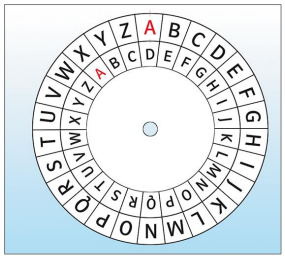
## Die Caesar-Verschlüsselung

**1** Conrad, Elif und die Caesar-Scheibe

Die Caesar-Verschlüsselung ist eine der frühesten und einfachsten Buchstabensubstitutionen. Der römische Staatsmann und Feldherr Gaius Julius Caesar (100 – 44 v. Chr.) benutzte zwei Scheiben mit den 26 Buchstaben des Alphabets (→ **Abb. 2**), um Nachrichten an seine Soldaten während der Gallienkriege zu verschlüsseln. Caesar hat große Angst gehabt, dass seine Nachrichten in falsche Hände geraten könnten. Boten und Spione, die die Nachrichten überbrachten, waren nicht in die Verschlüsselung eingeweiht. So konnten sie die Nachrichten auch nicht ausplaudern.



**2** Caesar-Scheibe

| **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** | 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 |

**3** Caesar-Verschiebung (um drei Stellen)

| **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 | 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 |

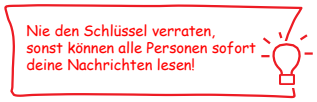
**4** ROT 13

### Auf Caesars Spuren

Wie hat Caesar seine Nachrichten verschlüsselt? Er hat einfach jeden Buchstaben in der Nachricht, durch den Buchstaben, der drei Stellen weiter im Alphabet liegt, ersetzt. Dadurch wird A zu D, B zu E usw. Der Schlüssel ist die Anzahl der Stellen, um die das Alphabet verschoben wurde. Entsprechend wurden die Scheiben eingestellt. Die äußere Scheibe enthielt die Buchstaben des Klartextes, die innere Scheibe die Buchstaben des Geheimtextes (→ **Abb. 2**).

Ein berühmtes Zitat Caesars lautet: *Alea iacta est.* Frei übersetzt bedeutet das: *Der Würfel ist gefallen.* Verschlüsselt mit der Caesar-Verschlüsselung erhält man: *Dohd ldfwd hvw.*

Nur drei oder darf es etwas mehr sein? Statt genau um drei Stellen zu verschieben, kannst du für deine Verschlüsselung auch eine andere Verschiebung wählen, z. B. um 5 oder 10 Stellen. **Eine** Verschiebung ergibt keinen Sinn. Weißt du auch welche?
Ein Spezialfall stellt die Verschiebung um 13 Stellen dar, die sogenannte ROT 13 (→ **Abb. 4**). ROT steht hier nicht für die Farbe rot, sondern ist die Abkürzung für Rotation (Drehung). Die Besonderheit dieser Verschlüsselung ist, dass die Buchstaben Pärchen bilden. A wird mit N verschlüsselt, N mit A usw.






### Unzählige Möglichkeiten

Das Schöne an der Caesar-Verschlüsselung ist, dass sie leicht anzuwenden ist. Für den Sender ist es einfach, einen Schlüssel festzulegen, er muss sich nur für eine Verschiebung der Buchstaben entscheiden.
Es gibt 25 verschiedene Möglichkeiten, das Alphabet zu verschieben.

Wenn wir uns nicht nur auf die Verschiebung beschränken, sondern jede beliebige Anordnung der Buchstaben zulassen, gibt es über 400 000 000 000 000 000 000 000 000 (Quadrillionen) Möglichkeiten. Da erscheint es unmöglich, eine verschlüsselte Nachricht zu entschlüsseln, wenn man die Anordnung nicht kennt. Oder doch?

### Projekt

**Ave Caesar!**

Teilt eure Klasse in Gruppen ein.
**Ihr braucht pro Person:** *ausgedruckte Caesar-Scheibe, Schere, Briefklammer*
**Vorarbeit:** Jeder erstellt seine Caesar-Scheibe.

**1 Für Anfänger**
Verschlüssele deinen Namen mit der Caesar-Verschlüsselung. Gebt eure Zettel an eine andere Gruppe zum Entschlüsseln weiter.

**2 Für Fortgeschrittene**
Wählt einen Satz mit max. zehn Wörtern von dieser Doppelseite aus und verschlüsselt ihn mit der Caesar-Verschlüsselung. Gebt den Zettel an eine andere Gruppe zum Entschlüsseln.

**3 Für Profis**
Einigt euch in der Gruppe auf einen Text (max. fünf Sätze). Wählt eine Variante der Caesar-Verschlüsselung und verschlüsselt den Text. Gebt den Text einer anderen Gruppe zum Entschlüsseln.

### Merke

- **Die Caesar-Verschlüsselung ist eine einfache Möglichkeit durch Buchstabenverschiebung Texte zu verschlüsseln.**
- **Caesar hat das Alphabet um drei Stellen verschoben, sodass A mit D, B mit E usw. ersetzt wurde.**
- **Das Alphabet kann aber auch um eine beliebige Anzahl Stellen verschoben werden. Ein Sonderfall ist die ROT 13.**

### Aufgaben

1 Führt gemeinsam das Projekt „Ave Caesar!“ durch.
2 Verschlüssele dieses Sprichwort mit dem Schlüssel *6*:
Lieber den Spatz in der Hand alsdie Taube auf dem Dach.
3 Du hast folgende Nachricht abgefangen:
LXG BPRWTC TXCT LPCSTGJCV.QGXCVT QXIIT GTVTCUTHIT ZATXSJCV BXI.
Dir ist bekannt, dass sie von Caesar persönlich stammt. Was möchte Caesar mitteilen?
4 Vereinbare mit einem Mitschüler, der nicht direkt neben dir sitzt, einen Schlüssel. Schreibt eine geheime Botschaft auf und schickt sie von eurem Platz aus über eure Mitschüler zu eurem Partner. Kannst du die verschlüsselten Nachrichten der anderen Schüler verstehen?
5 Simon meint: „Ich kann meinen Text doppelt verschlüsseln. Dann ist er doppelt sicher!“. Was meinst du, stimmt das? Erläutere deine Überlegung schriftlich.
6 Deine Lehrkraft hat dir eine verschlüsselte E-Mail geschickt. Leider hat sie vergessen, dir den Schlüssel zu geben. Kannst du die Nachricht trotzdem entschlüsseln? Notiere deine Vorgehensweise. Die Nachricht lautet:
KHXWH JLEW HV NHLQHKDXVDXIJDEHQ.



Abbildung 1: Analysematerial zur Thematik *Die Caesar-Verschlüsselung* (Hilbig et al. 2021[1]).

# Aufgabe

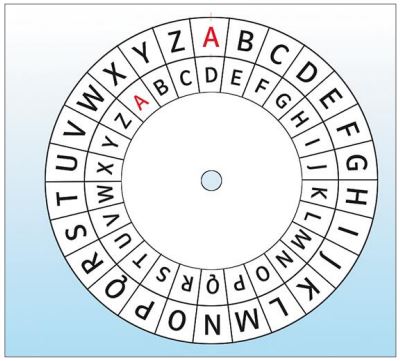
1. Analysieren Sie das vorliegende Material aus Abbildung 1 und identifizieren Sie, welche der zuvor genannten Merkmale/Herausforderungen auf der Wort-, Satz- und Textebene zu finden sind.

[1] André Hilbig et al. (2021): *starkeSeiten Informatik 5/6. Ausgabe Nordrhein-Westfalen Gymnasium: Schülerbuch Klasse 5/6*. Stuttgart: Ernst Klett Verlag, S. 78–79. ISBN: 978-3-12-007544-8.

# Die Caesar-Verschlüsselung

**1** Conrad, Elif und die Caesar-Scheibe

Die Caesar-Verschlüsselung ist eine der frühesten und einfachsten Buchstabensubstitutionen. Der römische Staatsmann und Feldherr Gaius Julius Caesar (100 – 44 v. Chr.) benutzte zwei Scheiben mit den 26 Buchstaben des Alphabets (→ **Abb. 2**), um Nachrichten an seine Soldaten während der Gallienkriege zu verschlüsseln. Caesar hat große Angst gehabt, dass seine Nachrichten in falsche Hände geraten könnten. Boten und Spione, die die Nachrichten überbrachten, waren nicht in die Verschlüsselung eingeweiht. So konnten sie die Nachrichten auch nicht ausplaudern.



