist eine Zahl. Sender und Empfänger müssen den Schlüssel **geheim** austauschen können, das heißt, ohne dass ein Dritter ihn erfährt.

Der geheime Schlüsselaustausch erfordert oft einige Rechenoperationen beim Sender wie auch beim Empfänger. Modulo ist eine Rechenoperation (wie z. B. Addition oder Multiplikation). Sie wird für zahlreiche Verschlüsselungsverfahren und Schlüsselaustausch-Verfahren benötigt. Auch der Diffie-Hellman-Algorithmus arbeitet mit der Modulo-Operation.
Die Modulo-Operation ist aber leicht zu verstehen.
Mit Modulo, **mod**, wird einfach der Rest der ganzzahligen Division bezeichnet.

Beispiel



Jeder von uns benutzt fast täglich die Modulo-Rechnung. Die kommt nämlich bei der Berechnung der Uhrzeit vor. Wir sagen zu der Uhrzeit 15:00 Uhr meist 3 Uhr (nachmittags). Das ist die Modulo-Rechnung mit der Zahl 12: $15 \; mod \; 12 \; = \; 3$, da $15 \; : \; 12 \; = \; 1, \quad \mathbf{3}$ bleibt übrig.

Natürlich rechnet man nicht immer $mod \; 12$. 12 kann durch jede ganze Zahl ersetzt werden. Bei den meisten Verschlüsselungsverfahren kommen keine negativen Zahlen vor, das macht es etwas einfacher.

Beispiel

Rechnungen

$18 \; mod \; 5 \; = \; 3$, da $18 \; : \; 5 \; = \; 3$ **(Rest 3)**

$10 \; mod \; 4 \; = \; 2$, da $10 \; : \; 4 \; = \; 2$ **(Rest 2)**

$14 \; mod \; 7 \; = \; 0$, da $14 \; : \; 7 \; = \; 2$ **(Rest 0)**

Aufgabe 1 **Berechne wie in den Beispielen auf dem Stationsblatt:**

25	mod	7	=		, da	25	:	7	=		**, Rest**	
90	mod	11	=		, da	90	:	11	=		**, Rest**	
23	mod	8	=		, da	23	:	8	=		**, Rest**	
10	mod	19	=		, da	10	:	19	=		**, Rest**	
106	mod	21	=		, da	106	:	21	=		**, Rest**	
42	mod	4	=		, da	42	:	4	=		**, Rest**	
8	mod	3	=		, da	8	:	3	=		**, Rest**	
33	mod	15	=		, da		:		=		**, Rest**	
107	mod	25	=		, da		:		=		**, Rest**	
2180	mod	54	=		, da		:		=		**, Rest**	
1011	mod	12	=		, da		:		=		**, Rest**	
1001	mod	13	=		, da		:		=		**, Rest**	
45	mod	14	=		, da		:		=		**, Rest**	
785	mod	43	=		, da		:		=		**, Rest**	

Version vom 2019-06-11

Aufgabe 1 **Berechne wie in den Beispielen auf dem Stationsblatt:**

25	*mod*	7	=	4	, da	25	:	7	=	3	**, Rest**	4
90	*mod*	11	=	2	, da	90	:	11	=	8	**, Rest**	2
23	*mod*	8	=	7	, da	23	:	8	=	2	**, Rest**	7
10	*mod*	19	=	10	, da	10	:	19	=	0	**, Rest**	10
106	*mod*	21	=	1	, da	106	:	21	=	5	**, Rest**	1
42	*mod*	4	=	2	, da	42	:	4	=	10	**, Rest**	2
8	*mod*	3	=	2	, da	8	:	3	=	2	**, Rest**	2
33	*mod*	15	=	3	, da	33	:	15	=	2	**, Rest**	3
107	*mod*	25	=	7	, da	107	:	25	=	4	**, Rest**	7
2180	*mod*	54	=	20	, da	2180	:	54	=	40	**, Rest**	20
1011	*mod*	12	=	3	, da	1011	:	12	=	84	**, Rest**	3
1001	*mod*	13	=	0	, da	1001	:	13	=	77	**, Rest**	0
45	*mod*	14	=	3	, da	45	:	14	=	3	**, Rest**	3
785	*mod*	43	=	11	, da	785	:	43	=	18	**, Rest**	11

Diffie-Hellman-Algorithmus

Schlüsselaustausch

Um einen Klartext zu verschlüsseln und auch anschließend zu entschlüsseln, brauchen Sender und Empfänger denselben Schlüssel. Dieser ist meist eine Zahl. Sender und Empfänger müssen den Schlüssel **geheim** austauschen können, das heißt, ohne dass ein Dritter ihn erfährt.

Lange galt es als unmöglich, im »öffentlichen Raum«, also für jeden mithörbar, einen geheimen Schlüssel auszutauschen. Aber 1976 wurde von Martin Hellman, Whitfield Diffie und Ralph Merkle der **Diffie-Hellman-Algorithmus** entwickelt. Er ermöglicht die Vereinbarung eines gemeinsamen geheimen Schlüssels über eine unsichere Verbindung.