**2** Caesar-Scheibe

### Auf Caesars Spuren

Wie hat Caesar seine Nachrichten verschlüsselt? Er hat einfach jeden Buchstaben in der Nachricht, durch den Buchstaben, der drei Stellen weiter im Alphabet liegt, ersetzt. Dadurch wird A zu D, B zu E usw. Der Schlüssel ist die Anzahl der Stellen, um die das Alphabet verschoben wurde. Entsprechend wurden die Scheiben eingestellt. Die äußere Scheibe enthielt die Buchstaben des Klartextes, die innere Scheibe die Buchstaben des Geheimtextes (→ **Abb. 2**).

Ein berühmtes Zitat Caesars lautet: *Alea iacta est.* Frei übersetzt bedeutet das: *Der Würfel ist gefallen.* Verschlüsselt mit der Caesar-Verschlüsselung erhält man: *Dohd ldfwd hvw.*

Nur drei oder darf es etwas mehr sein? Statt genau um drei Stellen zu verschieben, kannst du für deine Verschlüsselung auch eine andere Verschiebung wählen, z. B. um 5 oder 10 Stellen. **Eine** Verschiebung ergibt keinen Sinn. Weißt du auch welche?
Ein Spezialfall stellt die Verschiebung um 13 Stellen dar, die sogenannte ROT 13 (→ **Abb. 4**). ROT steht hier nicht für die Farbe rot, sondern ist die Abkürzung für Rotation (Drehung). Die Besonderheit dieser Verschlüsselung ist, dass die Buchstaben Pärchen bilden. A wird mit N verschlüsselt, N mit A usw.

Nie den Schlüssel verraten, sonst können alle Personen sofort deine Nachrichten lesen!

| **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** | 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 |

**3** Caesar-Verschiebung (um drei Stellen)

| **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 | 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 |

**4** ROT 13



### Unzählige Möglichkeiten

Das Schöne an der Caesar-Verschlüsselung ist, dass sie leicht anzuwenden ist. Für den Sender ist es einfach, einen Schlüssel festzulegen, er muss sich nur für eine Verschiebung der Buchstaben entscheiden.
Es gibt 25 verschiedene Möglichkeiten, das Alphabet zu verschieben.

Wenn wir uns nicht nur auf die Verschiebung beschränken, sondern jede beliebige Anordnung der Buchstaben zulassen, gibt es über 400 000 000 000 000 000 000 000 000 (Quadrillionen) Möglichkeiten. Da erscheint es unmöglich, eine verschlüsselte Nachricht zu entschlüsseln, wenn man die Anordnung nicht kennt. Oder doch?

### Projekt

**Ave Caesar!**

Teilt eure Klasse in Gruppen ein.
**Ihr braucht pro Person:** *ausgedruckte Caesar-Scheibe, Schere, Briefklammer*
**Vorarbeit:** Jeder erstellt seine Caesar-Scheibe.

**1 Für Anfänger**
Verschlüssele deinen Namen mit der Caesar-Verschlüsselung. Gebt eure Zettel an eine andere Gruppe zum Entschlüsseln weiter.

**2 Für Fortgeschrittene**
Wählt einen Satz mit max. zehn Wörtern von dieser Doppelseite aus und verschlüsselt ihn mit der Caesar-Verschlüsselung. Gebt den Zettel an eine andere Gruppe zum Entschlüsseln.

**3 Für Profis**
Einigt euch in der Gruppe auf einen Text (max. fünf Sätze). Wählt eine Variante der Caesar-Verschlüsselung und verschlüsselt den Text. Gebt den Text einer anderen Gruppe zum Entschlüsseln.

### Merke

- **Die Caesar-Verschlüsselung ist eine einfache Möglichkeit durch Buchstabenverschiebung Texte zu verschlüsseln.**
- **Caesar hat das Alphabet um drei Stellen verschoben, sodass A mit D, B mit E usw. ersetzt wurde.**
- **Das Alphabet kann aber auch um eine beliebige Anzahl Stellen verschoben werden. Ein Sonderfall ist die ROT 13.**

### Aufgaben

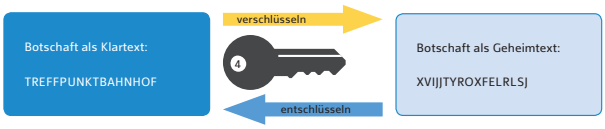
1 Führt gemeinsam das Projekt „Ave Caesar!“ durch.
2 Verschlüssele dieses Sprichwort mit dem Schlüssel *6*:
Lieber den Spatz in der Hand als die Taube auf dem Dach.
3 Du hast folgende Nachricht abgefangen:
LXG BPRWTC TXCT LPCSTGJCV.QGXCVT QXIIT GTVTCUTHIT ZATXSJCV BXI.
Dir ist bekannt, dass sie von Caesar persönlich stammt. Was möchte Caesar mitteilen?
4 Vereinbare mit einem Mitschüler, der nicht direkt neben dir sitzt, einen Schlüssel. Schreibt eine geheime Botschaft auf und schickt sie von eurem Platz aus über eure Mitschüler zu eurem Partner. Kannst du die verschlüsselten Nachrichten der anderen Schüler verstehen?
5 Simon meint: „Ich kann meinen Text doppelt verschlüsseln. Dann ist er doppelt sicher!“. Was meinst du, stimmt das? Erläutere deine Überlegung schriftlich.
6 Deine Lehrkraft hat dir eine verschlüsselte E-Mail geschickt. Leider hat sie vergessen, dir den Schlüssel zu geben. Kannst du die Nachricht trotzdem entschlüsseln? Notiere deine Vorgehensweise. Die Nachricht lautet:
KHXWH JLEW HV NHLQHKDXVDXIJDEHQ.

## 3 Sicher ist sicher: Daten verschlüsseln

Leon erzählt Ina von einem Agentenfilm, den er gestern Abend im Fernsehen anschauen durfte. „Das war spannend! Die Agenten konnten sich untereinander geheime Botschaften schicken, die sonst niemand entschlüsseln konnte!"
„Wenn wir so etwas hätten, könnten wir uns Nachrichten schicken, die nur wir verstehen!"

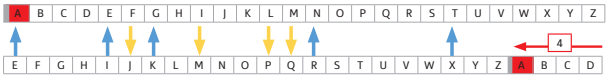
### Die Caesar-Verschlüsselung

Eines der ältesten Verschlüsselungsverfahren nutzte bereits der römische Kaiser Julius Caesar vor über 2000 Jahren. Damit konnte er seinen Soldaten Befehle schicken, die der Feind nicht verstehen konnte, auch wenn ihm die geheimen Botschaften in die Hände gefallen wären.




Das Verschlüsseln von Nachrichten funktioniert so: Jeder Buchstabe des Klartextes wird durch einen anderen Buchstaben ersetzt. Dazu schreibt man zwei Alphabete untereinander. In der oberen Reihe stehen die Buchstaben des Alphabets für den Klartext. In der unteren Reihe das verschobene Alphabet für den Geheimtext. Im Geheimtext sind die Buchstaben um eine bestimmte Zahl von Stellen nach links verschoben. Diese Zahl ist der **Schlüssel**. Den braucht man, um aus dem Klartext in der oberen Zeile einen Geheimtext zu machen und umgekehrt.

**Beispiel:** Verschlüsseln und Entschlüsseln mit dem Schlüssel 4




**Verschlüsseln:** Folgst du den gelben Pfeilen, wird aus dem Klartext „**FILM**" der Geheimtext „**JMPQ**".
**Entschlüsseln:** Folgst Du den blauen Pfeilen, wird aus dem Geheimtext „**EKIRX**" der Klartext „**AGENT**".

**Info: Knacken von Verschlüsselungen**
Versucht man eine Nachricht zu entschlüsseln, ohne den Schlüssel zu kennen, spricht man vom Knacken einer Verschlüsselung. Je besser eine Verschlüsselung ist, desto länger dauert es, sie zu knacken. Moderne Verfahren lassen sich auch mit den schnellsten Computern nicht knacken.

1 a) Verschlüssele deinen Vornamen.
b) Tauscht den verschlüsselten Namen in einer Kleingruppe aus und überprüft eure Ergebnisse gegenseitig.



### Die Caesar-Scheibe als Werkzeug

Um das Ver- und Entschlüsseln mit unterschiedlichen Schlüsseln zu vereinfachen, kann man sich eine sogenannte **Caesar-Scheibe** selbst basteln. Dazu müssen die beiden Alphabete auf zwei unterschiedlich große Scheiben geschrieben werden. Die beiden Scheiben fixiert man in der Mitte. Am Anfang stehen immer die gleichen Buchstaben untereinander. Nun kann der innere Kreis gedreht werden, sodass immer andere Buchstaben untereinander stehen.

Hier wurde die innere Scheibe um **drei Stellen** gegen den Uhrzeigersinn gedreht. Der Buchstabe A wird durch den Buchstaben D verschlüsselt. Durch die Drehung der inneren Scheibe lassen sich sehr einfach unterschiedliche Schlüssel einstellen.

**Eure Klasse knackt den Code!** Sprecht euch ab und entschlüsselt den folgenden Geheimtext:
NRJZJKUVILEKVIJTYZVUQNZJTYVETFUZVILEXLEUMVIJTYCLVJJVCLEX
**Lösungshinweis:**
Codieren ist wie das Übersetzen von Sprache A in Sprache B. Alle Personen, die die Sprache B sprechen, verstehen die Übersetzung. Beim Verschlüsseln wird ein Text ebenfalls von Sprache A in Sprache B übersetzt. Allerdings sollen nur Personen, die die Sprache B sprechen und einen Schlüssel haben, die Übersetzung verstehen.

1 Entschlüssele das Wort JXWJHPDFKW mithilfe der oben abgebildeten Caesar-Scheibe.

2 Der Geheimtext lautet BNCDFDJMZBJS. Es ist nur bekannt, dass der erste Buchstabe des Klartextes ein C war. Wie lautet die Botschaft? Nutze dazu eine selbst gebastelte Caesar-Scheibe oder schreibe die beiden Alphabete untereinander.

3 Vergleiche die Sicherheit der Caesar-Verschlüsselung mit der Sicherheit eines Zahlenschlosses. Beachte dabei die Anzahl der nötigen Versuche, bis der Code geknackt ist.

4 Das folgende Wort ist mit dem Caesar-Verfahren verschlüsselt worden: ZSGKPHCEJ. Versucht zu zweit den Geheimtext zu knacken und diskutiert, warum das Knacken hier besonders schwierig ist.

5 Codiere deinen Namen mithilfe der folgenden Tabelle. Versucht in einer Kleingruppe eure Geheimtexte zu knacken. Diskutiert ob diese Verschlüsselung sicherer ist, als die Caesar-Verschlüsselung.

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

6 Überlegt euch zu zweit eine eigenes Verschlüsselungsverfahren. Probiert es aus, indem ihr gegenseitig verschlüsselte Nachrichten austauscht.
Überlegt, wie gut euer Verfahren im Vergleich zur Caesar-Verschlüsselung ist.

Abbildung 2: Analysematerial zur Thematik *Die Caesar-Verschlüsselung* (Kuhn et al. 2021[2]).

# Aufgabe

1. Analysieren Sie das vorliegende Material aus Abbildung 2 und identifizieren Sie, welche der zuvor genannten Merkmale/Herausforderungen auf der Wort-, Satz- und Textebene zu finden sind.

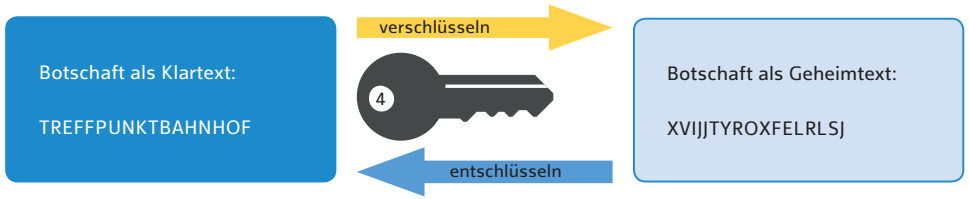
[2]Markus Kuhn et al. (2021): *Praxis Informatik 5/6: Nordrhein-Westfalen: Prüfauflage*. Braunschweig: Westermann, S. 39–40. ISBN: 978-3-14-116915-7.

# 3 Sicher ist sicher: Daten verschlüsseln

Leon erzählt Ina von einem Agentenfilm, den er gestern Abend im Fernsehen anschauen durfte. „Das war spannend! Die Agenten konnten sich untereinander geheime Botschaften schicken, die sonst niemand entschlüsseln konnte!“
„Wenn wir so etwas hätten, könnten wir uns Nachrichten schicken, die nur wir verstehen!"

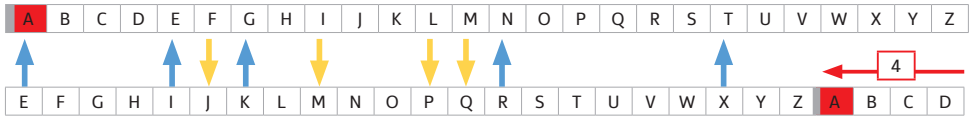
## Die Caesar-Verschlüsselung

Eines der ältesten Verschlüsselungsverfahren nutzte bereits der römische Kaiser Julius Caesar vor über 2000 Jahren. Damit konnte er seinen Soldaten Befehle schicken, die der Feind nicht verstehen konnte, auch wenn ihm die geheimen Botschaften in die Hände gefallen wären.




Das Verschlüsseln von Nachrichten funktioniert so: Jeder Buchstabe des Klartextes wird durch einen anderen Buchstaben ersetzt. Dazu schreibt man zwei Alphabete untereinander. In der oberen Reihe stehen die Buchstaben des Alphabets für den Klartext. In der unteren Reihe das verschobene Alphabet für den Geheimtext. Im Geheimtext sind die Buchstaben um eine bestimmte Zahl von Stellen nach links verschoben. Diese Zahl ist der **Schlüssel**. Den braucht man, um aus dem Klartext in der oberen Zeile einen Geheimtext zu machen und umgekehrt.

**Beispiel:** Verschlüsseln und Entschlüsseln mit dem Schlüssel 


**Verschlüsseln:** Folgst du den gelben Pfeilen, wird aus dem Klartext „**FILM**“ der Geheimtext „**JMPQ**“.
**Entschlüsseln:** Folgst Du den blauen Pfeilen, wird aus dem Geheimtext „**EKIRX**“ der Klartext „**AGENT**“.

**1** a) Verschlüssele deinen Vornamen.

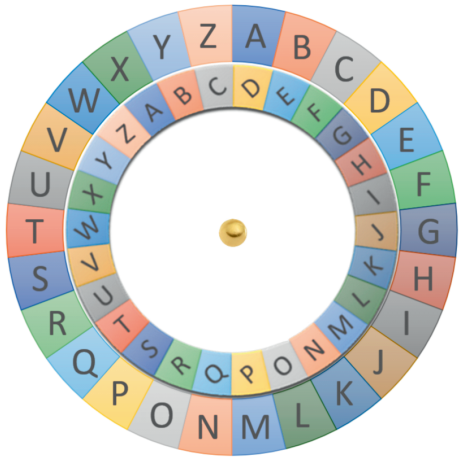
b) Tauscht den verschlüsselten Namen in einer Kleingruppe aus und überprüft eure Ergebnisse gegenseitig.

**Info: Knacken von Verschlüsselungen**
Versucht man eine Nachricht zu entschlüsseln, ohne den Schlüssel zu kennen, spricht man vom Knacken einer Verschlüsselung. Je besser eine Verschlüsselung ist, desto länger dauert es, sie zu knacken. Moderne Verfahren lassen sich auch mit den schnellsten Computern nicht knacken.



## Die Caesar-Scheibe als Werkzeug

Um das Ver- und Entschlüsseln mit unterschiedlichen Schlüsseln zu vereinfachen, kann man sich eine sogenannte **Caesar-Scheibe** selbst basteln. Dazu müssen die beiden Alphabete auf zwei unterschiedlich große Scheiben geschrieben werden. Die beiden Scheiben fixiert man in der Mitte. Am Anfang stehen immer die gleichen Buchstaben untereinander. Nun kann der innere Kreis gedreht werden, sodass immer andere Buchstaben untereinander stehen.