Hinweis: Der Diffie-Hellman-Algorithmus arbeitet mit der Modulo-Funktion. Falls du dich nicht sicher im Umgang damit fühlst, bearbeite bitte zuerst die entsprechende Station.

Mit dem Diffie-Hellman-Algorithmus können also zwei Beteiligte - nennen wir sie Alice und Bob - im öffentlichen Raum einen geheimen Schlüssel vereinbaren, ohne dass eine dritte Person, die alles mithört, - nennen wir sie Eve - den Schlüssel erfährt.

Der Algorithmus

Alice und Bob vereinbaren zu Beginn öffentlich eine Primzahl **p** und eine natürliche Zahl **g**. Dabei muss **g** kleiner sein als **p**. Zum Berechnen von **A** bzw. **B** wählte Alice die Zahl **a**, die nur sie kennt, und Bob wählt die Zahl **b**, die nur er kennt. **A** und **B** werden öffentlich ausgetauscht. (Berechnungen siehe unten)
Eve kennt also **p**, **g**, **A** und **B**, aber nicht **a** und **b**. Den geheimen Schlüssel **K** können Alice und Bob berechnen, Eve nicht. (Ein Beispiel gibt es auf der nächsten Seite.)

privater Raum:	öffentlicher Raum:	privater Raum:
Alice 	Eve 	Bob 
Wähle a, mit a < p Berechne $A = g^a \mod p$ Berechne $K = B^a \mod p$	p und g A → ← B	Wähle b, mit b < p Berechne $B = g^b \mod p$ Berechne $K = A^b \mod p$

Diffie-Hellman-Algorithmus

Schlüsselaustausch

Beispiel

Alice und Bob vereinbaren öffentlich: $p = 13$ und $g = 4$:

privater Raum:	öffentlicher Raum:	privater Raum:
Alice 	 Eve	Bob 
	$p = 13, g = 4$	
Wähle a, mit a < p		Wähle b, mit b < p
$a = 3$		$b = 5$
Berechne $A = g^a \mod p$		Berechne $B = g^b \mod p$
$A = g^a \mod p$ $A = 4^3 \mod 13$ $= 64 \mod 13$ $= 12$		$B = g^b \mod p$ $B = 4^5 \mod 13$ $= 1024 \mod 13$ $= 10$
	$A = 12 \longrightarrow$	
	$\longleftarrow B = 10$	
Berechne $K = B^a \mod p$		Berechne $K = A^b \mod p$
$K = 10^3 \mod 13$ $= 1000 \mod 13$ $= 12$		$K = 12^5 \mod 13$ $= 248832 \mod 13$ $= 12$

Der von Alice und Bob berechnete geheime Schlüssel in diesem Beispiel ist 12. Um den Schlüssel zu finden, müsste Eve nur alle Zahlen ausprobieren, die kleiner als p, hier also 13, sind. Das wäre einfach.
Normalerweise sind die Zahlen aber so groß, dass es auch mit den schnellsten Computern fast unmöglich ist, den Schlüssel durch Ausprobieren zu finden.

Version vom 2019-08-09

BERGISCHE UNIVERSITÄT WUPPERTAL

Aufgabe 1

Bildet eine Dreiergruppe und spielt den Diffie-Hellman-Algorithmus durch. Eine/r von euch ist Alice, eine/r Bob und der oder die Dritte ist Eve.
Alice und Bob tauschen den Schlüssel aus und Eve versucht den Schlüssel (K) herauszufinden, um die geheime Nachricht lesen zu können.
Führt den Algorithmus mit $p = 11$ und $g = 3$ ein- bis dreimal mit verschiedenen Rollen aus. Die unten stehende Tabelle ist euch beim Rechnen behilflich.
Notiert euer Ergebnis. Hat Eve den Schlüssel herausgefunden?

Tabelle mit vorberechneten Werten für x^y:

x^y	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	64	128	256	512	1024
3	3	9	27	81	243	729	2187	6561	19683	59049
4	4	16	64	256	1024	4096	16384	65536	262144	1048576
5	5	25	125	625	3125	15625	78125	390625	1953125	9765625
6	6	36	216	1296	7776	46656	279936	1679616	10077696	60466176
7	7	49	343	2401	16807	117649	823543	5764801	40353607	282475249
8	8	64	512	4096	32768	262144	2097152	16777216	134217728	1073741824
9	9	81	729	6561	59049	531441	4782969	43046721	387420489	3486784401
10	10	100	1000	10000	100000	1000000	10000000	100000000	1000000000	10000000000

Hinweis: Bei dieser Tabelle kann x die Werte von g, A oder B und y die Werte von a oder b annehmen.

Version vom 2019-06-11