Hier wurde die innere Scheibe um **drei Stellen** gegen den Uhrzeigersinn gedreht. Der Buchstabe A wird durch den Buchstaben D verschlüsselt. Durch die Drehung der inneren Scheibe lassen sich sehr einfach unterschiedliche Schlüssel einstellen.

**Eure Klasse knackt den Code!** Sprecht euch ab und entschlüsselt den folgenden Geheimtext:
NRJZJKUVILEKVIJTYZVUQNZJTYVETFUZVILEXLEUMVIJTYCLVJJVCLEX
**Lösungshinweis:**
Codieren ist wie das Übersetzen von Sprache A in Sprache B. Alle Personen, die die Sprache B sprechen, verstehen die Übersetzung. Beim Verschlüsseln wird ein Text ebenfalls von Sprache A in Sprache B übersetzt. Allerdings sollen nur Personen, die die Sprache B sprechen und einen Schlüssel haben, die Übersetzung verstehen.

**1** Entschlüssele das Wort JXWJHPDFKW mithilfe der oben abgebildeten Caesar-Scheibe.

**2** Der Geheimtext lautet BNCDFDJMZBJS. Es ist nur bekannt, dass der erste Buchstabe des Klartextes ein C war. Wie lautet die Botschaft? Nutze dazu eine selbst gebastelte Caesar-Scheibe oder schreibe die beiden Alphabete untereinander.

**3** Vergleiche die Sicherheit der Caesar-Verschlüsselung mit der Sicherheit eines Zahlenschlosses. Beachte dabei die Anzahl der nötigen Versuche, bis der Code geknackt ist.

**4** Das folgende Wort ist mit dem Caesar-Verfahren verschlüsselt worden: ZSGKPHCEJ. Versucht zu zweit den Geheimtext zu knacken und diskutiert, warum das Knacken hier besonders schwierig ist.

**5** Codiere deinen Namen mithilfe der folgenden Tabelle. Versucht in einer Kleingruppe eure Geheimtexte zu knacken. Diskutiert ob diese Verschlüsselung sicherer ist, als die Caesar-Verschlüsselung.

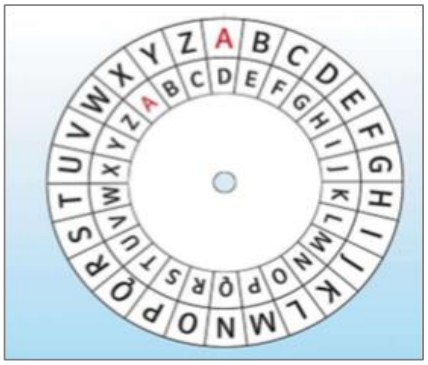
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| J | M | E | N | K | P | F | Q | G | R | V | T | O | U | C | H | D | W | B | X | S | I |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

**6** Überlegt euch zu zweit eine eigenes Verschlüsselungsverfahren. Probiert es aus, indem ihr gegenseitig verschlüsselte Nachrichten austauscht.
Überlegt, wie gut euer Verfahren im Vergleich zur Caesar-Verschlüsselung ist.

# Die Caesar-Verschlüsselung

1 Conrad, Elif und die Caesar-Scheibe

Die Caesar-Verschlüsselung ist eine der frühesten und einfachsten Buchstabensubstitutionen. Der römische Staatsmann und Feldherr Gaius Julius Caesar (100 – 44 v. Chr.) benutzte zwei Scheiben mit den 26 Buchstaben des Alphabets (→ **Abb. 2**), um Nachrichten an seine Soldaten während der Gallienkriege zu verschlüsseln. Caesar hat große Angst gehabt, dass seine Nachrichten in falsche Hände geraten könnten. Boten und Spione, die die Nachrichten überbrachten, waren nicht in die Verschlüsselung eingeweiht. So konnten sie die Nachrichten auch nicht ausplaudern.



2 Caesar-Scheibe

| 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 | 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 |

3 Caesar-Verschiebung (um drei Stellen)

| 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 | 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 |

4 ROT 13

### Auf Caesars Spuren

Wie hat Caesar seine Nachrichten verschlüsselt? Er hat einfach jeden Buchstaben in der Nachricht, durch den Buchstaben, der drei Stellen weiter im Alphabet liegt, ersetzt. Dadurch wird A zu D, B zu E usw. Der Schlüssel ist die Anzahl der Stellen, um die das Alphabet verschoben wurde. Entsprechend wurden die Scheiben eingestellt. Die äußere Scheibe enthielt die Buchstaben des Klartextes, die innere Scheibe die Buchstaben des Geheimtextes (→ **Abb. 2**).

Ein berühmtes Zitat Caesars lautet:
*Alea iacta est.* Frei übersetzt bedeutet das: *Der Würfel ist gefallen.* Verschlüsselt mit der Caesar-Verschlüsselung erhält man: *Dohd ldfwd hvw.*

Nur drei oder darf es etwas mehr sein? Statt genau um drei Stellen zu verschieben, kannst du für deine Verschlüsselung auch eine andere Verschiebung wählen, z. B. um 5 oder 10 Stellen. **Eine** Verschiebung ergibt keinen Sinn. Weißt du auch welche?
Ein Spezialfall stellt die Verschiebung um 13 Stellen dar, die sogenannte ROT 13 (→ **Abb. 4**). ROT steht hier nicht für die Farbe rot, sondern ist die Abkürzung für Rotation (Drehung). Die Besonderheit dieser Verschlüsselung ist, dass die Buchstaben Pärchen bilden. A wird mit N verschlüsselt, N mit A usw.

Nie den Schlüssel verraten, sonst können alle Personen sofort deine Nachrichten lesen!



### Unzählige Möglichkeiten

Das Schöne an der Caesar-Verschlüsselung ist, dass sie leicht anzuwenden ist. Für den Sender ist es einfach, einen Schlüssel festzulegen, er muss sich nur für eine Verschiebung der Buchstaben entscheiden.
Es gibt 25 verschiedene Möglichkeiten, das Alphabet zu verschieben.

Wenn wir uns nicht nur auf die Verschiebung beschränken, sondern jede beliebige Anordnung der Buchstaben zulassen, gibt es über 400 000 000 000 000 000 000 000 000 (Quadrillionen) Möglichkeiten. Da erscheint es unmöglich, eine verschlüsselte Nachricht zu entschlüsseln, wenn man die Anordnung nicht kennt. Oder doch?

### Projekt

**Ave Caesar!**

Teilt eure Klasse in Gruppen ein.
**Ihr braucht pro Person:** *ausgedruckte Caesar-Scheibe, Schere, Briefklammer*
**Vorarbeit:** Jeder erstellt seine Caesar-Scheibe.

**1 Für Anfänger**
Verschlüssele deinen Namen mit der Caesar-Verschlüsselung. Gebt eure Zettel an eine andere Gruppe zum Entschlüsseln weiter.

**2 Für Fortgeschrittene**
Wählt einen Satz mit max. zehn Wörtern von dieser Doppelseite aus und verschlüsselt ihn mit der Caesar-Verschlüsselung. Gebt den Zettel an eine andere Gruppe zum Entschlüsseln.

**3 Für Profis**
Einigt euch in der Gruppe auf einen Text (max. fünf Sätze). Wählt eine Variante der Caesar-Verschlüsselung und verschlüsselt den Text. Gebt den Text einer anderen Gruppe zum Entschlüsseln.

### Merke

- **Die Caesar-Verschlüsselung ist eine einfache Möglichkeit durch Buchstabenverschiebung Texte zu verschlüsseln.**
- **Caesar hat das Alphabet um drei Stellen verschoben, sodass A mit D, B mit E usw. ersetzt wurde.**
- **Das Alphabet kann aber auch um eine beliebige Anzahl Stellen verschoben werden. Ein Sonderfall ist die ROT 13.**

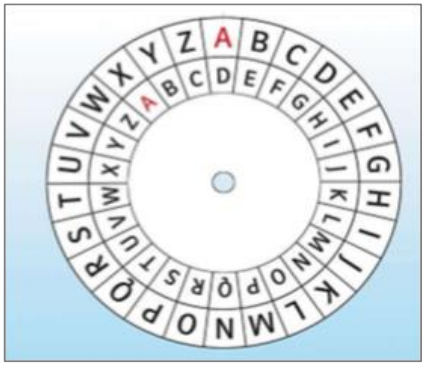
### Aufgaben

1 Führt gemeinsam das Projekt „Ave Caesar!“ durch.
2 Verschlüssele dieses Sprichwort mit dem Schlüssel *6*:
Lieber den Spatz in der Hand alsdie Taube auf dem Dach.
3 Du hast folgende Nachricht abgefangen:
LXG BPRWTC TXCT LPCSTGJCV.QGXCVT QXIIT GTVTCUTHIT ZATXSJCV BXI.
Dir ist bekannt, dass sie von Caesar persönlich stammt. Was möchte Caesar mitteilen?
4 Vereinbare mit einem Mitschüler, der nicht direkt neben dir sitzt, einen Schlüssel. Schreibt eine geheime Botschaft auf und schickt sie von eurem Platz aus über eure Mitschüler zu eurem Partner. Kannst du die verschlüsselten Nachrichten der anderen Schüler verstehen?
5 Simon meint: „Ich kann meinen Text doppelt verschlüsseln. Dann ist er doppelt sicher!“. Was meinst du, stimmt das? Erläutere deine Überlegung schriftlich.
6 Deine Lehrkraft hat dir eine verschlüsselte E-Mail geschickt. Leider hat sie vergessen, dir den Schlüssel zu geben. Kannst du die Nachricht trotzdem entschlüsseln? Notiere deine Vorgehensweise. Die Nachricht lautet:
KHXWH JLEW HV NHLQHKDXVDXIJDEHQ.

# Die Caesar-Verschlüsselung

**1** Conrad, Elif und die Caesar-Scheibe

Die Caesar-Verschlüsselung ist eine der frühesten und einfachsten Buchstabensubstitutionen. Der römische Staatsmann und Feldherr Gaius Julius Caesar (100 – 44 v. Chr.) benutzte zwei Scheiben mit den 26 Buchstaben des Alphabets (→ **Abb. 2**), um Nachrichten an seine Soldaten während der Gallienkriege zu verschlüsseln. Caesar hat große Angst gehabt, dass seine Nachrichten in falsche Hände geraten könnten. Boten und Spione, die die Nachrichten überbrachten, waren nicht in die Verschlüsselung eingeweiht. So konnten sie die Nachrichten auch nicht ausplaudern.



**2** Caesar-Scheibe

### Auf Caesars Spuren

Wie hat Caesar seine Nachrichten verschlüsselt? Er hat einfach jeden Buchstaben in der Nachricht, durch den Buchstaben, der drei Stellen weiter im Alphabet liegt, ersetzt. Dadurch wird A zu D, B zu E usw. Der Schlüssel ist die Anzahl der Stellen, um die das Alphabet verschoben wurde. Entsprechend wurden die Scheiben eingestellt. Die äußere Scheibe enthielt die Buchstaben des Klartextes, die innere Scheibe die Buchstaben des Geheimtextes (→ **Abb. 2**).

Ein berühmtes Zitat Caesars lautet:
*Alea iacta est.* Frei übersetzt bedeutet das: *Der Würfel ist gefallen.* Verschlüsselt mit der Caesar-Verschlüsselung erhält man: *Dohd ldfwd hvw.*

Nur drei oder darf es etwas mehr sein? Statt genau um drei Stellen zu verschieben, kannst du für deine Verschlüsselung auch eine andere Verschiebung wählen, z. B. um 5 oder 10 Stellen. **Eine** Verschiebung ergibt keinen Sinn. Weißt du auch welche?
Ein Spezialfall stellt die Verschiebung um 13 Stellen dar, die sogenannte ROT 13 (→ **Abb. 4**). ROT steht hier nicht für die Farbe rot, sondern ist die Abkürzung für Rotation (Drehung). Die Besonderheit dieser Verschlüsselung ist, dass die Buchstaben Pärchen bilden. A wird mit N verschlüsselt, N mit A usw.

Nie den Schlüssel verraten,
sonst können alle Personen sofort
deine Nachrichten lesen!

| **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** | 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 |

**3** Caesar-Verschiebung (um drei Stellen)

| **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 | 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 |

**4** ROT 13



### Unzählige Möglichkeiten

Das Schöne an der Caesar-Verschlüsselung ist, dass sie leicht anzuwenden ist. Für den Sender ist es einfach, einen Schlüssel festzulegen, er muss sich nur für eine Verschiebung der Buchstaben entscheiden.
Es gibt 25 verschiedene Möglichkeiten, das Alphabet zu verschieben.

Wenn wir uns nicht nur auf die Verschiebung beschränken, sondern jede beliebige Anordnung der Buchstaben zulassen, gibt es über 400 000 000 000 000 000 000 000 000 (Quadrillionen) Möglichkeiten. Da erscheint es unmöglich, eine verschlüsselte Nachricht zu entschlüsseln, wenn man die Anordnung nicht kennt. Oder doch?

### Projekt

**Ave Caesar!**

Teilt eure Klasse in Gruppen ein.
**Ihr braucht pro Person:** *ausgedruckte Caesar-Scheibe, Schere, Briefklammer*
**Vorarbeit:** Jeder erstellt seine Caesar-Scheibe.

**1 Für Anfänger**
Verschlüssele deinen Namen mit der Caesar-Verschlüsselung. Gebt eure Zettel an eine andere Gruppe zum Entschlüsseln weiter.

**2 Für Fortgeschrittene**
Wählt einen Satz mit max. zehn Wörtern von dieser Doppelseite aus und verschlüsselt ihn mit der Caesar-Verschlüsselung. Gebt den Zettel an eine andere Gruppe zum Entschlüsseln.

**3 Für Profis**
Einigt euch in der Gruppe auf einen Text (max. fünf Sätze). Wählt eine Variante der Caesar-Verschlüsselung und verschlüsselt den Text. Gebt den Text einer anderen Gruppe zum Entschlüsseln.

### Merke

- **Die Caesar-Verschlüsselung ist eine einfache Möglichkeit durch Buchstabenverschiebung Texte zu verschlüsseln.**
- **Caesar hat das Alphabet um drei Stellen verschoben, sodass A mit D, B mit E usw. ersetzt wurde.**
- **Das Alphabet kann aber auch um eine beliebige Anzahl Stellen verschoben werden. Ein Sonderfall ist die ROT 13.**

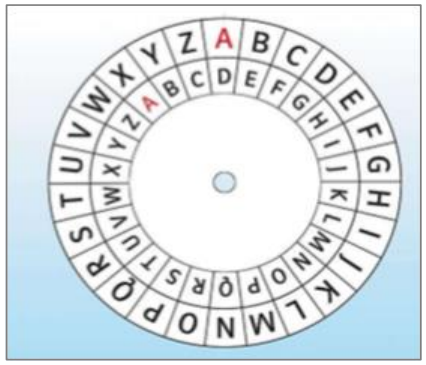
### Aufgaben

1 Führt gemeinsam das Projekt „Ave Caesar!“ durch.
2 Verschlüssele dieses Sprichwort mit dem Schlüssel *6*:
Lieber den Spatz in der Hand alsdie Taube auf dem Dach.
3 Du hast folgende Nachricht abgefangen:
LXG BPRWTC TXCT LPCSTGJCV.QGXCVT QXIIT GTVTCUTHIT ZATXSJCV BXI.
Dir ist bekannt, dass sie von Caesar persönlich stammt. Was möchte Caesar mitteilen?
4 Vereinbare mit einem Mitschüler, der nicht direkt neben dir sitzt, einen Schlüssel. Schreibt eine geheime Botschaft auf und schickt sie von eurem Platz aus über eure Mitschüler zu eurem Partner. Kannst du die verschlüsselten Nachrichten der anderen Schüler verstehen?
5 Simon meint: „Ich kann meinen Text doppelt verschlüsseln. Dann ist er doppelt sicher!“. Was meinst du, stimmt das? Erläutere deine Überlegung schriftlich.
6 Deine Lehrkraft hat dir eine verschlüsselte E-Mail geschickt. Leider hat sie vergessen, dir den Schlüssel zu geben. Kannst du die Nachricht trotzdem entschlüsseln? Notiere deine Vorgehensweise. Die Nachricht lautet:
KHXWH JLEW HV NHLQHKDXVDXIJDEHQ.

# Die Caesar-Verschlüsselung

**1** Conrad, Elif und die Caesar-Scheibe

Die Caesar-Verschlüsselung ist eine der frühesten und einfachsten Buchstabensubstitutionen. Der römische Staatsmann und Feldherr Gaius Julius Caesar (100 – 44 v. Chr.) benutzte zwei Scheiben mit den 26 Buchstaben des Alphabets (→ **Abb. 2**), um Nachrichten an seine Soldaten während der Gallienkriege zu verschlüsseln. Caesar hat große Angst gehabt, dass seine Nachrichten in falsche Hände geraten könnten. Boten und Spione, die die Nachrichten überbrachten, waren nicht in die Verschlüsselung eingeweiht. So konnten sie die Nachrichten auch nicht ausplaudern.



**2** Caesar-Scheibe

### Auf Caesars Spuren

Wie hat Caesar seine Nachrichten verschlüsselt? Er hat einfach jeden Buchstaben in der Nachricht, durch den Buchstaben, der drei Stellen weiter im Alphabet liegt, ersetzt. Dadurch wird A zu D, B zu E usw. Der Schlüssel ist die Anzahl der Stellen, um die das Alphabet verschoben wurde. Entsprechend wurden die Scheiben eingestellt. Die äußere Scheibe enthielt die Buchstaben des Klartextes, die innere Scheibe die Buchstaben des Geheimtextes (→ **Abb. 2**).

Ein berühmtes Zitat Caesars lautet: *Alea iacta est.* Frei übersetzt bedeutet das: *Der Würfel ist gefallen.* Verschlüsselt mit der Caesar-Verschlüsselung erhält man: *Dohd ldfwd hvw.*

Nur drei oder darf es etwas mehr sein? Statt genau um drei Stellen zu verschieben, kannst du für deine Verschlüsselung auch eine andere Verschiebung wählen, z. B. um 5 oder 10 Stellen. **Eine** Verschiebung ergibt keinen Sinn. Weißt du auch welche?
Ein Spezialfall stellt die Verschiebung um 13 Stellen dar, die sogenannte ROT 13 (→ **Abb. 4**). ROT steht hier nicht für die Farbe rot, sondern ist die Abkürzung für Rotation (Drehung). Die Besonderheit dieser Verschlüsselung ist, dass die Buchstaben Pärchen bilden. A wird mit N verschlüsselt, N mit A usw.

Nie den Schlüssel verraten, sonst können alle Personen sofort deine Nachrichten lesen!

| **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** | 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 |

**3** Caesar-Verschiebung (um drei Stellen)

| **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 | 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 |

**4** ROT 13



### Unzählige Möglichkeiten

Das Schöne an der Caesar-Verschlüsselung ist, dass sie leicht anzuwenden ist. Für den Sender ist es einfach, einen Schlüssel festzulegen, er muss sich nur für eine Verschiebung der Buchstaben entscheiden.
Es gibt 25 verschiedene Möglichkeiten, das Alphabet zu verschieben.

Wenn wir uns nicht nur auf die Verschiebung beschränken, sondern jede beliebige Anordnung der Buchstaben zulassen, gibt es über 400 000 000 000 000 000 000 000 000 (Quadrillionen) Möglichkeiten. Da erscheint es unmöglich, eine verschlüsselte Nachricht zu entschlüsseln, wenn man die Anordnung nicht kennt. Oder doch?

### Projekt

**Ave Caesar!**

Teilt eure Klasse in Gruppen ein.
**Ihr braucht pro Person:** *ausgedruckte Caesar-Scheibe, Schere, Briefklammer*
**Vorarbeit:** Jeder erstellt seine Caesar-Scheibe.

**1 Für Anfänger**
Verschlüssele deinen Namen mit der Caesar-Verschlüsselung. Gebt eure Zettel an eine andere Gruppe zum Entschlüsseln weiter.

**2 Für Fortgeschrittene**
Wählt einen Satz mit max. zehn Wörtern von dieser Doppelseite aus und verschlüsselt ihn mit der Caesar-Verschlüsselung. Gebt den Zettel an eine andere Gruppe zum Entschlüsseln.

**3 Für Profis**
Einigt euch in der Gruppe auf einen Text (max. fünf Sätze). Wählt eine Variante der Caesar-Verschlüsselung und verschlüsselt den Text. Gebt den Text einer anderen Gruppe zum Entschlüsseln.

### Merke

- Die Caesar-Verschlüsselung ist eine einfache Möglichkeit durch Buchstabenverschiebung Texte zu verschlüsseln.
- Caesar hat das Alphabet um drei Stellen verschoben, sodass A mit D, B mit E usw. ersetzt wurde.
- Das Alphabet kann aber auch um eine beliebige Anzahl Stellen verschoben werden. Ein Sonderfall ist die ROT 13.

### Aufgaben

**1** Führt gemeinsam das Projekt „Ave Caesar!“ durch.

**2** Verschlüssele dieses Sprichwort mit dem Schlüssel *6*:
Lieber den Spatz in der Hand als die Taube auf dem Dach.

**3** Du hast folgende Nachricht abgefangen:
LXG BPRWTC TXCT LPCSTGJCV. QGXCVT QXIIT GTVTCUTHIT ZATXSJCV BXI.
Dir ist bekannt, dass sie von Caesar persönlich stammt. Was möchte Caesar mitteilen?

**4** Vereinbare mit einem Mitschüler, der nicht direkt neben dir sitzt, einen Schlüssel. Schreibt eine geheime Botschaft auf und schickt sie von eurem Platz aus über eure Mitschüler zu eurem Partner. Kannst du die verschlüsselten Nachrichten der anderen Schüler verstehen?

**5** Simon meint: „Ich kann meinen Text doppelt verschlüsseln. Dann ist er doppelt sicher!“. Was meinst du, stimmt das? Erläutere deine Überlegung schriftlich.

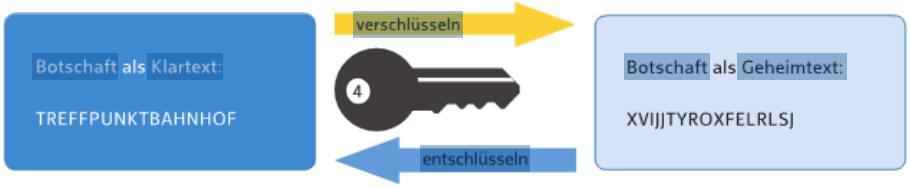
**6** Deine Lehrkraft hat dir eine verschlüsselte E-Mail geschickt. Leider hat sie vergessen, dir den Schlüssel zu geben. Kannst du die Nachricht trotzdem entschlüsseln? Notiere deine Vorgehensweise. Die Nachricht lautet:
KHXWH JLEW HV NHLQHKDXVDXIJDEHQ.

# 3 Sicher ist sicher: Daten verschlüsseln

Leon erzählt Ina von einem Agentenfilm, den er gestern Abend im Fernsehen anschauen durfte. „Das war spannend! Die Agenten konnten sich untereinander geheime Botschaften schicken, die sonst niemand entschlüsseln konnte!"
„Wenn wir so etwas hätten, könnten wir uns Nachrichten schicken, die nur wir verstehen!"

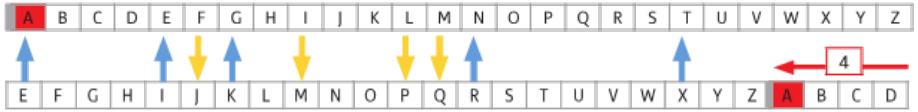
## Die Caesar-Verschlüsselung

Eines der ältesten Verschlüsselungsverfahren nutzte bereits der römische Kaiser Julius Caesar vor über 2000 Jahren. Damit konnte er seinen Soldaten Befehle schicken, die der Feind nicht verstehen konnte, auch wenn ihm die geheimen Botschaften in die Hände gefallen wären.




Das Verschlüsseln von Nachrichten funktioniert so: Jeder Buchstabe des Klartextes wird durch einen anderen Buchstaben ersetzt. Dazu schreibt man zwei Alphabete untereinander. In der oberen Reihe stehen die Buchstaben des Alphabets für den Klartext. In der unteren Reihe das verschobene Alphabet für den Geheimtext. Im Geheimtext sind die Buchstaben um eine bestimmte Zahl von Stellen nach links verschoben. Diese Zahl ist der Schlüssel. Den braucht man, um aus dem Klartext in der oberen Zeile einen Geheimtext zu machen und umgekehrt.

**Beispiel:** Verschlüsseln und Entschlüsseln mit dem Schlüssel 


**Verschlüsseln:** Folgst du den gelben Pfeilen, wird aus dem Klartext „FILM" der Geheimtext „JMPQ".
**Entschlüsseln:** Folgst Du den blauen Pfeilen, wird aus dem Geheimtext „EKIRX" der Klartext „AGENT".

**Info: Knacken von Verschlüsselungen**
Versucht man eine Nachricht zu entschlüsseln, ohne den Schlüssel zu kennen, spricht man vom Knacken einer Verschlüsselung. Je besser eine Verschlüsselung ist, desto länger dauert es, sie zu knacken. Moderne Verfahren lassen sich auch mit den schnellsten Computern nicht knacken.

1 a) Verschlüssele deinen Vornamen.
b) Tauscht den verschlüsselten Namen in einer Kleingruppe aus und überprüft eure Ergebnisse gegenseitig.



## Die Caesar-Scheibe als Werkzeug

Um das Ver- und Entschlüsseln mit unterschiedlichen Schlüsseln zu vereinfachen, kann man sich eine sogenannte Caesar-Scheibe selbst basteln. Dazu müssen die beiden Alphabete auf zwei unterschiedlich große Scheiben geschrieben werden. Die beiden Scheiben fixiert man in der Mitte. Am Anfang stehen immer die gleichen Buchstaben untereinander. Nun kann der innere Kreis gedreht werden, sodass immer andere Buchstaben untereinander stehen.

Hier wurde die innere Scheibe um **drei Stellen** gegen den Uhrzeigersinn gedreht. Der Buchstabe A wird durch den Buchstaben D verschlüsselt. Durch die Drehung der inneren Scheibe lassen sich sehr einfach unterschiedliche Schlüssel einstellen.


**Eure Klasse knackt den Code!** Sprecht euch ab und entschlüsselt den folgenden Geheimtext:
NRJZJKUVILEKVIJTYZVUQNZJTYVETFUZVILEXLEUMVIJTYCLVJJVCLEX
**Lösungshinweis:**
Codieren ist wie das Übersetzen von Sprache A in Sprache B. Alle Personen, die die Sprache B sprechen, verstehen die Übersetzung. Beim Verschlüsseln wird ein Text ebenfalls von Sprache A in Sprache B übersetzt. Allerdings sollen nur Personen, die die Sprache B sprechen und einen Schlüssel haben, die Übersetzung verstehen.

1 Entschlüssele das Wort JXWJHPDFKW mithilfe der oben abgebildeten Caesar-Scheibe.

2 Der Geheimtext lautet BNCDFDJMZBJS. Es ist nur bekannt, dass der erste Buchstabe des Klartextes ein C war. Wie lautet die Botschaft? Nutze dazu eine selbst gebastelte Caesar-Scheibe oder schreibe die beiden Alphabete untereinander.

3 Vergleiche die Sicherheit der Caesar-Verschlüsselung mit der Sicherheit eines Zahlenschlosses. Beachte dabei die Anzahl der nötigen Versuche, bis der Code geknackt ist.

4 Das folgende Wort ist mit dem Caesar-Verfahren verschlüsselt worden: ZSGKPHCEJ. Versucht zu zweit den Geheimtext zu knacken und diskutiert, warum das Knacken hier besonders schwierig ist.

5 Codiere deinen Namen mithilfe der folgenden Tabelle. Versucht in einer Kleingruppe eure Geheimtexte zu knacken. Diskutiert ob diese Verschlüsselung sicherer ist, als die Caesar-Verschlüsselung.

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

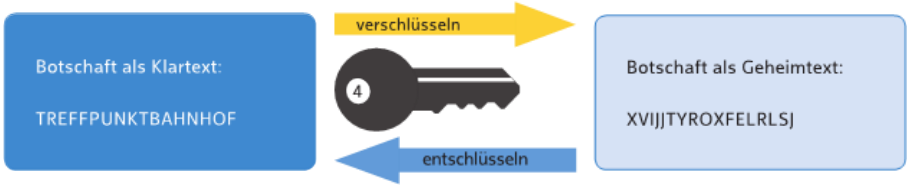
6 Überlegt euch zu zweit eine eigenes Verschlüsselungsverfahren. Probiert es aus, indem ihr gegenseitig verschlüsselte Nachrichten austauscht.
Überlegt, wie gut euer Verfahren im Vergleich zur Caesar-Verschlüsselung ist.

# 3 Sicher ist sicher: Daten verschlüsseln

Leon erzählt Ina von einem Agentenfilm, den er gestern Abend im Fernsehen anschauen durfte. „Das war spannend! Die Agenten konnten sich untereinander geheime Botschaften schicken, die sonst niemand entschlüsseln konnte!"
„Wenn wir so etwas hätten, könnten wir uns Nachrichten schicken, die nur wir verstehen!"

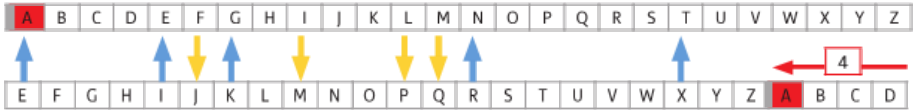
## Die Caesar-Verschlüsselung

Eines der ältesten Verschlüsselungsverfahren nutzte bereits der römische Kaiser Julius Caesar vor über 2000 Jahren. Damit konnte er seinen Soldaten Befehle schicken, die der Feind nicht verstehen konnte, auch wenn ihm die geheimen Botschaften in die Hände gefallen wären.




Das Verschlüsseln von Nachrichten funktioniert so: Jeder Buchstabe des Klartextes wird durch einen anderen Buchstaben ersetzt. Dazu schreibt man zwei Alphabete untereinander. In der oberen Reihe stehen die Buchstaben des Alphabets für den Klartext. In der unteren Reihe das verschobene Alphabet für den Geheimtext. Im Geheimtext sind die Buchstaben um eine bestimmte Zahl von Stellen nach links verschoben. Diese Zahl ist der **Schlüssel**. Den braucht man, um aus dem Klartext in der oberen Zeile einen Geheimtext zu machen und umgekehrt.

**Beispiel:** Verschlüsseln und Entschlüsseln mit dem Schlüssel 


**Verschlüsseln:** Folgst du den gelben Pfeilen, wird aus dem Klartext „FILM" der Geheimtext „JMPQ".
**Entschlüsseln:** Folgst Du den blauen Pfeilen, wird aus dem Geheimtext „EKIRX" der Klartext „AGENT".

**Info:** **Knacken von Verschlüsselungen**
Versucht man eine Nachricht zu entschlüsseln, ohne den Schlüssel zu kennen, spricht man vom Knacken einer Verschlüsselung. Je besser eine Verschlüsselung ist, desto länger dauert es, sie zu knacken. Moderne Verfahren lassen sich auch mit den schnellsten Computern nicht knacken.

**1** a) Verschlüssele deinen Vornamen.

b) Tauscht den verschlüsselten Namen in einer Kleingruppe aus und überprüft eure Ergebnisse gegenseitig.



## Die Caesar-Scheibe als Werkzeug

Um das Ver- und Entschlüsseln mit unterschiedlichen Schlüsseln zu vereinfachen, kann man sich eine sogenannte **Caesar-Scheibe** selbst basteln. Dazu müssen die beiden Alphabete auf zwei unterschiedlich große Scheiben geschrieben werden. Die beiden Scheiben fixiert man in der Mitte. Am Anfang stehen immer die gleichen Buchstaben untereinander. Nun kann der innere Kreis gedreht werden, sodass immer andere Buchstaben untereinander stehen.

Hier wurde die innere Scheibe um **drei Stellen** gegen den Uhrzeigersinn gedreht. Der Buchstabe A wird durch den Buchstaben D verschlüsselt. Durch die Drehung der inneren Scheibe lassen sich sehr einfach unterschiedliche Schlüssel einstellen.

**Eure Klasse knackt den Code!** Sprecht euch ab und entschlüsselt den folgenden Geheimtext:
NRJZJKUVILEKVIJTYZVUQNZJTYVETFUZVILEXLEUMVIJTYCLVJJVCLEX
**Lösungshinweis:**
Codieren ist wie das Übersetzen von Sprache A in Sprache B. Alle Personen, die die Sprache B sprechen, verstehen die Übersetzung. Beim Verschlüsseln wird ein Text ebenfalls von Sprache A in Sprache B übersetzt. Allerdings sollen nur Personen, die die Sprache B sprechen und einen Schlüssel haben, die Übersetzung verstehen.

**1** Entschlüssele das Wort JXWJHPDFKW mithilfe der oben abgebildeten Caesar-Scheibe.

**2** Der Geheimtext lautet BNCDFDJMZBJS. Es ist nur bekannt, dass der erste Buchstabe des Klartextes ein C war. Wie lautet die Botschaft? Nutze dazu eine selbst gebastelte Caesar-Scheibe oder schreibe die beiden Alphabete untereinander.

**3** Vergleiche die Sicherheit der Caesar-Verschlüsselung mit der Sicherheit eines Zahlenschlosses. Beachte dabei die Anzahl der nötigen Versuche, bis der Code geknackt ist.

**4** Das folgende Wort ist mit dem Caesar-Verfahren verschlüsselt worden: ZSGKPHCEJ. Versucht zu zweit den Geheimtext zu knacken und diskutiert, warum das Knacken hier besonders schwierig ist.

**5** Codiere deinen Namen mithilfe der folgenden Tabelle. Versucht in einer Kleingruppe eure Geheimtexte zu knacken. Diskutiert ob diese Verschlüsselung sicherer ist, als die Caesar-Verschlüsselung.

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

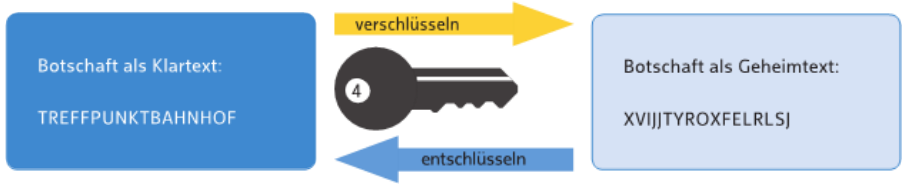
**6** Überlegt euch zu zweit eine eigenes Verschlüsselungsverfahren. Probiert es aus, indem ihr gegenseitig verschlüsselte Nachrichten austauscht.
Überlegt, wie gut euer Verfahren im Vergleich zur Caesar-Verschlüsselung ist.

# 3 Sicher ist sicher: Daten verschlüsseln

Leon erzählt Ina von einem Agentenfilm, den er gestern Abend im Fernsehen anschauen durfte. „Das war spannend! Die Agenten konnten sich untereinander geheime Botschaften schicken, die sonst niemand entschlüsseln konnte!"
„Wenn wir so etwas hätten, könnten wir uns Nachrichten schicken, die nur wir verstehen!"

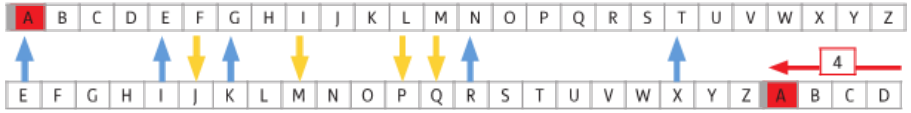
## Die Caesar-Verschlüsselung

Eines der ältesten Verschlüsselungsverfahren nutzte bereits der römische Kaiser Julius Caesar vor über 2000 Jahren. Damit konnte er seinen Soldaten Befehle schicken, die der Feind nicht verstehen konnte, auch wenn ihm die geheimen Botschaften in die Hände gefallen wären.




Das Verschlüsseln von Nachrichten funktioniert so: Jeder Buchstabe des Klartextes wird durch einen anderen Buchstaben ersetzt. Dazu schreibt man zwei Alphabete untereinander. In der oberen Reihe stehen die Buchstaben des Alphabets für den Klartext. In der unteren Reihe das verschobene Alphabet für den Geheimtext. Im Geheimtext sind die Buchstaben um eine bestimmte Zahl von Stellen nach links verschoben. Diese Zahl ist der **Schlüssel**. Den braucht man, um aus dem Klartext in der oberen Zeile einen Geheimtext zu machen und umgekehrt.

**Beispiel:** Verschlüsseln und Entschlüsseln mit dem Schlüssel 


**Verschlüsseln:** Folgst du den gelben Pfeilen, wird aus dem Klartext „FILM" der Geheimtext „JMPQ".
**Entschlüsseln:** Folgst Du den blauen Pfeilen, wird aus dem Geheimtext „EKIRX" der Klartext „AGENT".

**1** I a) Verschlüssele deinen Vornamen.

I b) Tauscht den verschlüsselten Namen in einer Kleingruppe aus und überprüft eure Ergebnisse gegenseitig.

**Info: Knacken von Verschlüsselungen**
Versucht man eine Nachricht zu entschlüsseln, ohne den Schlüssel zu kennen, spricht man vom Knacken einer Verschlüsselung. Je besser eine Verschlüsselung ist, desto länger dauert es, sie zu knacken. Moderne Verfahren lassen sich auch mit den schnellsten Computern nicht knacken.



## Die Caesar-Scheibe als Werkzeug

Um das Ver- und Entschlüsseln mit unterschiedlichen Schlüsseln zu vereinfachen, kann man sich eine sogenannte **Caesar-Scheibe** selbst basteln. Dazu müssen die beiden Alphabete auf zwei unterschiedlich große Scheiben geschrieben werden. Die beiden Scheiben fixiert man in der Mitte. Am Anfang stehen immer die gleichen Buchstaben untereinander. Nun kann der innere Kreis gedreht werden, sodass immer andere Buchstaben untereinander stehen.

Hier wurde die innere Scheibe um **drei Stellen** gegen den Uhrzeigersinn gedreht. Der Buchstabe A wird durch den Buchstaben D verschlüsselt. Durch die Drehung der inneren Scheibe lassen sich sehr einfach unterschiedliche Schlüssel einstellen.

**Eure Klasse knackt den Code!** Sprecht euch ab und entschlüsselt den folgenden Geheimtext:
NRJZJKUVILEKVIJTYZVUQNZJTYVETFUZVILEXLEUMVIJTYCLVJJVCLEX
**Lösungshinweis:**
Codieren ist wie das Übersetzen von Sprache A in Sprache B. Alle Personen, die die Sprache B sprechen, verstehen die Übersetzung. Beim Verschlüsseln wird ein Text ebenfalls von Sprache A in Sprache B übersetzt. Allerdings sollen nur Personen, die die Sprache B sprechen und einen Schlüssel haben, die Übersetzung verstehen.

**1** I Entschlüssele das Wort JXWJHPDFKW mithilfe der oben abgebildeten Caesar-Scheibe.

**2** II Der Geheimtext lautet BNCDFDJMZBJS. Es ist nur bekannt, dass der erste Buchstabe des Klartextes ein C war. Wie lautet die Botschaft? Nutze dazu eine selbst gebastelte Caesar-Scheibe oder schreibe die beiden Alphabete untereinander.

**3** II Vergleiche die Sicherheit der Caesar-Verschlüsselung mit der Sicherheit eines Zahlenschlosses. Beachte dabei die Anzahl der nötigen Versuche, bis der Code geknackt ist.

**4** III Das folgende Wort ist mit dem Caesar-Verfahren verschlüsselt worden: ZSGKPHCEJ. Versucht zu zweit den Geheimtext zu knacken und diskutiert, warum das Knacken hier besonders schwierig ist.

**5** III Codiere deinen Namen mithilfe der folgenden Tabelle. Versucht in einer Kleingruppe eure Geheimtexte zu knacken. Diskutiert ob diese Verschlüsselung sicherer ist, als die Caesar-Verschlüsselung.

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

**6** III Überlegt euch zu zweit eine eigenes Verschlüsselungsverfahren. Probiert es aus, indem ihr gegenseitig verschlüsselte Nachrichten austauscht.
Überlegt, wie gut euer Verfahren im Vergleich zur Caesar-Verschlüsselung ist.